EUROPEAN
COMMISSION

Brussels, 24.7.2019
SWD(2019) 650 final

COMMISSION STAFF WORKING DOCUMENT
Accompanying the document

REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities

{COM(2019) 370 final}

INDHOLD

1. INDLEDNING

Den Finansielle Aktionsgruppe (FATF) henstiller, at landene under hensyn til deres kapacitet og erfaring inden for hver enkelt sektor foretager risikovurderinger i henhold til kravene vedrørende bekæmpelse af hvidvask af penge og bekæmpelse af finansiering af terrorisme. De skal identificere, vurdere og forstå risiciene vedrørende hvidvask af penge og finansiering af terrorisme og træffe forebyggende foranstaltninger, der står på mål hermed.

I erkendelse af vigtigheden af en supranational tilgang til identifikation af risici giver direktiv (EU) 2015/849 (fjerde hvidvaskdirektiv) Kommissionen mandat til at foretage en vurdering af konkrete risici for hvidvask af penge og finansiering af terrorisme, der påvirker det indre marked og vedrører grænseoverskridende aktiviteter

Kommissionen offentliggjorde sin første supranationale risikovurdering i 2017.[1] Artikel 6, stk. 1, i det fjerde direktiv om bekæmpelse af hvidvask af penge kræver også, at Kommissionen ajourfører sin rapport hvert andet år (eller oftere, hvis det er relevant). Den aktuelle rapportering ajourfører oplysningerne i 2017-rapporten, analyserer de aktuelle risici vedrørende hvidvask og terrorfinansiering og foreslår en omfattende indsats for at gøre noget ved disse. Det vurderes, i hvilket omfang Kommissionens anbefalinger til forebyggende foranstaltninger er blevet gennemført, og de resterende risici vurderes, idet der tages hensyn til nye produkter og sektorer.

De nærmere oplysninger i risikoanalysen for hver enkelt sektor og hvert enkelt produkt er anført i **bilag 1.**

2. DEN ANVENDTE METODE I DEN SUPRANATIONALE RISIKOVURDERING

Denne supranationale risikovurdering følger den metode[2], der blev anvendt ved den supranationale risikovurdering i 2017, som giver en systematisk analyse af de risici for hvidvask af penge og terrorfinansiering, der er forbundet med de metoder, som anvendes af lovovertrædere. Formålet er at identificere de omstændigheder, hvorunder tjenesteydelser og produkter inden for en given sektor kan blive misbrugt til hvidvask af penge og terrorfinansiering, uden at der fældes dom over sektoren som helhed.

Denne supranationale risikovurdering fokuserer på sårbarheder på EU-niveau, både hvad angår den lovgivningsmæssige ramme og dens faktiske anvendelse. Den præsenterer de største risici for det indre marked inden for en bred vifte af sektorer samt de horisontale sårbarheder, der kan påvirke disse sektorer.

---

1 Rapport fra Kommissionen til Europa-Parlamentet og Rådet om vurderingen af de risici for hvidvask og finansiering af terrorisme, der påvirker det indre marked og vedrører grænseoverskridende aktiviteter, COM(2017) 340 final.

2 Se flere detaljer i SWD(2017) 241.

I denne rapport gøres der rede for risikobegrænsende foranstaltninger, der bør træffes på EU-plan og nationalt plan for at imødegå risiciene, og der fremsættes en række henstillinger til de forskellige berørte aktører. Den foregriber ikke de risikobegrænsende foranstaltninger, som nogle medlemsstater har truffet eller kan beslutte at træffe som reaktion på nationale risici for hvidvask af penge og terrorfinansiering. De risikobegrænsende foranstaltninger i denne rapport skal derfor ses som et udgangspunkt, der kan tilpasses, afhængigt af de nationale foranstaltninger, som allerede findes.

Efter artikel 6, stk. 4, i det fjerde direktiv om bekæmpelse af hvidvask af penge skal medlemsstaterne, hvis de beslutter ikke at gennemføre nogen af henstillingerne i den tidligere supranationale risikovurdering, underrette Kommissionen herom og forelægge den en begrundelse for det ("følg eller forklar"). Kommissionen har indtil dato ikke modtaget en sådan underretning.

Procedure

Under udarbejdelsen af denne rapport gennemførte Kommissionen en bred høringsrunde med alle relevante interessenter, hvorunder den henvendte sig til forskellige sektorer gennem målrettede spørgeskemaer og særlige workshops.

Kommissionen hørte i juli 2018 medlemsstaterne ved hjælp af et spørgeskema med bilag om:

- nationale risikobegrænsende foranstaltninger
- skabeloner for data om finansielle forhold og retsforfølgning mht. hvidvask af penge og terrorfinansiering, og
- nye risici.

Ved udgangen af 2018 havde Kommissionen modtaget 23 svar.[3] Efterfølgende blev medlemsstaterne yderligere hørt i særlige møder i Ekspertgruppen vedrørende Hvidvask af Penge og Finansiering af Terrorisme[4] den 10. december 2018 og den 11. februar 2019.

I november-december 2018 gennemførte Kommissionen fire workshops med interessenter fra den private-sektor, én med repræsentanter for de finansielle institutioner, to med "udpegede ikke-finansielle virksomheder og erhverv" (DNFBP'er)[5] og én med civilsamfundet (NPO'er) og universitetsverdenen. Anden fase af denne møderunde fandt sted i januar 2019. De mundtlige indlæg fra den private sektor blev suppleret med 15 skriftlige svar.

---

[3] BG, CY, FR, HR og IE besvarede ikke spørgeskemaet om opfølgning på henstillingerne.

[4] Denne gruppe består af højtstående embedsmænd med ansvar for bekæmpelse af hvidvask af penge i EU/EØS-landene. http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=2914

[5] Repræsentanter for spilindustrien blev hørt i et særskilt møde.

Kommissionen hørte også andre tilsynsførende instanser og myndigheder som Europol og de europæiske tilsynsmyndigheder (ESA'er).[6]

Formålet med denne brede høring var todelt: at følge op på de henstillinger, der blev givet i 2017 og at ajourføre den supranationale risikovurdering.

I betragtning af, at truslerne og sårbarhederne i forhold hvidvask af penge og terrorfinansiering udvikler sig hele tiden, skal den supranationale risikovurdering have en integreret tilgang til vurderingen af effektiviteten af nationale ordninger til bekæmpelse af hvidvask af penge og terrorfinansiering.

Kommissionen tager med henblik at overvåge deres overensstemmelse med EU-krav, gennemførelsen af dem og deres forebyggende kapacitet behørigt hensyn til nationale risikovurderinger, der er udarbejdet af medlemsstaterne med henblik på at sikre korrekt identifikation og afbødning af konkrete nationale risici.[7]

De enkelte sektorer er ansvarlige for et tredje lag af risikovurdering, der tager højde for risikofaktorer, herunder dem, der vedrører konkrete kunder, lande, produkter, tjenesteydelser, transaktioner og fordelingskanaler.

Disse tre lag (supranationale, nationale og sektorspecifikke) af risikovurdering tillige med risikobegrænsning indgår på passende måde i en omfattende bevidstheds- og analyseproces vedrørende risici mht. hvidvask af penge og terrorfinansiering i EU, hvori forskellige lag supplerer hinanden og er lige relevante.

Kommissionen bygger på og supplerer de nationale og sektorspecifikke vurderinger ved at vurdere risici, som påvirker Unionens indre marked og er forbundet med grænseoverskridende aktiviteter.

Retsgrundlaget

Risikovurderingen skal give et øjebliksbillede af risiciene for hvidvask af penge og terrorfinansiering og kræver nøjagtig timing. Vurderingen af risici, der berører EU, blev foretaget på et tidspunkt, hvor den relevante rammelovgivning stadig var det fjerde direktiv om bekæmpelse af hvidvask af penge. Selvom det femte direktiv om bekæmpelse af hvidvask af penge var vedtaget, var gennemførelsen af det endnu ikke afsluttet.

Derfor er den supranationale risikovurdering baseret på den EU-lovgivning, der var gældende på vurderingstidspunktet. Dette er især vigtigt at understrege, da nogle sektorer ikke, eller kun i begrænset omfang, var omfattet af bestemmelserne i fjerde direktiv om

---

[6] Den Europæiske Banktilsynsmyndighed (EBA), Den Europæiske Tilsynsmyndighed for Forsikrings- og Arbejdsmarkedspensionsordninger (EIOPA) og Den Europæiske Værdipapir- og Markedstilsynsmyndighed (ESMA).

[7] Dette berører ikke vurderinger fra relevante internationale organisationer og standardsættere som FATF og Ekspertkomiteen for Evaluering af Foranstaltninger til Bekæmpelse af Hvidvask af Penge (Moneyval). Moneyval er et permanent overvågningsorgan for Europarådet. Det vurderer overensstemmelsen med de vigtigste internationale standarder for bekæmpelse af hvidvask af penge og terrorfinansiering, og hvor effektivt disse er gennemført, og det fremkommer med henstillinger til nationale myndigheder om, hvordan de kan forbedre deres systemer, https://www.coe.int/en/web/moneyval

bekæmpelse af hvidvask af penge. Derfor kan risikoniveauet blive vurderet anderledes i de medlemsstater, der allerede har bragt den strengere ordning i anvendelse. Men ændringerne i det femte direktiv om bekæmpelse af hvidvask af penge, som skal være gennemført senest i januar 2020, er ikke desto mindre blevet foregrebet i forbindelse med fastlæggelsen af nye risikobegrænsende foranstaltninger.

EU's vigtigste instrument er direktivet om bekæmpelse af hvidvask af penge, men Unionens retlige rammer for bekæmpelse af hvidvask af penge og finansiering af terrorisme suppleres af anden EU-lovgivning. En orienterende liste er vedhæftet i **bilag 2.**

Desuden er en oversigt over anvendte forkortelser i forbindelse med risikoanalysen vedhæftet som **bilag 3** og en bibliografi som **bilag 4**.

3. RESULTATERNE AF DEN SUPRANATIONALE RISIKOVURDERING

Denne supranationale risikovurdering fokuserer på de risici, der er forbundet med hver enkelt relevant sektor og vurderer de henstillinger, der er givet med henblik på at imødegå de pågældende risici. Kommissionen har identificeret **47 produkter og tjenesteydelser,** som den anser for at være potentielt sårbare over for risici for hvidvask af penge og terrorfinansiering på det indre markeds niveau, i forhold til 40 i 2017. Disse 47 produkter og tjenesteydelser omfatter **11 sektorer**, herunder:

- De 10 sektorer eller produkter, som er omhandlet i det fjerde direktiv om bekæmpelse af hvidvask af penge, dvs. kredit- og finansielle institutioner, pengeoverførselsvirksomheder, vekselkontorer, forhandlere af meget værdifulde varer og aktiver-, ejendomsmæglere, udbydere af tjenester til truster og selskaber, revisorer, eksterne regnskabssagkyndige og skatterådgivere, notarer og andre selvstændige retlige aktører samt udbydere af spiltjenester
- 1 kategori af forskellige produkter, som ikke er dækket i det fjerde direktiv om bekæmpelse af hvidvask af penge, men anses for relevante for den risikovurdering, som omfatter kontantintensive virksomheder, virtuelle valutaer, crowdfunding og nonprofitorganisationer. Denne kategori omfatter også visse uformelle procedurer, som anvendes af Hawala[8] og andre tjenesteydere inden for uformel værdioverførsel, og
- fire nye produkter/tjenester, der ikke blev vurderet i 2017-rapporten, nemlig privatejede pengeautomater, professionel fodbold, frihavne samt ordninger vedrørende statsborgerskab og opholdsret for investorer ("gyldne pas/visa").

Derudover indeholder denne rapport en udvidet analyse af nogle af de tjenester, der blev vurderet i 2017, nemlig FinTech, platforme til handel med virtuelle valutaer og udbydere af (virtuelle) tegnebøger samt bankkonti tilhørende ikke-fastboende.

Beskrivelserne og vurderingerne af mange af de produkter/sektorer, som blev analyseret i 2017-rapporten er ikke blevet væsentligt ændret i løbet af de seneste to år, mens Unionens

[8] Hawala er et populært og uformelt system til overførsel af værdier baseret på opfyldelse og ære i et enormt net af pengemæglere ("hawaladarer") frem for flytning af kontante penge.
Uformelle overførsler af værdier ske i systemer eller net, der modtager penge med henblik på, at der kan udbetales penge eller tilsvarende værdier til tredjepart andetsteds, i samme eller en anden form. De finder normalt sted uden for det traditionelle banksystem.

reviderede retlige rammer om bekæmpelse af hvidvask af penge og finansiering af terrorisme er blevet ajourført i væsentligt omfang siden 2017.

Den foreliggende vurdering er en opdatering af oplysningerne i 2017-rapporten, den finjusterer på flere områder (f.eks. nonprofitorganisationer /NPO'er) og ajourfører tal og informationskilder. Desuden er den foreliggende vurdering blevet opdateret, så den indeholder henvisninger til Unionens aktuelle retlige ramme vedrørende bekæmpelse af hvidvask af penge og finansiering af terrorisme, og således, at der er taget hensyn til, at de fleste henstillinger om risikobegrænsende foranstaltninger i den supranationale risikovurdering 2017[9] nu er indeholdt i det femte direktiv om bekæmpelse af hvidvask af penge. Desuden blev opmærksomheden særlig rettet mod medlemsstaternes foranstaltninger til gennemførelse af det fjerde direktiv om bekæmpelse af hvidvask af penge, som skulle være gennemført senest i juli 2017. Andre risikobegrænsende foranstaltninger, der blev anbefalet i den supranationale risikovurdering 2017, er der nu taget højde for i nyere EU-lovgivning som f.eks. direktivet om selskabsret[10] eller den nye forordning om kontrol med likvide midler.[11]

BILAG 1 - RISIKOANALYSE EFTER PRODUKT/SEKTOR

Denne supranationale risikovurdering følger en nærmere bestemt metode, som omfatter systematisk analyse af de risici for hvidvask af penge og finansiering af terrorisme, der er forbundet med lovovertræderens metoder. Formålet er at identificere de omstændigheder, hvorunder de tjenesteydelser og produkter, en given sektor producerer, kan blive misbrugt til hvidvask af penge og terrorfinansiering (uden at der fældes dom over sektoren som helhed).

Den er baseret på direktiv (EU) 2015/849 (fjerde direktiv om bekæmpelse af hvidvask af penge), som var den lovgivning, der var gældende på tidspunktet for analysen. Det femte direktiv om bekæmpelse af hvidvask af penge (direktiv (EU) 2018/843), som ændrede det fjerde direktiv om bekæmpelse af hvidvask af penge, anses som en del af de risikobegrænsende foranstaltninger.

[9] Nogle af dem blev udformet i lyset af Europa-Parlamentets og Rådets direktiv 2005/60/EF af 26. oktober 2005 om forebyggende foranstaltninger mod anvendelse af det finansielle system til hvidvaskning af penge og finansiering af terrorisme EUT L 309 af 25.11.2005, s. 15.

[10] Europa-Parlamentets og Rådets direktiv (EU) 2017/1132 af 14. juni 2017 om visse aspekter af selskabsretten, EUT L 169 af 30.6.2017, s. 46. Dette direktiv dækker:

- Offentlighed omkring selskabsdokumenter, gyldigheden af et selskabs forpligtelser samt ugyldighed. Det gælder for alle aktieselskaber og andre selskaber med begrænset ansvar. Stiftelse af aktieselskaber og regler om bevarelse af og ændring af deres kapital. Det sætter et minimumskapitalkrav for EU-aktieselskaber på 25 000 EUR. Oplysningskrav til udenlandske filialer af selskaber. Det dækker EU-selskaber, som etablerer sig i et andet EU-land eller virksomheder fra tredjelande, der opretter filialer i EU.

[11] Europa-Parlamentets og Rådets forordning (EU) 2018/1672 af 23. oktober 2018 om kontrol med likvide midler, der føres ind i eller ud af Unionen, og om ophævelse af forordning (EF) nr. 1889/2005, EUT L 284 af 12.11.2018, s. 6. Denne forordning supplerer EU's retlige ramme vedrørende forebyggelse og terrorfinansiering som fastsat i direktiv 2015/849. Den dækker områder, hvorpå en evaluering af forordning (EF) nr. 1889/2005 (forordning om kontrol med likvide midler) konstaterede plads til forbedringer og gennemfører et antal handlingstiltag, som fremgår af Kommissionens handlingsplan med henblik på at styrke bekæmpelsen af finansiering af terrorisme, COM (2016) 50 final, af 02.02.2016.

Hver risiko er bedømt i forhold til trussel og sårbarhed. Bedømmelserne ligger på en skala fra 1 til 4:

1) **mindre betydelig (værdi: 1)**
2) **i moderat grad betydelig (værdi: 2)**
3) **betydelig (værdi: 3)**
4) **meget betydelig (værdi: 4)**

Bedømmelserne blev kun brugt til at sammenfatte analysen. De bør ikke betragtes isoleret fra den faktuelle beskrivelse af risikoen.

LIKVIDE MIDLER

1. Pengekurerer

Produkt
Pengekurerer / bevægelser af likvide midler over den ydre grænse

Generel beskrivelse af den pågældende sektor og det/den relevante produkt/aktivitet
Denne vurdering omfatter de overstatslige risici – dvs. likvider, der kommer ind i/forlader Den Europæiske Union ved EU's ydre grænser.

Udviklingen af internationale standarder til kontrolaf grænseoverskridende strømme af likvide midler, evalueringen af, i hvilken udstrækning forordningen har nået sit mål, og oplysninger modtaget fra medlemsstaterne førte til, at Kommissionen konkluderede, at selvom det samlede resultat af forordningens virkninger var tilfredsstillende, bør en række områder styrkes for at forbedre dens funktion.

For at tage fat på disse områder og som en del af den europæiske dagsorden om sikkerhed og handlingsplan til styrkelse af bekæmpelsen af finansiering af terrorisme vedtog Kommissionen i december 2016 et forslag til en ny forordning om kontrol med likvide midler. Efter lovgivningsarbejdet i Europa-Parlamentet og Rådet blev den nye forordning (EU) nr. 2018/1672[12] vedtaget i oktober 2018 og finder anvendelse fra juni 2021.

Den nugældende forordning om kontrol med likvide midler (forordning (EU) 1889/2005)[13]fastlægger en fælles EU-metode til kontrol med likvide midler på grundlag af et obligatorisk angivelsessystem. Hvis en fysisk person, der ankommer til eller forlader EU (herunder i transit) transporterer kontanter til en værdi af 10 000 EUR eller mere, skal han/hun angive disse midler. Tærskelen på 10 000 EUR anses for højt nok til ikke at belaste flertallet rejsende og forretningsdrivende med uforholdsmæssige administrative

[12] Europa-Parlamentets og Rådets forordning (EU) 2018/1672 af 23. oktober 2018 om kontrol med likvide midler, der føres ind i eller ud af Unionen, og om ophævelse af forordning (EF) nr. 1889/2005, EUT L 284 af 12.11.2018, s. 6.
[13] Forordning nr. 1889/2005/EF, EUT L 284 af 12,11.2018, s. 6.

formaliteter. Men når der er tegn på ulovlige aktiviteter i forbindelse med flytning af likvide midler under 10 000 EUR, er indsamling og registrering af oplysninger om disse flytninger også tilladt. Denne bestemmelse blev indført for at begrænse anvendelsen af "smølfing" eller "strukturering", dvs. den praksis, hvorefter man med overlæg er i besiddelse af beløb under tærsklen i den hensigt at unddrage sig forpligtelsen til at angive (f.eks. opdeling mellem forskellige samhørende personer fra samme gruppe/familie).

De gældende regler om bevægelser af likvide midler ind og ud af EU har fundet anvendelse siden den 15. juni 2007 og er en integreret del af EU's ramme om bekæmpelse af hvidvask af penge og af finansiering af terrorisme. Den nye forordning ajourfører disse regler og supplerer EU's retlige rammer for forebyggelse af hvidvask af penge og finansiering af terrorisme, der fremgår af direktiv 2015/849 som ændret ved direktiv 2018/843.

Den nye forordning om kontrol med likvide midler, som finder anvendelse fra 2021, forbedrer den nuværende kontrolordning for likvide midler, der indføres til eller forlader EU – den seneste udvikling i de internationale standarder for bekæmpelse af hvidvask af penge og af finansiering af terrorisme, der er udviklet af FATF, vil komme til udtryk i EU-lovgivningen.

Ifølge den nye forordning er definitionen af likvide midler udvidet til ikke kun at omfatte kontante penge og ihændehaverpapirer, men også højlikvide råvarer som guld. Forordningen udvides også til at dække likvide midler, der sendes med post, fragt eller budforsendelse. Derudover giver den toldmyndighederne mulighed for at handle på beløb, der er lavere end angivelsestærsklen på 10 000 EUR, hvor der er mistanke om kriminel aktivitet, samtidig med at udvekslingen af oplysninger mellem myndigheder (told og finansielle efterretningsenheder) og medlemsstater forbedres.

Den nye lovgivning udvider forpligtelsen for enhver rejsende, der rejser ind i eller ud af EU med likvide midler en værdi af 10 000 EUR eller mere, til at angive dem til toldmyndighederne. Angivelsen vil blive krævet, uanset om rejsende medbringer likvide midler på deres person, i deres bagage eller i deres transportmiddel. Efter myndighedernes anmodning skal de stille dem til rådighed med henblik på kontrol.

Hvis de likvide midler sendes med andre midler ("uledsagede likvide midler"), vil de kompetente myndigheder få hjemmel til at anmode afsenderen eller modtageren om at foretage en angivelse med oplysninger. Myndighederne vil kunne foretage kontrol af alle forsendelser, pakker eller transportmidler, som kan indeholde uledsagede likvide midler.

Medlemsstaterne vil udveksle oplysninger, hvor der er tegn på, at likvide midler har forbindelse til kriminelle handlinger, som kan have en negativ indflydelse på EU's økonomiske interesser. Denne information vil også blive sendt til Kommissionen.

Derudover bestemmes det i den nye forordning om kontrol med likvide midler artikel 5, stk. 4, at de risikovurderinger, der er udarbejdet af Kommissionen og af FIU'er, skal tages i betragtning af toldmyndighederne, når de fastlægger de fælles risikokriterier for udførelse af kontrol.

Den nye forordning vil ikke forhindre medlemsstaterne i at foretage supplerende national kontrol med bevægelser af likvide midler inden for EU i henhold til deres nationale

lovgivning, forudsat at disse kontroller er i overensstemmelse med Unionens grundlæggende frihedsrettigheder.

Der indgives årligt i gennemsnit 90 000 angivelser af likvide midler, svarende til et samlet beløb på ca. 52 millioner EUR. Toldkontrollen opdager 12.000 tilfælde, hvor likvide midler ikke var blevet angivet, svarende til ca. 345 millioner EUR årligt.

Generel bemærkning

Dette risikoscenarie er uløseligt knyttet til risikoscenariet for anvendelsen af/betaling i kontanter og for pengesedler med høj pålydende værdi.[14]

Kriminelle eller personer, der finansierer terror, og som generer/akkumulerer likvide udbytter, søger at samle og flytte overskuddet fra deres kilde, enten ved at flytte midler til et andet land eller ved at flytte dem til steder, hvor man har lettere adgang til placering i den legale økonomi.

Det karakteristiske ved sådanne steder er en overvejende brug af kontanter, mere lempeligt tilsyn med det finansielle system eller strengere regler om bankhemmelighed. Det kan også bruges af terrorister til at overføre penge hurtigt og sikkert fra et sted til et andet, herunder ved at bruge likvide midler skjult i transitflyvning.

Pengekurerer kan bruge luft- eller søvejen, vej eller jernbane til at krydser en ydre EU-grænse. Derudover kan likvide midler flyttes over ydre grænser uledsaget f.eks. i containere eller andre former for gods eller skjult i postpakker. Hvis lovovertrædere ønsker at flytte meget store beløb i likvide midler, er det ofte en skattet mulighed at skjule det i gods, der kan lægges i containere eller blive transporteret over grænserne på anden måde.

Lovovertrædere kan også bruge avancerede metoder til at skjule likvide midler i gods, som enten bringes over den ydre grænse af en kurer eller sendes med almindelig post eller pakkepost. Selvom uledsagede forsendelser har tendens til at være mindre end dem, der skjules i transportmidler eller på pengekurerers person, kan brugen af pengesedler med høj pålydende værdi stadig resultere i beslaglæggelser af betydelig værdi.

Trussel

Finansiering af terrorisme

Vurderingen af truslen om finansiering af terrorisme i forbindelse med pengekurerer/uledsagede bevægelser af likvide midler viser, at terroristgrupper har gjort brug af forskellige teknikker til at flytte fysiske likvide midler over de ydre grænser, hvilket navnlig er tilfældet for større organisationer.

Denne trussel er især relevant for pengekurerer fra EU til tredjelande. Retshåndhævende myndigheder har beslaglagt store pengebeløb i konfliktzoner, der skulle finansiere terrororganisationer. Yderligere er der konstateret tilfælde, hvor (kommende) udenlandske

[14] Se generelt Europols rapport (2015) *Why is cash still king?:* https://www.europol.europa.eu/sites/default/files/documents/europolcik%20%281%29.pdf

terrorkrigere også optrådte som pengekurerer for at finansiere deres rejser og ophold i konfliktområder. Disse personer medbringer typisk mindre beløb, som er sværere at opdage og eventuelt ikke er omfattet af en forpligtelse til at angive, der påhviler fysiske personer, som medbringer 10 000 EUR eller mere i likvide midler. Da den giver mulighed for anonymitet, opfattes denne fremgangsmåde som attraktiv og temmelig sikker, selvom den trods alt indebærer nogle risici. Det er grunden til, at denne fremgangsmåde også skal ses i sammenhæng med analysen af pengesedler med høj pålydende værdi. Jo flere pengesedler med høj pålydende værdi, der bruges, jo lettere er transporten af likvide midler – selvom de risici, der er forbundet med erhvervelse af store sedler (ikke let tilgængelige) muligvis ikke opvejet fordelene ved ekstra kompakthed. Transport af likvide midler har været en tilbagevendende fremgangsmåde for terroristgrupper i Syrien – selvom det gennemsnitlige beløb, der medbringes af en udenlandsk kriger, der forlader EU, måske ikke er betydeligt sammenlignet med lokalt tilgængelige midler.

Der kan også være en trussel om transport af likvide midler ind i EU fra tredjelande, især fra lande udsat for risici for terrorfinansiering eller fra konfliktområder (f.eks. er der rapporteret om pengekurerer fra Syrien, Golfen og Rusland ind i EU). Der er begrænsede indikationer for bevægelser af meget store likvide beløb ind i EU (dvs. langt over angivelsestærsklen) med det formål at finansiere terrorisme. Der er konstateret tilfælde af mindre beløb, der omfatter integration af likvide beløb, som medbringes fra tredjelande, ind i det finansielle system/den legale økonomi i EU (analyseret særskilt nedenfor).

Fra en lovovertræders risikostyringssynspunkt er forsendelse af likvide midler via post eller med fragt ved brug af mange sendinger, der hver indeholder mindre beløb, en teoretisk set attraktiv mulighed, da der ikke er nogen fysisk kurer, som krydser den ydre grænse medbringende likvide midler, og som vil kunne fanges. Der kan være tale om toldkontrol, men den giver ikke mulighed for fangst af alle relevante data.

Endelig kan lovovertrædere også have et incitament til at konvertere kontanter til andre typer anonyme aktiver, der ikke skal angives (guld, forudbetalte kort - dækket af særskilt analysere nedenfor).[15]

Konklusion: Retshåndhævende myndigheder har samlet bevis for, at pengekurerer gang på gang bruges af terrorgrupper til at finansiere deres aktiviteter eller finansiere udenlandske terrorkrigeres rejser. I lighed med den analyse, der blev foretaget vedrørende likvide midler, frembyder kriminelle elementers eller terrorfinansierende personers anvendelse af pengekurerer fordele for dem, da denne fremgangsmåde er let tilgængeligt og hverken kræver nogen særlig planlægning eller ekspertise. I denne henseende anses truslen om finansiering af terrorisme i relation til pengekurerer som meget betydelig (niveau 4).

[15] Den nye forordning om kontrol med likvide midler, der finder anvendelse fra juni 2021, dækker også guld. For forudbetalte kort er forholdet det, at hvis der foreligger stærke beviser på, at forudbetalte kort misbruges af kriminelle til at føre værdier over EU's grænser under omgåelse lovgivningen, vil en delegeret retsakt kunne bruges til også at lade forudbetalte kort blive omfattet af forordningens anvendelsesområde.

Hvidvask af penge

FATF-rapport: Money laundering through the physical transportation of cash (October 2015) [Hvidvask af penge gennem fysisk transport af likvide midler][16]

På grundlag af et arbejdspapir fra Den Europæiske Centralbank – Forbrugernes anvendelse af kontanter – en landesammenligning med undersøgelsesdata vedrørende betalingsdagbøger,[17] anføres det i rapporten, at i de undersøgte lande gennemføres mellem 46 % og 82 % af alle økonomiske transaktioner kontant, nemlig Australien (65 %), Østrig (82 %), Canada (53 %), Frankrig (56 %), Tyskland (82 %), Nederlandene (52 %) og USA (46 %).[18]

Med hensyn til en økonomi, der er forbundet med grænseoverskridende organiseret kriminalitet, pegede rapporten på fysisk transport af kontanter over en international grænse, som er "en af de ældste og mest basale former for hvidvask" og også bruges til terrorfinansiering.[19] Selvom der ikke foreligger pålidelige data om størrelsen af det beløb, der bliver "hvidvasket" på denne måde, anslog rapporten omfanget til at ligge mellem "hundreder af milliarder og en billion dollar om året". I rapporten forklares det, at de valutaer, man oftest støder på, og som bliver "hvidvasket," er stabile og udbredte valutaer som dollar, euro, schweizerfranc og britiske pund, sædvanligvis ved brug af sedler med høj pålydende værdi. Rapporten fremhæver også, at de kriminelle udnytter mekanismerne i eksisterende angivelsesordninger for likvide midler f.eks. ved "at genbruge angivelser af likvide midler flere gange til samme formål".[20]

Ifølge Europols rapport fra 2015 *Why is cash still king?* bekræfter politiets undersøgelser, at likvide midler, navnlig sedler med høj pålydende værdi, er almindeligt anvendt af kriminelle grupperinger til at gøre det lettere at hvidvaske penge. Selve aktionerne afslører, at enorme summer i kontanter er blevet flyttet og gemt af kriminelle, og at de til stadighed bliver investeret og indført i det legale økonomiske kredsløb på en lang række måder, så de kriminelle bliver fri for voluminøse kontantbeholdninger, der risikerer at blive konfiskeret. Disse metoder kræver en hær af kriminelle medarbejdere og medskyldige eller uagtsomme dørvagter for at sikre, at indføringen af pengene i den legale økonomi ikke vækker mistanke.

I EU er anvendelsen af kontanter stadig den vigtigste årsag til indberetninger om mistænkelige transaktioner i det finansielle system og tegner sig for 34% af alle rapporter.

Kriminelle, som genererer likvide udbytter, søger at samle og flytte udbyttet fra kilden, enten ved at flytte midler til et andet land eller ved at flytte dem til steder, hvor man har lettere adgang til placering i den legale økonomi, måske på grund af den fremherskende brug af kontanter i nogle landes økonomier, mere lempeligt tilsyn med det finansielle system eller strengere regler om bankhemmelighed, eller fordi de kan have større indflydelse i det etablerede økonomiske og politiske system.

[16] http://www.fatf-gafi.org/media/fatf/documents/reports/money-laundering-through-transportation-cash.pdf
[17] https://www.ecb.europa.eu/pub/pdf/scpwps/ecbwp1685.pdf
[18] ECB Arbejdspapir, nr. 1685/juni 2014, tabel 1, s. 38.
[19] FATF-rapporten, s. 3.
[20] sst., s. 16.

Smugling af kontanter kan forekomme i andre led og bruges også ved lovovertrædelser, der ikke genererer likvider. F.eks. benyttes pengekurerer ved cyberkriminalitet som phishing og hacking til at modtage og hæve beløb, man svigagtigt har modtaget fra ofrenes bankkonti, i kontanter. Disse midler sendes derefter via bankoverførsel til andre lande, hvor de modtages i kontanter af et antal udvalgte personer, muligvis med henblik på videretransport.

Efter 2017 er likvide midler forblevet en relevant trussel i forbindelse med hvidvask af penge. Europæiske undersøgelser viser, at bevægelser af likvide midler i og uden for EU er forbundet med lovovertrædelser. De mest relevante kriminalitetsområde er narkotikahandel. Narkotikarelaterede kontante udbytter fra salg og distribution af primært kokain og hash bliver akkumuleret og modtaget af udpegede pengeopsamlere. Narkohandlerorganisationerne træder derefter i forbindelse med pengemæglere (traditionelt uden for EU), og disse mæglere opkræver et gebyr for at sørge for, at narkohandlerorganisationerne modtager værdien af deres udbytter. Mæglerne råder over deres egne hvidvasknetværk i forskellige lande. Når dette er arrangeret, afleverer pengeopsamlere det kontante udbytte til de udvalgte mellemmænd. Derfra begynder pengene at bevæge sig gennem EU mod det udpegede udpassagested eller passerer direkte ud af EU. Den nuværende retlige ramme i EU har i betydelig grad lagt hindringer i vejen for mulighederne for at føre store beløb i fortjenester fra ulovlig narkohandel ind i det finansielle system. På grund af dette bruges pengene i handelsbaserede hvidvaskordninger[21] eller føres af EU mod mere "kontantvenlige" lande. Dubai og Beirut har i de seneste år til stadighed vist sig at være foretrukne kontantdestinationer og voksende økonomiske knudepunkter i EU.

Pengekurererne forbindes med truslen fra pengesedler med høj pålydende værdi: 500 og 200 euro-sedler.

Konklusion: niveauet for truslen vedrørende hvidvask af penge i relation til pengekurerer betragtes som meget betydeligt (niveau 4)

Sårbarhed

Finansiering af terrorisme

a) risikoeksponering

Vurderingen af sårbarheden over for finansiering af terrorisme relateret til pengekurerer viser, at på grund af karakteren af kontante penge gør brugen af pengekurerer det muligt, at store volumener af transaktioner/transport kan finde sted hurtigt og anonymt.

Det grænseoverskridende aspekt af denne fremgangsmåde øger risikoen at involvering af geografiske områder, der er identificeret som højrisikoområder.

[21] Forretningsbaseret hvidvask af penge er den proces, hvorved kriminelle benytter en lovlig forretning til at tilsløre det kriminelle udbytte fra deres skruppelløse kilder. Kriminaliteten omfatter en række ordninger, der har til formå at komplicere dokumentationen af lovlige samhandstransaktioner; disse handlinger kan bestå i flytning af ulovlige varer, forfalskning af dokumenter, forvanskning af finansielle transaktioner samt under- eller overfakturering af varers værdi.

b) risikobevidsthed

Den eksisterende lovgivning (fysiske personers obligatoriske angivelser af likvide midler ved EU's ydre grænser) har øget risikobevidstheden, i hvert fald for så vidt angår personer. Risikobevidstheden eksisterer for uledsaget transport af likvide midler, som nu er omfattet af den nye forordning, – men er mere begrænset.

c) retsgrundlag og kontroller

Der findes kontroller gennem den obligatoriske angivelse af transport af likvide midler ved EU's ydre grænser (forordning om kontrol med likvide midler) og den nye forordning udvider disse toldkontrollet til kontanter sendt som postpakker eller fragt, forudbetalte kort og værdifulde råvarer som guld, der ikke tidligere har været underkastet toldkontrol. Denne lovgivning har øget risikobevidstheden, i hvert fald for så vidt angår fysiske personer. Disse angivelser af kontanter gør det lettere at afsløre mistænkelige transaktioner og rapportere til FIU'erne.

For så vidt angår uledsagede likvide midler (kontanter sendt som vareforsendelser eller pakker) gør den nye forordning det muligt for de kompetente myndigheder at kræve, at afsenderen eller i givet fald modtageren angiver oplysningerne. Angivelsen skal være udfærdiget skriftligt eller elektronisk ved hjælp af en standardformular. Myndighederne vil også have beføjelse til at kontrollere af alle forsendelser, beholdere eller transportmidler, som kan indeholde uledsagede likvide midler.

Konklusion: Risikoeksponeringen i relation til pengekurerer, der er fysiske personer, er nøje forbundet med den kontantbaserede aktivitet (stort volumen, anonymitet, hurtighed) – som skærpes yderligere af den omstændighed – især i en terrorismekontekst – den enkelte kurer oftest medfører beløb under angivelsestærsklen. Mængden af kontanter kan være større for pengekurerer end for uledsagede forsendelser, men risikobevidsthed og kontrolforanstaltninger er til stede.

Brugen af pengekurerer eller metoder til at sende uledsagede likvide midler ind i/ud af EU kombineret med kontante penges anonymitet og (i hvert fald for så vidt angår uledsagede likvide midler) en ufuldkommen kontrolmekanisme, udgør en betydelig udfordring. Selvom mængden af uledsagede likvide midler, der sendes ind i/ud af EU, sandsynligvis er lavere end for ledsagede kurerpostsendinger, udgør risikobevidstheden og kontrollerne af sidstnævnte en større udfordring.

I denne henseende anses sårbarheden over for terrorfinansiering i relation til pengekurerer, der er fysiske personer, som betydelig (niveau 3). Niveauet af sårbarhed over for terrorfinansiering i relation til post/fragt er meget betydelig i betragtning af de eksisterende kontroller/lovgivningsmæssige rammer, mere end den iboende risikoeksponering (niveau 4).

Hvidvask af penge

a) risikoeksponering

Vurderingen af sårbarheden over for hvidvask af penge i relation til pengekurerer viser, at risikoeksponeringen er uløseligt forbundet med den kontantbaserede aktivitet (anonymitet,

hurtighed). Derfor spiller risikoeksponeringen en særlig rolle i forbindelse med denne fremgangsmåde.

b) risikobevidsthed

Den eksisterende lovgivning (obligatoriske angivelser ved EU's ydre grænser af likvide midler, der medføres af fysiske personer) har øget risikobevidstheden, i hvert fald for så vidt angår personer.

Risikobevidsthed eksisterer mht. uledsaget fysisk transport af likvide midler – men er mere begrænset med hensyn til forsendelse/fragt/kurerer.

c) retsgrundlag og kontroller

Som med terrorfinansiering findes der kontroller gennem den obligatoriske angivelse af fysiske personers transport af likvide midler ved EU's ydre grænser (forordning om kontrol med likvide midler).

Disse angivelser af likvide midler gør det lettere at afsløre mistænkelige transaktioner, og de indberettes til FIU'erne (dog er der mangler mht. informationsdeling, og håndhævelsen kan også variere mellem medlemsstaterne).

For så vidt angår uledsagede likvide midler (kontanter sendt som vareforsendelser eller pakker) giver den nye forordning de kompetente myndigheder mulighed for at foretage en risikoanalyse og koncentrere indsatsen om de leverancer, som de anser for at udgøre den største risiko, hvorimod der ikke er pålagt yderligere systematiske formaliteter. Angivelsespligten har en grænseværdi, der er identisk med den, der gælder for kontanter, som medføres af fysiske personer.

Konklusion: Risikoeksponeringen i relation til pengekurerer, der er fysiske personer, er uløseligt forbundet med den kontantbaserede aktivitet (stort volumen, anonymitet, hurtighed). Mængden af kurerpost med kontanter kan være større, men risikobevidsthed og kontrolforanstaltninger er til stede. Brugen af pengekurerer eller metoder til at sende uledsagede likvide midler ind i/ud af EU kombineret med kontante penges anonymitet og (i hvert fald for så vidt angår uledsagede likvide midler) en ufuldkommen kontrolmekanisme, udgør en betydelig udfordring. Selvom mængden af uledsagede likvide midler, der sendes ind i/ud af EU, sandsynligvis er lavere end for ledsagede ere udfordring. I denne henseende anses sårbarheden over for hvidvask af penge i relation til pengekurerer, der er fysiske personer, som betydelig (niveau 3) og ved post/fragt som meget betydelig (niveau 4).

Risikobegrænsende foranstaltninger:

Den nye forordning om kontrol med likvide midler, der gælder fra den 3. juni 2021, styrker de eksisterende regler om bevægelser af likvide midler:

- Den giver myndighederne mulighed for at handle på beløbsstørrelser, der ligger under angivelsestærsklen på 10 000 EUR, hvor der er mistanke om kriminelle handlinger

- Forbedrer informationsudvekslingen mellem myndigheder og medlemsstaterne

- Gør det muligt for de kompetente myndigheder at kræve oplysninger om kontanter sendt i uledsagede forsendelser, f.eks. kontanter sendt i pakker eller fragt

- Udvider definitionen af "likvide midler" til også at omfatte varer, der fungerer som højlikvide kapitalanbringelser som f.eks. guld, og forudbetalte betalingskort, der i øjeblikket ikke er omfattet af standardangivelsen vedrørende likvide midler.

2. Kontantintensiv virksomhed

Produkt
Kontantintensiv virksomhed

Sektor
Barer, restauranter, byggevirksomheder, bilforhandlere, bilvask, kunst- og antikvitetshandlere, auktionshuse, pantelånere, juvelerer, detailforhandlere af tekstiler, spiritus- og tobaksforretninger, detail-/døgnbutikker, spiltjenester, stripklubber, massageklinikker.

Generel beskrivelse af den pågældende sektor og det/den relevante produkt/aktivitet

Den Europæiske Centralbank har givet en interessant beskrivelse af brugen af kontanter i sin rapport *Trends and developments in the use of euro cash over the past ten years*[22] (udgivet som en del af ECB's Økonomiske Bulletin, nummer 6/2018).[23]

Den 2. februar 2016 offentliggjorde Kommissionen en meddelelse til Europa-Parlamentet og Rådet om en handlingsplan med henblik på yderligere at styrke bekæmpelsen af finansiering af terrorisme.[24] Handlingsplanen byggede på de eksisterende EU-regler med henblik på tilpasning til nye trusler og med det formål at opdatere EU's politikker i overensstemmelse med internationale standarder. Den berørte mange emner og løsninger inden for forskellige områder med tilknytning til finansiering af terrorisme.

I forbindelse med Kommissionens indsats for at udvide anvendelsesområdet for forordningen om kontrol med likvide midler, der føres ind i eller ud af EU, blev der henvist til det hensigtsmæssige i at undersøge relevansen af mulige øvre grænser for kontante betalinger.[25] I handlingsplanen bemærkedes videre, at "Flere medlemsstater har indført forbud mod kontantbetalinger over en given tærskel". Sådanne forbud har imidlertid ikke være overvejet på EU-niveau.

Figuren nedenfor viser de begrænsninger af kontante betalinger, der i øjeblikket findes i EU's medlemsstater, samt om der er planer om at tilpasse eller ændre dem. Den første infografik viser, at der aktuelt er kontantforbud i kraft i 16 EU-medlemsstater. Tærsklen varierer fra 500 EUR i Grækenland og 1 000 EUR i Frankrig til ca. 13 800 EUR i Kroatien og 15 000 EUR i Polen. Nederlandene er det eneste land, der har vedtaget en forpligtelse til at angive, og de resterende 11 EU-lande har ikke har nogen gældende kontantbegrænsninger.

I flere EU-medlemsstater er særlige erhvervssektorer eller forbrugere undtaget fra eller mål for kontantforbuddene. I Frankrig, Italien og Spanien skelnes der mellem hjemmehørende

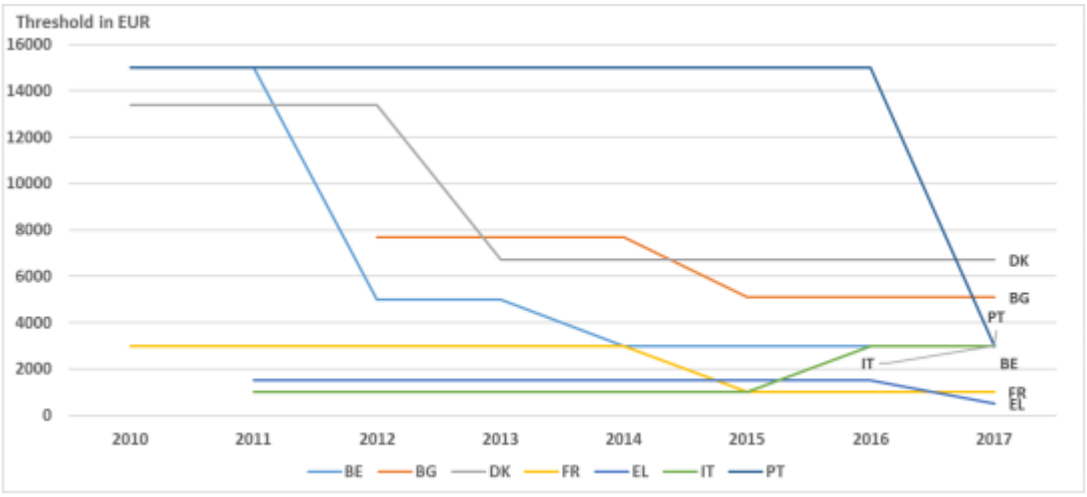
[22] https://www.ecb.europa.eu/pub/economic-bulletin/articles/2018/html/ecb.ebart201806_03.en.html#toc2
[23] https://www.ecb.europa.eu/pub/economic-bulletin/html/eb201806.en.html
[24] COM (2016)50.
[25] I handlingsplanen hedder det, at "Kontantbetalinger anvendes i vid udstrækning til at finansiere terrorhandlinger… I den forbindelse kunne relevansen af eventuelle øvre grænser for kontantbetalinger også undersøges. Flere medlemsstater har indført forbud mod kontantbetalinger over en given tærskel".

i de respektive lande og ikke-hjemmehørende. I den henseende kan ikke-hjemmehørende i Frankrig og Spanien foretage betalinger op til en højere tærskelværdi (15 000 EUR), mens den generelle tærskelværdi ikke gælder for ikke-hjemmehørende i Italien. Andre lande undtager nærmere bestemte sektorer fra kontantrestriktionerne og gør det derved muligt for erhvervsdrivende inden for disse sektorer at gennemføre transaktioner kontant over den almindeligt gældende tærskelværdi. For eksempel er elleve erhvervskategorier inklusive banker og advokater undtaget for tærskelværdierne i Danmark. For så vidt angår Belgien og Kroatien gælder der visse lavere tærskelværdier inden for visse sektorer. For eksempel er kontante transaktioner fuldstændig forbudt i Belgien inden for ejendomssektoren.

Vedtagelse af nye forbud mod kontant betaling diskuteres i en række lande, mens andre overvejer at ændre deres nuværende tærskel. Belgien overvejer at udvide anvendelsesområdet for restriktionerne og inddrage alle transaktioner bortset fra mellem private. Tyskland og Malta overvejer at indføre et forbud mod kontant betaling. Problemstillingen behandles også i Luxembourg og Kroatien, men der er ikke noget konkret forslag til hverken mere eller mindre restriktive foranstaltninger under forberedelse. Tjekkiet er det eneste land, der overvejer at gå i retning af mindre restriktive foranstaltninger.

Source: Ecorys and CEPS own elaboration.

Nedenstående figur viser, at seks EU-lande, som har gældende forbud mod kontant betaling, har sænket tærsklen inden for de seneste syv år. Italien er den eneste EU-medlemsstat, der vedtog et forbud mod kontant betaling med en lavere tærskelværdi (1 000 EUR) og derpå hævde den til 3 000 EUR i 2016.



Source: Ecorys and CEPS own elaboration.

Beskrivelse af risikoscenariet

Lovovertrædere bruger kontantintensive virksomheder:

- til at hvidvaske store mængder kontanter, der er udbytte af kriminel aktivitet, ved at hævde, at midlerne stammer fra økonomiske aktiviteter

- til at hvidvaske kontantbeløb, der er udbyttet af kriminel aktivitet, ved at begrunde deres oprindelse med fiktive økonomiske aktiviteter (både for så vidt angår varer som tjenesteydelser).
- til at finansiere terroraktivitet uden sporbarhed, ofte gennem små kontantbeløb.

Generel bemærkning

Dette risikoscenarie er uløseligt knyttet til risikoscenariet for anvendelsen af/betaling i kontanter og for pengesedler med høj pålydende værdi.

Trussel

Finansiering af terrorisme

Vurderingen af truslen om terrorfinansiering i relation til kontantintensiv virksomhed viser, at kontantintensive virksomheder almindeligvis drives af enkeltpersoner gennem barer, restauranter, telefonbutikker osv., men styres af et net af personer, der danner en terrororganisation. Generelt er de vant til at skaffe rene kontanter i en fart (f.eks. ved at sælge biler eller smykker). Imidlertid bruges dette risikoscenarie ikke i lige stort omfang af alle terrororganisationer (aldrig set for Daesh for eksempel) og er ikke vidt udbredt, da det kræver kvalifikationer at drive virksomheden.

Konklusion: de oplysninger, som er indsamlet af de retshåndhævende myndigheder og de finansielle efterretningsenheder, viser, at der kun er registreret få tilfælde , hvilket betyder, at terrorgrupper ikke foretrækker dette risikoscenarie, da det kræver en vis faglig kunnen og investeringer at drive selve virksomheden, hvilket gør denne fremgangsmåde mindre attraktiv. Men da denne risiko ikke er rent hypotetisk, og da sovende celler er aktive inden for kontantintensiv virksomhed, anses truslen om terrorfinansiering i relation til kontantintensiv virksomhed for i moderat grad betydelig (niveau 2).

Hvidvask af penge

Vurderingen af truslen om hvidvask af penge i relation til kontantintensiv virksomhed viser, at denne fremgangsmåde bliver udnyttet af kriminelle, da den udgør en brugbar mulighed, som er ganske attraktiv og sikker. Den er den letteste måde, hvorpå man kan skjule ulovligt udbytte fra kriminalitet. Men ligesom for terrorfinansiering kræver det et moderat niveau af kvalifikationer at kunne drive virksomheden og at undgå at blive afsløret.

De retshåndhævende myndigheder bekræfter, at kontantintensiv virksomhed fortsat anvendes til at hvidvaske udbyttet af kriminalitet.

Konklusion: kontantintensiv virksomhed foretrækkes af kriminelle organisationer til at hvidvaske udbyttet af kriminalitet. Da det kræver et vist niveau af kvalifikationer at drive virksomheden, betrages truslen om hvidvask af penge i relation til kontantintensiv virksomhed som betydelig (niveau 3).

Sårbarhed

Finansiering af terrorisme

Vurderingen af sårbarheden over for finansiering af terrorisme relation til kontantintensiv virksomhed viser, at de væsentligste faktorer er knyttet til den risiko, som er forbundet med kontanter.

a) risikoeksponering

Kontantintensiv virksomhed er mindre attraktiv for terrororganisationer end for kriminelle (se trusselsvurderingen nedenfor), men når de bruges af terrorister, viser de sårbarheder, fordi den underliggende risiko er den, der er forbundet med kontanter. Sårbarhedsvurderingen vedrørende finansiering af terrorisme i relation til kontantintensiv virksomhed er snævert forbundet med vurderingen i relation til brugen af/betalinger med kontanter generelt og kan følge det samme rationale. Kontantintensive virksomheder gør det muligt at behandle et stort antal anonyme transaktioner, som ikke kræver administration af nye teknologier og sporingsværktøjer. Følgelig er den iboende risikoeksponering høj.

b) risikobevidsthed

Risikobevidstheden synes at være temmelig lav, for selvom store summer penge kan skaffes gennem kontantintensiv virksomhed, bemærker nogle finansielle

efterretningsenheder, at terrororganisationer synes at foretrække pengesedler med lavere pålydende værdi, som ikke så let bliver betragtet som mistænkelige af forpligtede enheder og retshåndhævende myndigheder.

c) retsgrundlag og eksisterende kontroller

De eksisterende retlige rammer i relation til begrænsninger i kontantbetaling, som nogle medlemsstater har indført. Denne ramme varierer meget fra medlemsstat til medlemsstat for så vidt angår kontrol med kontanter og begrænsninger af kontantbetaling, og således kan kontroller potentielt være ikke-eksisterende.

Konklusion: sårbarheden i forhold til kontantintensiv virksomhed er snævert forbundet med brugen af kontanter i almindelighed. Forskelligheden i de eksisterende retlige rammer, den udbredte brug af kontanter i EU's økonomier og det forhold, at sektoren ikke synes at være bevidst om denne risiko, hvorfor sårbarheden over for terrorfinansiering i relation til kontantintensiv virksomhed anses som meget betydelig (niveau 4).

Hvidvask af penge

Vurderingen af sårbarheden over for hvidvask af penge i relation til kontantintensiv virksomhed viser, at de væsentligste faktorer er knyttet til risikoen ved kontanter.

a) risikoeksponering

Sårbarhedsvurderingen vedrørende hvidvask af penge i relation til kontantintensiv virksomhed er snævert forbundet med vurderingen i relation til brugen af/betalinger med kontanter generelt og kan følge det samme rationale. Kontantintensive virksomheder gør det muligt at behandle et stort antal anonyme transaktioner, som ikke kræver administration af nye teknologier og sporingsværktøjer. Denne risikoeksponering omfatter kontant betaling både for varer og tjenesteydelser. Følgelig er den iboende risikoeksponering høj.

b) risikobevidsthed

Forpligtede enheder er normalt bevidste om risikoen ved kontanter - selvom kontroller ikke er lette at gennemføre. Men for andre erhverv, der ikke er omfattet af forpligtelser til bekæmpelse af hvidvask af penge og af finansiering af terrorisme, er risikobevidstheden fortsat en udfordring.

c) retsgrundlag og eksisterende kontroller

Der findes for tiden ingen øvre grænser for kontantbetalinger på EU-plan. I sin handlingsplan for styrkelse af bekæmpelsen af finansiering af terrorisme har Kommissionen allerede signaleret, at øvre grænser for kontantbegrænsninger kunne

undersøges nærmere som et yderligere initiativ til at supplere den nuværende europæiske ramme for bekæmpelsen hvidvask af penge og finansiering af terrorisme.[26]

Sektorens sårbarhed er påvirket af eksistensen, eller manglen på samme, af regler vedrørende begrænsninger af kontant betaling:

- hvor begrænsningsregler findes, er sårbarheder over for hvidvask af penge i relation til kontantintensiv virksomhed lettere blevet begrænset takket være lovkrav, som gør det muligt at afvise kontantbetalinger over en vis tærskel. I disse tilfælde eksisterer kontrollerne og gør det muligt lettere at opdage advarselssignaler og mistænkelige transaktioner. Derudover opfattes disse kontantbetalingsgrænser af sektoren og af de retshåndhævende myndighed som mere effektive og efterhånden som mindre byrdefulde end at indføre kundekendskabskrav. Disse lovlige virksomheder kan imidlertid også skjule skumle og ulovlige aktiviteter, der kan omgå kontantbegrænsningerne.

- hvor der ikke findes begrænsningsregler, ved sektoren ikke, hvordan den skal administrere risiciene, også selvom risikobevidstheden er ganske høj. Den har ingen værktøjer til at kontrollere og opfange mistænkelige transaktioner. Resultatet er, at antallet af rapporter om mistænkelige transaktioner er forholdsvis lavt, eller slet ikke eksisterer.

Nogle medlemsstater har indført krav om rapporter om kontanttransaktioner, som skal angives for kontanttransaktioner over en vis tærskel. Der er imidlertid ingen fælles ordning på europæisk plan.

Set i forhold til det indre marked øger forskellene mellem medlemsstaternes lovgivninger om kontantbegrænsninger det indre markeds sårbarhed; lovovertræderne kan lettere omgå kontrollen i deres oprindelsesland ved at investere i kontantintensiv virksomhed i en anden medlemsstat, der har mere begrænset/ingen kontrol med hensyn til kontantbegrænsning. Eksistensen af begrænsninger i forbindelse med kontantbetalinger i nogle medlemsstater, men ikke i andre medlemsstater skaber muligheden for at omgå restriktionerne ved at flytte til de medlemsstater, hvor der ikke findes begrænsninger og udøve terroristvirksomheden eller andre ulovlige aktiviteter i den "strengere" medlemsstat.

For at øge årvågenheden og mindske de risici, der er forbundet med sådanne kontantbetalinger, er personer, der handler med varer, omfattet af direktivet, såfremt de foretager eller modtager kontant betaling af 10 000 EUR eller mere. Denne tærskel henvises der yderligere til i direktiv 2018/843 (det femte hvidvaskdirektiv). Medlemsstaterne kan fastsætte lavere tærskler, yderligere generelle begrænsninger for brugen af kontanter og yderligere skærpede bestemmelser.

Men effektiviteten af disse foranstaltninger er stadig begrænset i betragtning af antallet af indberetninger af mistænkelige transaktioner. Antallet af indberetninger af mistænkelige transaktioner er generelt lavt, fordi kontanttransaktioner er vanskelige at opfange, der ikke er ret meget tilgængelig information, og forhandlere kan miste deres kunder til konkurrenter, der anvender mere lempelige kontroller. Desuden kan det være vanskeligt

[26] Se COM2015(50).

for en forhandler af meget værdifulde varer at udforme retningslinjer for bekæmpelse af hvidvask af penge og af finansiering af terrorisme i det begrænsede antal tilfælde, hvor en kontanttransaktion over tærsklen finder sted (dvs. det er ikke sektoren i sig selv, der er dækket af ordningen for bekæmpelse af hvidvask af penge og af finansiering af terrorisme – men kun forhandlere af meget værdifulde varer i forbindelse med kontanttransaktioner over en tærskel). Af denne grund har nogle medlemsstater udvidet anvendelsesområdet med bestemte sektorer, uanset om der bruges kontanter. Nogle medlemsstater har også besluttet at anvende en generel ordning med kontantbegrænsning på denne tærskel for at mindske risikoen for, at forhandlere af meget værdifulde varer anvender kundekendskabskravene på en ineffektiv eller besværlig måde. Dette begrænser dog ikke risikoen mht. de situationer, hvor der er tale om kontantintensiv virksomhed, der baserer sig på kontanttransaktioner med mindre beløb – eller et gentaget antal kontanttransaktioner med små beløb.

Hertil kommer, at kontantintensive virksomheder efter deres karakter er risikable, fordi der ikke findes regler om virksomhedsledernes egnethed og hæderlighed. Nogle kontantintensive virksomheder er mere sårbare end andre, fordi de lettere kan give anledning til udveksling af kontanter (bilforhandlere eller pantelånere).

Konklusion: kontantintensive virksomheders risikoeksponering i forhold til hvidvask af penge påvirkes af eksistensen af lovbestemte kontantbegrænsninger, der er effektive i forhold til at begrænse risiciene, men de er ikke altid tilstrækkelige. I en grænseoverskridende kontekst udgør variationerne i reguleringen af kontantbetalinger også en sårbarhedsfaktor. Når der ingen regler findes, er sektorens risikobevidsthed ganske lav, hvilket fører til kun få indberetninger af mistænkelige transaktioner til finansielle efterretningsenheder. Det giver så de retshåndhævende myndigheds ret begrænsede muligheder for efterforskning. I lyset af dette anses niveauet for sårbarhed over for hvidvask af penge i relation til kontantintensiv virksomhed som meget betydeligt (niveau 4).

Risikobegrænsende foranstaltninger:

- Kommissionen undersøgte, om den hurtigt skulle styrke EU's bestemmelser om forebyggelse af finansiering af terrorisme ved at øge gennemsigtigheden af kontantbetalinger gennem indførelse af en restriktion på kontant betaling eller med andre passende midler.[27] Organiseret kriminalitet og terrorfinansiering benytter kontanter til betaling for at gennemføre deres ulovlige aktiviteter og opnår fordele af dem. Ved at begrænse mulighederne for at bruge kontanter ville forslaget bidrage til at afbryde finansieringen af terrorisme og navnlig hvidvaskrelaterede aktiviteter,[28] da behovet for at bruge ikke anonyme betalingsmidler enten ville afskrække fra aktiviteten eller bidrage til, at den lettere kunne afsløres og efterforskes. Rapporten nåede frem til

[27] En rapport fra Kommissionen til Europa-Parlamentet og Rådet om restriktioner for kontantbetalinger (COM (2018) 483 final) blev forelagt den 12. juni 2018.

[28] Det er værd at bemærke, at det i den ovennævnte kommissionsrapport anføres, at *"...begrænsninger af kontantbetalinger ikke i væsentlig grad ville forhindre finansiering af terrorisme. Derimod viste undersøgelsen, at sådanne restriktioner kan være nyttige i bekæmpelsen af hvidvaskning af penge."*

den konklusion, at yderligere lovgivning på området ikke ville blive foreslået for øjeblikket.

- Kommissionen vil fortsat overvåge forhandleres anvendelse af forpligtelserne til bekæmpelse af hvidvask af penge og af finansiering af terrorisme med hensyn til varer, der er omfattet af direktivet om bekæmpelse af hvidvask af penge, og vurdere de risici, der er forbundet med de udbydere af tjenesteydelser, der accepterer kontante betalinger. Den vil desuden vurdere nytteværdien og fordelene for at lade yderligere sektorer blive omfattet af regler om bekæmpelse af hvidvask af penge og af finansiering af terrorisme.

- Medlemsstaterne bør i deres nationale risikovurderinger tage risiciene ved kontant betaling i betragtning med henblik på at fastlægge passende risikobegrænsende foranstaltninger til imødegåelse af risikoen. Medlemsstaterne bør overveje at lade sektorer, der i særlig grad er udsat for risici for hvidvask af penge og terrorfinansiering, blive omfattet af de forebyggende ordninger vedrørende bekæmpelse af hvidvask af penge og af finansiering af terrorisme på grundlag af deres nationale tilsynsmyndigheders resultater.

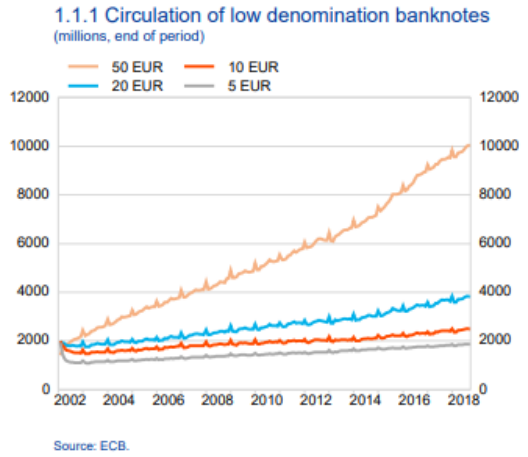
3. Pengesedler med høj pålydende værdi

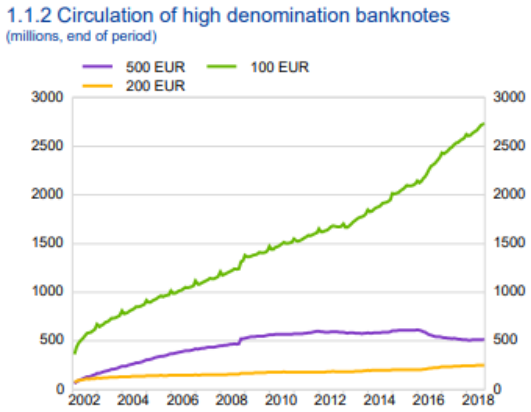
Produkt
Pengesedler med høj pålydende værdi

Sektor
/

Generel beskrivelse af den pågældende sektor og det/den relevante produkt/aktivitet

Til trods for den stadige vækst i pengeløse betalingsmetoder og et moderat fald i anvendelsen af kontante betalinger stiger den samlede værdi af eurosedler i omløb fortsat år for år, ud over inflationsraten. Kontanter anvendes i vid udstrækning til betalinger af beskeden værdi, og anvendelsen heraf i forbindelse med transaktioner skønnes at udgøre ca. en tredjedel af de pengesedler, der er i omløb. Samtidig er efterspørgslen efter sedler med høj pålydende værdi som 500-eurosedlen, der normalt ikke forbindes med betalinger, stadig stor. Dette er en unormal situation, der kan være knyttet til kriminel aktivitet.





Måske det mest betydningsfulde resultat omkring kontanter er, at der ikke foreligger tilstrækkelige oplysninger om brugen af dem, hverken for så vidt angår lovlige eller ulovlige formål. Kontanter og karakteren af den kriminelle økonomi betyder, at der eller kun i få tilfælde findes pålidelige oplysninger om omfanget af almindelige borgeres brug af kontanter, endsige kriminelles.

Et af de få pålidelige tal, der er til rådighed, nemlig om mængden og værdien sedler, der er udstedt og i omløb i EU, efterlader ubesvarede spørgsmål omkring den anvendelse, der gøres af en stor del af de udstedte kontanter, navnlig når man ser på 500-eurosedlen. Af de i alt omkring 1 billion EUR i sedler, der var i omløb ved udgangen af 2014, er brugen af en væsentlig del af disse fortsat ukendt. Desuden tegner 500-eurosedlen alene sig for over 30 % af værdien af alle eurosedler i omløb, selvom den ikke er et almindeligt betalingsmiddel. Selvom der er tegn på, at disse sedler anvendes til hamstring, er denne antagelse ikke dokumenteret. Selv hvis dette er tilfældet, er karakteren af de kontanter, der hamstres (ulovligt eller lovligt) ukendt.

Den 4. maj 2016 besluttede Styrelsesrådet for Den Europæiske Centralbank (ECB) at indstille produktionen og udstedelsen af 500-eurosedlen. Det gjorde det under hensyn til Europols[29] og mange medlemsstaters bekymringer for, at denne pengeseddel letter ulovlige aktiviteter. På baggrund af ECB's beslutning er sedlen ikke siden 27. april 2019 sedlen blevet udstedt af centralbankerne i euroområdet, men fortsætter med at være lovligt betalingsmiddel og kan bruges til at betale med.

Beskrivelse af risikoscenariet

Lovovertræderne bruger sedler med høj pålydende værdi, f.eks. 500-eurosedler, for at gøre transporten af kontanter lettere (jo højere værdi, jo flere penge kan stuves sammen, så de fylder mindre).

Generel bemærkning

Dette risikoscenarie er uløseligt knyttet til risikoscenariet for anvendelsen af/betaling med kontanter og risikoscenariet for kontantintensiv virksomhed.

Trussel

Finansiering af terrorisme

Vurderingen af truslen om terrorfinansiering i relation til pengesedler med høj pålydende værdi viser, at terrorgrupper ikke er ivrige efter at bruge sedler med høj pålydende værdi. De er ikke nødvendigvis lette at komme i nærheden af, og da de ganske let kan opspores, er de ikke attraktive for terrorgrupper, hvis primære mål er at skaffe kontanter så hurtigt som muligt. Af diskretionshensyn har terrorgrupper tendens til at foretrække små sedler. De retshåndhævende myndigheder har kun opdaget få tilfælde, hvilket synes at vise, at forsættet og kapaciteten ikke er ret betydelig.

Konklusion: i denne henseende anses trusselsniveauet fra terrorfinansiering i relation til pengesedler med høj pålydende værdi som i moderat grad betydeligt (niveau 2).

Hvidvask af penge

Vurderingen af truslen om hvidvask af penge i relation til pengesedler med høj pålydende værdi viser, at de gennemgående bliver udnyttet af kriminelle organisationer til at hvidvaske udbyttet af kriminalitet. Risikoen i relation til sedler med høj pålydende værdi er ikke begrænset til 500 EUR, og så længe store summer i kontanter bliver samlet, anses de for at være attraktive for kriminelle organisationer. Det kræver ingen større planlægning eller kompliceret operation – dvs. lovovertrædere har de tekniske færdigheder til let at kunne anvende dette produkt. Det er en aktivitet med "lave omkostninger", som gør det muligt at lagre store beløb på meget lidt plads – hvilket gør det meget attraktivt for organiseret kriminalitet. Retshåndhævende myndigheder har rapporteret, at nogle kriminelle grupperinger søger efter 500-eurosedler ved at betale en præmie for at få adgang til de store pålydende pålydender, hvilket viser sedlens tiltrækningskraft.

[29] https://www.europol.europa.eu/newsroom/news/europol-welcomes-decision-of-ecb-to-stop-printing-eur-500-notes

Selve aktionerne afslører, at enorme summer i kontanter er blevet flyttet og gemt af kriminelle, og at de til stadighed bliver investeret og indført i det legale økonomiske kredsløb på en lang række måder, så de kriminelle bliver fri for voluminøse kontantbeholdninger, der risikerer at blive konfiskeret. Disse metoder kræver masser af kriminelle medhjælpere og medskyldige eller uagtsomme vagter for at sikre, at pengene indgår i den legale økonomi uden at vække mistanke.

I EU er anvendelsen af kontanter stadig den vigtigste årsag til indberetninger om mistænkelige transaktioner i det finansielle system og tegner sig for 34% af alle rapporter.

Kriminelle, som genererer likvide udbytter, søger at samle og flytte udbyttet fra kilden, enten ved at flytte midler til et andet land eller ved at flytte dem til steder, hvor man har lettere adgang til placering i den legale økonomi, måske på grund af den fremherskende brug af kontanter i nogle landes økonomier, mere lempeligt tilsyn med det finansielle system eller strengere regler om bankhemmelighed, eller fordi de kan have større indflydelse i det etablerede økonomiske og politiske system.

Smugling af kontanter kan forekomme i andre led og bruges også ved lovovertrædelser, der ikke genererer likvider. F.eks. benyttes pengekurerer ved cyberkriminalitet som phishing og hacking til at modtage og hæve beløb, man svigagtigt har modtaget fra ofrenes bankkonti, i kontanter. Disse midler sendes derefter via bankoverførsel til andre lande, hvor de modtages i kontanter af et antal udvalgte personer, muligvis med henblik på videretransport.

Pengekurererne forbindes med truslen fra pengesedler med høj pålydende værdi: 500 og 200 euro-sedler. Disse sedler bruges ikke som betalingsmiddel, og faktisk er der mange steder i Europa, hvor de ikke accepteres som betaling. De store pengesedler bruges af kriminelle til at lagre værdi eller til transport (et højt samlet beløb fylder mindre). For eksempel fandt man i værdiboksen for en belgisk undergrundsaktør, der blev afsløret i forbindelse med efterforskningen af hvidvask af udbyttet af organiserede marokkanske kriminelle gruppers salg af hash, overvejende 500 og 200 sedler til en samlet værdi af 1 600 000 euro.

Falske eurosedler smugles fortsat i store mængder på lastbiler og af kurerer. Post- og pakkeforsendelser anvendes i stigende grad til at distribuere falske eurosedler, der sælges via onlineplatforme. Falskmøntnere fortsætter med at sætte falske pengesedler i omløb ved at købe billige varer med pengesedler med høj pålydende værdi og modtage lovlige penge som byttepenge.

<u>Konklusion</u>: pengesedler (500-eurosedler, men ikke kun disse) bruges gennemgående af kriminelle organisationer. Denne fremgangsmåde er let tilgængelig og har beskedne omkostninger. Men henblik på hvidvask af penge er den ganske let at misbruge og kræver ingen særlig planlægning eller viden. I denne henseende anses trusselsniveauet fra hvidvask af penge i relation til pengesedler med høj pålydende værdi som <u>meget betydeligt</u> (niveau 4).

Sårbarhed

Finansiering af terrorisme

Vurderingen af sårbarhed over for terrorfinansiering i relation til pengesedler med høj pålydende værdi viser, at produktet er lige så sårbart over for terrorfinansiering som over for hvidvask af penge, af følgende grunde:

a) risikoeksponering
Der er store mængder sedler med høj pålydende værdi i omløb, på trods af beskeden anvendelse i handelstransaktioner. Kontanter gør det stadig muligt at gennemføre transaktioner hurtigt, anonymt og sporløst.

b) risikobevidsthed
Især har de retshåndhævende myndigheder og finansielle efterretningsenheder en høj risikobevidsthed, og det samme har de forpligtede enheder, der er omfattet af forpligtelserne vedrørende bekæmpelse af hvidvask af penge og af finansiering af terrorisme. Risikobevidstheden hos de sektorer, der ikke er omfattet af forpligtelser vedrørende bekæmpelse af hvidvask af penge og af finansiering af terrorisme eller begrænsningsforpligtelser mht. kontanter, er fortsat en udfordring. Den foreliggende litteratur, navnlig Europol-rapporter, peger på den blinde plet i risikobevidstheden (dvs. den præcise brug af pengesedler med høj pålydende værdi, forskellen mellem medlemsstaterne vedrørende udstedelse, frakobling fra bruttonationalproduktet). Der findes ingen eller næsten ingen pålidelige oplysninger om omfanget af almindelige borgeres brug af kontanter, endsige kriminelles.

c) retsgrundlag og eksisterende kontroller
Terrorgrupper er mindre tiltrukket af pengesedler med høj pålydende værdi, men afsløring er ganske vanskelig, fordi der ikke er nogen EU-harmonisering af retsreglerne vedrørende brug af pengesedler med høj pålydende værdi. Kontrollerne er ujævnt fordelt. Der er ret få rapporter til de finansielle efterretningsenheder, og de fleste af dem kan ikke skelne mellem hvidvask af penge og terrorfinansiering. Brugen af pengesedler af høj værdi til hvidvask af penge kan blive påvirket af Den Europæiske Centralbanks beslutning om gradvis at udfase 500-eurosedlen på grund af de erkendte forbindelser til kriminelle aktiviteter. Men returraten er generelt ret lav, og disse sedler kan fortsat være i brug i lang tid. Derfor kan dette ikke betragtes som en umiddelbar risikobegrænsende foranstaltning.

<u>Konklusion</u>: fra et sårbarhedssynspunkt er risikoeksponeringen høj, risikobevidstheden er lav, og de eksisterende kontrolforanstaltninger er ikke harmoniseret, hvilket skaber potentielle smuthuller, når der er tale om grænseoverskridende transaktioner. I denne henseende anses sårbarhedsniveauet for terrorfinansiering i relation til pengesedler med høj pålydende værdi som <u>meget betydeligt</u> (niveau 4).

Hvidvask af penge

Vurderingen af sårbarheden over for hvidvask af penge i relation til pengesedler med høj pålydende værdi viser følgende karakteristika:

a) risikoeksponering

Sedler med høj pålydende værdi gør det muligt at lagre store mængder kontanter eller sætte dem i omløb på en hurtig og anonym måde. Der er store mængder sedler med høj pålydende værdi i omløb, på trods af den beskedne anvendelse i handelstransaktioner. Brugen af sedler med høj pålydende værdi hejser advarselssignaler, men det ændrer ikke ved, at disse sedler ikke nødvendigvis anvendes til betalinger, men derimod til at flytte pengemidler. Store beløb kan opbevares på meget lidt plads. De er sværere at opdage for finansielle efterretningsenheder og forpligtede enheder.

b) risikobevidsthed

Især har de retshåndhævende myndigheder og finansielle efterretningsenheder en høj risikobevidsthed, og det samme har de forpligtede enheder, der er omfattet af forpligtelserne vedrørende bekæmpelse af hvidvask af penge og af finansiering af terrorisme. Risikobevidstheden hos de sektorer, der ikke er omfattet af forpligtelser vedrørende bekæmpelse af hvidvask af penge og af finansiering af terrorisme eller begrænsningsforpligtelser mht. kontanter, er fortsat en udfordring. Den foreliggende litteratur, navnlig Europol-rapporter, peger på den blinde plet i risikobevidstheden (dvs. den præcise brug af pengesedler med høj pålydende værdi, forskellen mellem medlemsstaterne vedrørende udstedelse, frakobling fra bruttonationalproduktet). Der findes ingen eller næsten ingen pålidelige oplysninger om omfanget af almindelige borgeres brug af kontanter, endsige kriminelles.

c) retsgrundlag og eksisterende kontroller

Brugen af pengesedler af høj værdi til hvidvask af penge kan blive påvirket af Den Europæiske Centralbanks beslutning om gradvis at udfase 500-eurosedlen på grund af de erkendte forbindelser til kriminelle aktiviteter. Men returraten er generelt ret lav, og disse sedler kan fortsat være i brug i lang tid. 500-eurosedlen vil forsat være lovligt betalingsmiddel og kan derfor fortsat anvendes som betalingsmiddel og middel til opbevaring af værdi. Derfor kan dette ikke betragtes som en umiddelbar risikobegrænsende foranstaltning.

<u>Konklusion:</u> i lighed med resultaterne af vurderingen af sårbarheden i forhold til terrorfinansiering i relation til pengesedler med høj pålydende værdi anses sårbarheden over for hvidvask af penge i relation til disse produkter for <u>meget betydelig</u> (niveau 4).

Risikobegrænsende foranstaltninger:

- Overvågningen af returraten for 500-eurosedler vil fortsætte, og der vil ske en vurdering af udviklingen i brugen af 200-eurosedlen.

4. Kontantbetalinger

Produkt
Kontantbetalinger

Sektor
/

Generel beskrivelse af den pågældende sektor og det/den relevante produkt/aktivitet

Den Europæiske Centralbank (ECB) har gennemført en omfattende undersøgelse[30] for at analysere brugen af kontanter, kreditkort og andre betalingsmidler, der brugtes af euroområdets forbrugere ved salgssteder i 2016. Resultaterne af undersøgelsen viser, at i 2016 var kontanter den dominerende betalingsmiddel ved salgssteder. Målt i antal blev 79 % af alle transaktioner gennemført ved brug af kontanter, svarende til 54 % af den samlede værdi af alle betalinger. Kort var det næstmest anvendte betalingsinstrument ved salgssteder; 19 % af alle transaktioner blev gennemført ved brug af et betalingskort. Målt i værdi svarer dette til 39 % af den samlede værdi, der blev betalt ved salgssteder.

Det er således ubestrideligt den foretrukne betalingsmetode blandt forbrugerne for transaktioner af beskeden værdi (dvs. mindre end 20 EUR).

Beskrivelse af risikoscenariet

Lovovertrædere har ofte behov for at bruge en betydelig del af de penge, de har fået, til at betale for de ulovlige varer, de har solgt, for at købe yderligere beholdninger eller til at afholde diverse udgifter i forbindelse med transport af varerne, hvor der er behov for det.

På trods af fordelene og ulemperne ved at handle kontant (beskrevet tidligere i denne rapport) er der ofte intet valg for for kriminelle grupperinger. Den kriminelle økonomi er stadig overvejende kontantbaseret. Det betyder, at uanset om de bryder sig om det eller ej, vil lovovertrædere, der sælger en eller anden form for ulovligt produkt, sandsynligvis blive betalt kontant. Jo mere succesrige lovovertræderne er, og jo mere af varen, de sælger, jo flere kontanter vil de få. Det kan medføre betydelige problemer for lovovertrædere mht. at bruge, opmagasinere og komme af med af deres udbytte. Men på trods af disse problemer opfattes det således, at kontanter giver dem betydelige fordele.

Hertil kommer, at de kriminelles formål er at hvidvaske store mængder kontanter, der er udbytte af kriminel aktivitet, ved at hævde, at midlerne stammer fra økonomiske aktiviteter De kan hvidvaske kontantbeløb ved at begrunde deres oprindelse med fiktive økonomiske aktiviteter (både for så vidt angår varer som tjenesteydelser). Terrorister kan gennem ofte

[30] *The use of cash by households in the euro area,* ECB Occasional Paper Series No 201 / november 2017: https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op201.en.pdf

små kontantbeløb finansiere terroraktiviteter uden sporbarhed (se den generelle beskrivelse under kontantintensiv virksomhed).

Generel bemærkning

Dette risikoscenarie er uløseligt knyttet til risikoscenariet for henholdsvis kontantintensiv virksomhed og pengesedler med høj pålydende værdi.

Trussel

Finansiering af terrorisme

Vurderingen af truslen om terrorfinansiering i relation til kontantbetalinger viser, at terrorgrupper gennemgående bruger kontanter, idet denne fremgangsmåde er let tilgængelig og med beskedne omkostninger. Kontanter ligger til grund for enhver form for ulovlig handel og ulovligt køb af produkter. Generelt er kontanter virkelig attraktive, svære (umulige) at opdage og kræver ikke særlige kvalifikationer at anvende.

Konklusion: på baggrund af feedback fra retshåndhævende myndigheder og finansielle efterretningsenheder anses trusselsniveauet for terrorfinansiering for meget betydeligt (niveau 4).

Hvidvask af penge

Vurderingen af truslen om hvidvask af penge i relation til kontantbetalinger anses for at svare til vurderingen af truslen om terrorfinansiering. For så vidt angår hvidvask af penge er kontanter også det kriminelles foretrukne valg, som gør det muligt let at skjule ulovligt udbytte af kriminalitet og hurtigt at flytte midler, herunder over grænserne. Som mht. terrorfinansiering kræver det ikke særlig kvalifikationer viden eller planlægningskapacitet.

Ulovlige kontanter udleveres til mellemhandlere til at købe varer i lande med ingen eller få begrænsninger for kontantbetalinger. De købte produkter har enten betydelig værdi som f.eks. luksusvarer, eller for hvilke der er en særlig, men betydelig efterspørgsel af f.eks. redskaber (det være sig brugte eller luksusudgaver af entreprenørmaskiner).

Integration af kontanter gennem køb af varer fra lovlige handelsselskaber, der eksporteres til markedspris, er stigende.

Konklusion: på baggrund af feedback fra retshåndhævende myndigheder og finansielle efterretningsenheder anses trusselsniveauet for hvidvask af penge og for meget betydeligt (niveau 4).

Sårbarhed

Finansiering af terrorisme

Vurderingen af sårbarhed over for finansiering af terrorisme i relation til pengesedler med høj pålydende værdi viser følgende karakteristika:

a) risikoeksponering

Kontantbetalinger muliggør hurtige og anonyme transaktioner. Niveauet for risikoeksponering er meget højt, idet store summer også kan flyttes over grænser og kan omfatte højrisikokunder og/eller geografiske områder med høj risiko.

b) risikobevidsthed

Især har de retshåndhævende myndigheder og finansielle efterretningsenheder en høj risikobevidsthed, og det samme har de forpligtede enheder, der er omfattet af forpligtelserne vedrørende bekæmpelse af hvidvask af penge og af finansiering af terrorisme. Risikobevidstheden hos de sektorer, der ikke er omfattet af forpligtelser vedrørende bekæmpelse af hvidvask af penge og af finansiering af terrorisme eller begrænsningsforpligtelser mht. kontanter, er fortsat en udfordring. Den foreliggende litteratur, navnlig en Europol-rapport, peger på den blinde plet i risikobevidstheden (dvs. den præcise brug af pengesedler med høj pålydende værdi, forskellen mellem medlemsstaterne vedrørende udstedelse, frakobling fra bruttonationalproduktet). Der findes ingen eller næsten ingen pålidelige oplysninger om omfanget af almindelige borgeres brug af kontanter, endsige kriminelles.

c) retsgrundlag og eksisterende kontroller

Begrænsninger af kontantbetalinger kan gøre det muligt at reducere sårbarheden, men de eksisterende retlige rammer vedrørende begrænsninger af kontantbetalinger kan variere meget fra den ene medlemsstat til den anden, og dermed kan kontroller potentielt være ikke-eksisterende. Set i forhold til det indre marked øger forskellene mellem medlemsstaternes lovgivninger om kontantbegrænsninger det indre markeds sårbarhed. Lovovertræderne kan lettere omgå kontrollen i deres oprindelsesland ved at investere i kontantintensiv virksomhed i en anden medlemsstat, der har mindre/ingen kontrol med hensyn til kontantbegrænsning.

Det fjerde hvidvaskdirektiv foreskriver, at forhandlere af meget værdifulde varer, der modtager betaling i kontanter ud over 10 000 EUR , er omfattet af reglerne om bekæmpelse af hvidvask af penge og af finansiering af terrorisme og skal gennemføre kundekendskabskrav. Denne forpligtelse gælder for enhver, der handler med varer, når betalingen sker kontant ud over 10 000 EUR, men den omfatter ikke tjenesteydelser, bortset fra spiltjenester, og i så fald, når der foretages transaktioner, der beløber sig til 2 000 EUR. Denne tærskel følges i direktiv 2018/843 (det femte hvidvaskdirektiv).

Men effektiviteten af disse foranstaltninger er stadig begrænset i betragtning af antallet af indberetninger af mistænkelige transaktioner. af indberetninger af mistænkelige transaktioner er generelt lavt, fordi kontanttransaktioner er vanskelige at opfange, der kun lidt tilgængelig information, og forhandlere kan miste deres kunder til konkurrenter med mere lempelige kontroller. De medlemsstater, der har indført pengetransaktionsrapporter, er for det meste ikke tilsluttet nogen indberetninger af mistænkelige transaktioner, og så kan analysen ikke udføres (f.eks.vil store beløb, der hæves i en pengeautomat, udløse en pengetransaktionsrapport, men der er ingen konkret mistanke, og den finansielle efterretningsenhed kan ikke iværksætte nogen undersøgelser).

Desuden kan det være vanskeligt for en forhandler af meget værdifulde varer at udforme retningslinjer for bekæmpelse af hvidvask af penge og af finansiering af terrorisme i det begrænsede antal tilfælde, hvor en kontanttransaktion over tærsklen finder sted (dvs. det er ikke sektoren i sig selv, der er dækket af ordningen for bekæmpelse af hvidvask af penge og af finansiering af terrorisme – men kun forhandlere af meget værdifulde varer i forbindelse med kontanttransaktioner over en tærskel). Af denne grund har nogle medlemsstater udvidet anvendelsesområdet med bestemte sektorer, uanset om der bruges kontanter. Nogle medlemsstater har også besluttet at anvende en generel ordning med kontantbegrænsning på denne tærskel for at mindske risikoen for, at forhandlere af varer af høj værdi anvender kundekendskabskravene på en ineffektiv eller besværlig måde. Dette begrænser dog ikke risikoen mht. de situationer, hvor der er tale om kontantintensiv virksomhed, der baserer sig på kontanttransaktioner med mindre beløb – eller et gentaget antal kontanttransaktioner med små beløb.

Under alle omstændigheder mener nogle kompetente myndigheder, at selv når der findes begrænsninger af kontante betalinger, er håndhævelsen af disse begrænsninger en stor udfordring og kan begrænse deres indvirkning på terrorfinansieringsaktiviteter.

Konklusion: i betragtning af, at kontantbetalinger at foretage store transaktioner, herunder grænseoverskridende, hurtigt og anonymt, at alle sektorer potentielt kan komme ud for kontantbetalinger, og som, selvom de er bevidste om, at disse betalinger kan indebære risici, ikke er rustet til at imødegå dem (enten fordi der ikke eksistere nogen ramme/kontrol, eller fordi håndhævelsen af kontrollerne ikke er effektiv), anses sårbarhedsniveauet for terrorfinansiering i relation til kontant betaling for meget betydeligt (niveau 4).

Hvidvask af penge

Vurderingen af sårbarheden over for hvidvask af penge i relation til kontantbetalinger viser følgende karakteristika:

a) risikoeksponering

Sektoren udviser den samme sårbarhed over for terrorfinansiering som over for hvidvask af penge. Ligesom mht. terrorfinansiering muliggør kontantbetalinger hurtige og anonyme transaktioner med henblik på hvidvask af udbyttet af kriminalitet vedrørende hvidvask. Niveauet for risikoeksponering er meget højt, idet store summer også kan flyttes over grænser og kan omfatte højrisikokunder og/eller geografiske områder med høj risiko.

b) risikobevidsthed

Især har de retshåndhævende myndigheder og finansielle efterretningsenheder en høj risikobevidsthed, det samme har de forpligtede enheder, der er omfattet af forpligtelserne vedrørende bekæmpelse af hvidvask af penge og af finansiering af terrorisme. Risikobevidstheden hos de sektorer, der ikke er omfattet af forpligtelser vedrørende bekæmpelse af hvidvask af penge og af finansiering af terrorisme eller begrænsningsforpligtelser mht. kontanter, er fortsat en udfordring. Den foreliggende litteratur, navnlig Europol-rapporten, peger på den blinde plet i risikobevidstheden (dvs. den præcise brug af pengesedler med høj pålydende værdi, forskellen mellem

medlemsstaterne vedrørende udstedelse, frakobling fra bruttonationalproduktet). Der findes ingen eller næsten ingen pålidelige oplysninger om omfanget af almindelige borgeres brug af kontanter, endsige kriminelles.

c) retsgrundlag og eksisterende kontroller

Begrænsninger af kontantbetalinger kan gøre det muligt at reducere graden af sårbarhed, men de eksisterende retlige rammer vedrørende begrænsninger af kontantbetalinger kan variere meget fra den ene medlemsstat til den anden, og dermed kan kontroller potentielt være ikke-eksisterende. Set i forhold til det indre marked øger forskellene i medlemsstaternes lovgivninger om kontantbegrænsninger det indre markeds sårbarhed; lovovertræderne kan lettere omgå kontrollen i deres oprindelsesland ved at investere i kontantintensiv virksomhed i en anden medlemsstat, der har mindre/ingen kontrol med hensyn til kontantbegrænsning.

Omfanget af rapporteringet er meget lille, idet kontanttransaktioner er svære at opdage. De medlemsstater, der har indført pengetransaktionsrapporter, er for det meste ikke tilsluttet nogen indberetninger af mistænkelige transaktioner, og så kan analysen ikke udføres (f.eks.vil store beløb, der hæves i en pengeautomat, udløse en pengetransaktionsrapport, men der er ingen konkret mistanke knyttet til den pågældende, og den finansielle efterretningsenhed kan ikke udløse nogen undersøgelser).

Under alle omstændigheder mener nogle kompetente myndigheder, at selv når der findes begrænsninger af kontante betalinger, er håndhævelsen af disse begrænsninger virkelig en udfordring og kan begrænse deres indvirkning på terrorfinansieringsaktiviteter.

Konklusion: i betragtning af, at kontantbetalinger gør det muligt at foretage store transaktioner, herunder grænseoverskridende, hurtigt og anonymt at alle sektorer potentielt kan komme ud for kontantbetalinger, og som, selvom de er bevidste om, at disse betalinger kan indebære risici, ikke er rustet til at imødegå dem (enten fordi der ikke eksistere nogen ramme/kontrol, eller fordi håndhævelsen af kontrollerne ikke er effektiv), anses sårbarhedsniveauet over for terrorfinansiering i relation til kontant betaling meget betydeligt (niveau 4).

Risikobegrænsende foranstaltninger:

- Kommissionen vil fortsat overvåge forhandleres anvendelse af forpligtelserne til bekæmpelse af hvidvask af penge og af finansiering af terrorisme med hensyn til varer, der er omfattet af direktivet om bekæmpelse af hvidvask af penge, og vurdere de risici, der er forbundet med de udbydere af tjenesteydelser, der accepterer kontante betalinger. Den vil desuden vurdere nytteværdien og fordelene for at lade yderligere sektorer blive omfattet af regler om bekæmpelse af hvidvask af penge og af finansiering af terrorisme.

- Medlemsstaterne bør i deres nationale risikovurderinger tage risiciene ved kontantbetalinger i betragtning med henblik på at fastlægge passende risikobegrænsende foranstaltninger. Medlemsstaterne bør overveje at lade sektorer, der i særlig grad er udsat for risici for hvidvask af penge og terrorfinansiering, blive omfattet af de forebyggende ordninger vedrørende bekæmpelse af hvidvask af penge og af finansiering af terrorisme på grundlag af deres nationale tilsynsmyndigheders resultater.

5. Privatejede pengeautomater

Produkt
Privatejede pengeautomater

Sektor
/

Generel beskrivelse af den pågældende sektor og det/den relevante produkt/aktivitet

De retshåndhævende myndigheder er blevet gjort opmærksom på et muligt misbrug af pengeautomater til hvidvask af penge. Ifølge de modtagne oplysninger skaber privates mulighed for lovligt at købe og leje pengeautomater hos engrosleverandører et smuthul, som kriminelle drager fordel af.

For mange forretningsdrivende, ejere af diskoteker, barer samt restauranter har installationen af en af disse pengeautomater vist sig at være en god beslutning forretningsmæssigt – kunden tilbydes den bekvemmelighed at hæve kontanter, og den forretningsdrivende maksimerer sandsynligheden for at nogle af disse kontanter vil blive brugt i vedkommendes forretning.

Beskrivelse af risikoscenariet

A) Mulighederne mht. opfyldning af pengeautomater

Med hensyn til opfyldning af maskinen er en af mulighederne at benytte sig af en værdihåndterings-/kontantleveringsvirksomheds tjenesteydelser.

En anden mulighed for den forretningsdrivende, der driver en virksomhed, er at fylde op med kontanter fra kassen. Dette giver yderligere muligheder for den erhvervsdrivende for at begå skattesvig ved at sælge varer i bytte for penge uden at udstede kvitteringer. De placerer simpelthen deres sorte penge i deres pengeautomat og venter på, at pengene bliver hævet af almindelige kunder. Ved udgangen af året bliver disse salg aldrig opgivet til de erhvervsdrivendes skattemyndigheder

Den tredje og mest foruroligende mulighed er simpelthen at fylde pengeautomaten op med kriminelle kontanter. Indsamlede efterretningsoplysninger viser, at i sager, hvor kriminelle kontanter bruges, er fremgangsmåden følgende: en kurer leverer kriminelle kontanter til automatejeren/den forretningsdrivende. De kan stamme fra forskellige kontantgenererende aktiviteter som narkotikahandel, illegal migration, menneskehandel, udnyttelse af arbejdskraft og seksuel udnyttelse, salg eller forfalskning af smuglervarer, tyveri, røveri mv. De kriminelle kontanter fyldes derefter i maskinen. Når intetanende kunder eller forbipasserende, der har brug for kontanter, bruger deres kort til at hæve kontanter, bliver det samme beløb debiteret fra deres bankkonti og krediteret på kontoen tilhørende ejeren af pengeautomaten/den forretningsdrivende. Efterfølgende kan vedkommende simpelthen overføre pengene til en given konto, der er kontrolleret af den kriminelle, med fradrag af den aftalte provision.

b) Risici i forbindelse med afkobling af bankkonti og internationalisering

Et internationalt, potentielt langt farligere risikosenarie tegner sig, når nationale bestemmelser kræver, at en privat virksomhed, der køber en pengeautomat, ved købet skal oplyse et nationalt bankkontonummer, som er forbundet med pengeautomaten og dens aktiviteter, men der ikke er noget krav om, at den forretningsdrivende skal anmode om penge til pengeautomaten fra den samme bankkonto, som vedkommende knyttede til sin pengeautomat, eller ikke engang fra samme bank.

En gennemgang af de virksomheder, der tilbyder private pengeautomattjenester viser, at der findes flere store udbydere, britiske og amerikanske,[31] som har formået at gøre deres virksomhed international.[32]

Der rejser sig vigtige spørgsmål vedrørende de konti, som er knyttet til disse pengeautomater (solgt af virksomheder i EU og USA og placeret i EU-lande). Hvis de er knyttet til en bankkonto i et EU-land, men fysisk befinder sig i et andet land, så er det stort set umuligt at fastslå oprindelsen af de kontanter, der indsættes på dem.

c) Skatteunddragelse og -svig

Private pengeautomater bliver også brugt til skatteunddragelse og -svig, især fordi nogle kontantintensive forretningsdrivende opfordrer deres kunder til at hæve penge til ydelser, der ikke bliver faktureret eller registreret. Størrelsen af beløb mistet i skatteindtægter på grund af skatteunddragelse og -svig gennem private pengeautomater er større end det beløb, der bliver hvidvasket.

d) Mikrostrukturering gennemført af organiserede kriminelle

Med hensyn til hvidvask af penge bruges private pengeautomater ofte til at "mikrostrukturere", dvs. indsætte og hæve små pengesummer, som svarer til de beløb, der normalt hæves i pengeautomater, så de ikke opdages ved bankkontroller. Organiserede kriminelle vil foretage en masse små daglige kontante indskud på 100 eller flere bankkonti via private pengeautomater for at undgå aktivering af rapporteringskrav i forhold til bekæmpelse af hvidvask.

Generel bemærkning

Private pengeautomater vil ofte være placeret i kontantintensive virksomheder. Derudover findes privatejede pengeautomater også i pengeservicevirksomheder. I betragtning af, at

[31] For eksempel: YourCash Europa – en virksomhed, der kontrollerer 32% af markedet for frit tilgængelige pengeautomater i Det Forenede Kongerige – har filialer i Nederlandene, Belgien og Irland samt pengeautomater i andre lande. Derudover opererer Cardtronics (nogle afdelinger arbejder under varemærket DC Payments) i 11 lande. Ud over de nævnte filialer uden for Europa (Syd- og Nordamerika, Australien, New Zealand og Sydafrika) og afdelingen i Storbritannien, driver selskabet virksomhed i Irland, Tyskland, Polen og Spanien.

[32] Som et yderligere eksempel det afsnit, der viser pengeautomaters placering på webstedet LINK: (https://www.link.co.uk/consumers/locator/) viser, at der findes privatejede UK pengeautomater, der er fysisk placeret i Belgien, Tjekkiet, Frankrig, Tyskland, Gibraltar, Grækenland, Nederlandene, Irland og Schweiz samt Guernsey, Isle of Man og Jersey.

det er ulogisk at placere en pengeautomat i en pengeservicevirksomhed, på grund af pengeservicevirksomhedens karakter, og at mange hawaladares[33] lovlige bivirksomhed er at drive en pengeservicevirksomhed eller et vekselkontor, ses risikoen for misbrug tydeligt.

Trussel

Finansiering af terrorisme

Der findes for tiden kun få konkrete vurderinger af truslen om terrorfinansiering i relation til privatejede pengeautomater. Ikke desto mindre viser både vurderingen af kontantbetalinger og analysen af pengekurerfirmaer, at denne fremgangsmåde er let tilgængelig og har beskedne omkostninger.

Der kan også bestå en trussel om transport af likvide midler ind i EU fra tredjelande, især fra lande udsat for risici for terrorfinansiering eller fra konfliktområder. Der er konstateret tilfælde af beskedne beløb, der omfatter integration af kontanter, som medbringes fra tredjelande, ind i det finansielle system/den legale økonomi i EU (analyseret i et særskilt afsnit i denne rapport).

Konklusion: på baggrund af feedback fra retshåndhævende myndigheder og finansielle efterretningsenheder anses trusselsniveauet for terrorfinansiering for meget betydeligt (niveau 4).

Hvidvask af penge

Vurderingen af truslen om hvidvask af penge i relation til privatejede pengeautomater viser, at denne fremgangsmåde bliver udnyttet af kriminelle, da den udgør en realistisk mulighed, som er ganske attraktiv og sikker. Den udgør en let måde, hvorpå man kan undgå skat og skjule ulovligt udbytte af kriminalitet. Men ligesom for terrorfinansiering kræver det et moderat niveau af kvalifikationer at kunne drive virksomheden og at undgå at blive afsløret.

Konklusion: på baggrund af feedback fra retshåndhævende myndigheder og finansielle efterretningsenheder anses trusselsniveauet for hvidvask af penge for meget betydeligt (niveau 4).

Sårbarhed

Finansiering af terrorisme

Vurderingen af sårbarheden over for terrorfinansiering i relation til privatejede pengeautomater viser, at de væsentligste faktorer er knyttet til risikoen ved kontanter.

a) risikoeksponering

Sårbarhedsvurderingen vedrørende terrorfinansiering i relation til privatejede pengeautomater er snævert forbundet med vurderingen i relation til brugen af/betalinger med kontanter generelt og kan følge det samme rationale. Privatejede pengeautomater gør det muligt at behandle et stort antal anonyme transaktioner, hvilket kun kræver en investering i starten. Følgelig er den iboende risikoeksponering høj.

[33] Se afsnittet om "Hawala".

b) risikobevidsthed
Risikobevidstheden synes at være temmelig lav.

c) retsgrundlag og eksisterende kontroller
De eksisterende retlige rammer vedrørende varierer meget fra den ene medlemsstat til den anden, og dermed kan kontroller potentielt være ikke-eksisterende.

<u>Konklusion:</u> sårbarheden i forhold til privatejede pengeautomater er nøje forbundet med sårbarhederne i relation til brugen af kontanter i almindelighed.
På baggrund af en udbredt brug af kontanter i EU's økonomier, og at sektoren ikke synes at være bevidst om denne risiko, hvorfor sårbarheden i forhold til terrorfinansiering anses som meget betydelig (niveau 4).

Risikobegrænsende foranstaltninger:

Virksomheder, der udbyder private pengeautomater, udgør en øget risiko for banker og bør behandles som højrisikovirksomhed i forbindelse med risikovurderinger mht. overholdelse af regler om hvidvask. Risiciene for bankerne er ikke blot økonomiske, men angår også deres renommé.

- For det første bør kunder, der har privat ejede eller drevne pengeautomater, være behørigt identificeret.

- Når banken har identificeret en ejer eller operatør af pengeautomater, bør den indhente yderligere oplysninger med henblik på at få indblik i automatejerens/-operatørens forhold samt indblik i automatejerens procedurer.

- Efter at der er indhentet tilstrækkelige oplysninger, bør den sponsorerende bank gennemføre en procedure til systematisk overvågning af ejerne af pengeautomaterne. De oplysninger, der er indhentet i forbindelse med kundekendskabsproceduren, burde gøre det muligt for banken at fastlægge omfanget og hyppigheden af den nødvendige overvågning, samt hvor ofte.

- Medlemsstaterne bør sikre pligten til at lade sig registrere, begrænse retten til at eje, overvåge eller undersøge privatejede pengeautomater – til og med forpligtelsen til at knytte pengeautomaterne til en bankkonto i den medlemsstat, hvor de er placeret fysisk.

1. Indskud på konti

Produkt
Indskud på konti

Sektor
Kredit- og finansielle institutioner

Generel beskrivelse af den pågældende sektor og det/den relevante produkt/aktivitet

Tendenserne er ifølge oplysninger fra European Banking Federation, at indenlandske eller euroområdets indlån i EU siden 1998 er steget med 3,1 % til 23,6 billioner EUR i december 2017 (17,5 billioner EUR i euroområdet og 5,3 billioner EUR i de øvrige EU-medlemsstater). Det var det højeste registrerede niveau, hvor det tidligere højeste niveau på 23,1 billioner EUR var i 2012. Indskud fra andre monetære finansielle institutioner steg for første gang siden 2011 til 7,1 billion EUR.

Det samlede indlån fra ikke-monetære finansielle institutioner med undtagelse af centralregeringer steg med 2,5 %. i 2017 til 16,3 billioner EUR i EU ved udgangen af 2017, hvoraf 12,1 billioner EUR blev indsat i euroområdet.

Væksten har været drevet af en stigning i indlån fra husholdninger, der steg med 2,9 procent i forhold til året før til 9,1 billioner EUR, og fra ikkefinansielle selskaber, med 6,7 % til 3,2 billioner EUR.

Beskrivelse af risikoscenariet

Lovovertrædere placerer udbyttet af kriminalitet i det finansielle system gennem den organiserede kredit- og finanssektor med henblik på at skjule udbyttets ulovlige oprindelse. Terrorister, støtter eller formidlere placerer midler fra lovlige eller kriminelle kilder i det finansielle system med henblik på at bruge det til terrorformål.

Pengekurermekanismer kan bruges til at føre udbytte ud af banksektoren gennem brug af personlige konti, enten gennem cyberkriminalitet (bedrageri, falske bankwebsteder mv.) eller gennem penge- eller værdioverførselstjenester.

"Brokonti" bliver også brugt til at hvidvaske penge. Der er tale om konti tilhørende juridiske eller fysiske personer i EU, der alene har det formål at overføre midler til lande uden for EU.

Trussel

Finansiering af terrorisme

Vurderingen af truslen om terrorfinansiering i relation til kontoindskud viser, at dette risikoscenarie både vedrører indsættelse og hævning af midler (dvs. kontoindsættelser og brug af denne konto til at hæve disse midler eller overføre dem til andre bankkonti).

Indskud på konti bruges er hyppigt af terrorister, men også af slægtninge/venner; dette udvider anvendelsesområdet for hensigts- og kapacitetsanalysen.[34] Desuden har de retshåndhævende myndigheder rapporteret om terroristers brug af forfalskede eller stjålne dokumenter til at åbne bankkonti. Ifølge oplysninger fra kompetente myndigheder hæver udenlandske terrorkrigere i almindelighed indeståender på bankkonti via pengeautomater placeret i højrisikolande uden for EU eller konfliktområder generelt eller i nabolande. Terrorister uden for konfliktområder hæver også midler via pengeautomater for at betale nogle af de udgifter, der er forbundet med deres aktiviteter, kontant. Imidlertid kan brugen af indlånskonti til terrorfinansiering i konfliktområder være kompliceret af vanskeligheder med at få adgang til midlerne, især hvor adgangen til pengeautomater eller et fungerende banksystem er afbrudt. Kilden til de midler indestående på bankkonti kan være af både legitim og ikke-legitim oprindelse.

Generelt er brug af indlånskonti lettilgængelig, især når der anvendes lovlige midler, og de udløser derfor ingen mistanke, når bankkontoen åbnes. Det ser ud til, at terrorgrupper ikke oplever særlige udfordringer i forbindelse med at skjule den reelle modtager af midlerne eller det præcise formål med transaktionen (midlernes bestemmelsessted), idet de blot kan lade familiemedlemmer eller slægtninge indgå i ejerkæden. Dette kræver i det mindste basal planlægning og basal viden om, hvordan banksystemerne fungerer. Når det er sat i værk, muliggør kontanthævninger samtidig grænseoverskridende bevægelser, hvilket gør dette risikoscenarie ganske attraktivt.

Konklusion: Terrorgrupper bruger temmelig ofte indskud på konti til på en let måde at anbringe kontanter på bankkonti og hæve penge til terroraktiviteter, selvom det kræver en vis grundlæggende viden og planlægningskapacitet at sikre, at indsatte midler fremstår lovlige. Som følge heraf er denne metode temmelig attraktiv for terrorgrupper. Herefter anses niveauet for truslen om terrorfinansiering i relation til indskud på konti som betydeligt/meget betydeligt (niveau 3/4).

[34] Hensigts- og kapacitetsanalysen er beskrevet i metodebeskrivelsen:

- *"Hensigtskomponenten"* af truslen afhænger af kendt hensigt (konkret forekomst af truslen) succesfuld eller forpurret, og hvor attraktiv terrorfinansiering gennem en bestemt metode/mekanisme anses for at være. Mens den bredere hensigt om at finansiere terror vurderes til at være konstant høj, afhænger hensigten om at anvende bestemte fremgangsmåder/metoder af, hvor attraktiv fremgangsmåden anses for at være, og af den kendte eksistens af sikkerhedsforanstaltninger vedrørende bekæmpelse af terrorfinansiering.
- Ved *"kapacitetskomponenten"* af truslen forstås kapaciteten hos trusselsgrupper (terrorister) til at faktisk at overføre ulovlige eller lovlige midler med henblik på finansielt at opretholde et terrornetværk.

  Vurderingen af kapacitetskomponenten vil se på, hvor let det er at anvende en bestemt fremgangsmåde til terrorfinansiering (nødvendige tekniske kvalifikationer og understøttelse), tilgængeligheden og de relative omkostninger (økonomisk kapacitet), der er forbundet med at anvende en bestemt fremgangsmåde.

Hvidvask af penge

Vurderingen af truslen om hvidvask af penge i relation til kontoindskud viser, at dette risikoscenarie både vedrører indsættelse og hævning af midler (dvs. indsættelser på en konto og efterfølgende brug af denne konto, hæve penge fra den pågældende konto eller overføre penge for at tilsløre midlernes oprindelse).

Indsættelse på konti bruges hyppigt af organiserede forbryderorganisationer, men også af slægtninge/nære forretningspartnere, hvilket udvider anvendelsesområdet for hensigts- og kapacitetsanalysen.[35] Retshåndhævende myndigheder rapporterer om hyppig brug af denne metode, da det er en af de letteste måder til at indføre ulovlige midler i det finansielle system. Når der er tale om små pengebeløb, er dybtgående planlægning og kendskab til, hvordan banksystemerne virker, måske ikke nødvendig, men i tilfælde af kompleks hvidvask, som involverer penge på konti, der bevæger sig via en kæde af komplekse operationer, er mere dybtgående viden nødvendig, og lovovertræderne kan eventuelt benytte sagkundskab, der kan fås hos mellemmænd.

Konklusion: På baggrund af ovenstående trusler, særlig kriminelle organisationers anvendelse, anses truslen om hvidvask i relation til indskud på konti som meget betydelig (niveau 4).

Sårbarhed

Finansiering af terrorisme

Ved vurderingen af sårbarheden over for terrorfinansiering i relation til indlån på konti sås på indsættelsen og hævningen af midler.

a) risikoeksponering

Banker er fortsat udsat for terrorfinansieringsrisici, idet indskud på konti udgør den letteste måde til at bringe penge ind i det finansielle system. For så vidt angår risikoen fra terrorfinansiering er risikoeksponeringen endda højere, når midlernes oprindelse er lovlig. Brugen af midler på indlånskonti til terrorformål er vanskeligt at opdage, da terrorgrupper normalt bruger små pengebeløb. Med hensyn til at sende penge til konfliktområder er risikoen for terrorfinansiering mindre med indskud på konti, idet lovovertræderne foretrækker andre produkter som penge- eller værdioverførselstjenester eller e-pengeprodukter.

b) risikobevidsthed

Risikobevidstheden hos kredit- og finansieringsinstitutter er generelt god, og banksektoren har indført vejledning i at opdage de relevante advarselssignaler om terrorfinansiering. De systemer og kontroller, virksomhederne har indført for at begrænse risikoen for terrorfinansiering, ligner imidlertid og er ofte de samme som de kontroller, der er indført til bekæmpelse af hvidvask af penge. Tilsynsmyndigheder og retshåndhævende

[35] Se forrige fodnote.

myndigheder er opmærksomme på sårbarheder over for terrorfinansiering og er proaktivt i kontakt med sektoren.

c) retsgrundlag og kontroller

Indskud på konti har været omfattet af reglerne om bekæmpelse af hvidvask af penge og bekæmpelse af finansiering af terrorisme siden den første lovgivning herom på EU-plan i 1991. De eksisterende kontroller anses generelt for at være effektive, selvom sanktionsscreening ikke er en erstatning for effektive kontroller i forbindelse med bekæmpelsen af finansiering af terrorisme. Økonomiske sanktioner rettes mod enkeltpersoner eller grupper, som man allerede ved, udgør en trussel, men risikoen fra terrorfinansiering udgår ofte fra personer, som ikke bliver opfanget af sanktionssystemet. Derfor er risikobaserede kontroller i forbindelse med bekæmpelse af hvidvask af penge og af terrorfinansiering samt især transaktionsovervågning nøglen til en effektiv bekæmpelse af terrorfinansiering.

Sædvanligvis har bankerne ikke adgang til relevante oplysninger, der ville kunne hjælpe dem med at identificere risici for terrorfinansiering, før de bliver til noget, idet det ofte er de retshåndhævende myndigheder, der ligger inde med disse oplysninger. Tilsvarende kan de retshåndhævende myndigheders bestræbelser på at forpurre terroristernes aktiviteter og net blive vanskeliggjort, hvis de ikke er i stand til at indhente oplysninger om finansielle strømme, som kun virksomheder kan give. Der pågår for tiden initiativer på nationalt og supranationalt niveau med henblik på at finde ud af, hvordan retshåndhævende myndigheder kan give virksomhederne mere konkrete og væsentlige oplysninger om konkrete personer af interesse, som kan give virksomhederne mulighed for at fokusere deres transaktionsovervågning på disse personer.

Konklusion: risikoeksponeringen kan betragtes som ret høj, og sektoren har behov for, trods et pænt niveau af risikobevidsthed, at forbedre effektiviteten af kontrollerne med henblik på at begrænse risikoen for terrorfinansiering. Samarbejde med retshåndhævende myndigheder er afgørende på dette område. Som følge heraf anses niveauet for sårbarhed over for terrorfinansiering i relation til indskud på konti som betydeligt (niveau 3).

Hvidvask af penge

Sårbarheden over for hvidvask afhænger hovedsagelig af overvågningssystemernes effektivitet til at opdage mistænkelige transaktioner, når kontanter går ind på bankkonti eller transaktioner forbundet med kontanter. Sårbarheden er også stor i forbindelse med overførsler af midler fra højrisikokunder.

a) risikoeksponering

Indskud på konti udgør den enkleste måde, hvorpå man kan føre penge fra ulovlige aktiviteter ind i det finansielle system. Der er store mængder af produkter, hvor oprindelsen af midler ikke altid kan spores for så vidt angår kontanter. Indlånsforretninger er en temmelig almindelig praksis for kredit- og finansielle institutioner, og de udgør et stort antal transaktioner, der kan implicere flere forskellige slags kunder. Nogle kunder kan være

i højrisikokategorien, fordi de er politisk eksponerede, eller fordi de er identificeret som højrisiko-kunder (dvs. nogle udlandskonti i EU-banker).

Den udbredte brug af kontanter i nogle undersektorer og i nogle medlemsstater anses af de fleste tilsynsmyndigheder for at være en af de medvirkende faktorer, der gør sektoren sårbar over for hvidvask, navnlig hvor sektoren består af mange detailbanker. Tilsynsmyndighederne anser også grænseoverskridende aktiviteter for udsat for en betydelig og meget betydelig risiko for hvidvask af penge, navnlig i de medlemsstater, der er kendt som internationale finanscentre. Udenlandske kunder fra højrisiko-lande og off-shore virksomheder bidrager også til den forhøjede iboende risiko i denne sektor. I nogle medlemsstater, hvor den indenlandske indskudsbase er lille i forhold til størrelsen af den finansielle sektor, er udenlandske indskud navnlig fra tilgrænsende ikke-EU-lande en attraktiv finansieringskilde. Men de senere års erfaringer har vist, at sådanne indskud, afhængig af oprindelseslandet og andre omstændigheder, ofte krævede forstærkede hvidvask-kontroller, som ikke eksisterede eller ikke stod i et rimeligt forhold til det risikoniveau, de udgjorde. Det forhold, at kreditinstitutter tog for store risici, resulterede i, at EU-landene i betydelig grad blev udsat for strømmen af midler med potentielt mistænkelig oprindelse fra tredjelande. En nyere tendens er et støt fald i andelen af udlandskonti i EU-lande – både på grund af banksektorens frivillige nedbringelse af risikoen samt reglerne i de berørte EU-lande.

b) risikobevidsthed

Risikobevidstheden er generelt god, da sektoren har indført vejledning i at afsløre de relevante advarselssignaler om terrorfinansiering. Banksektoren er generelt set i høj grad udsat for risici mht. hvidvask af penge, men den har også de fornødne værktøjer til at opdage dem. Dette bekræftes af høje rapporteringsniveauer. Finansielle efterretningsenheder og retshåndhævende myndigheder er også bevidst om sektorens sårbarheder og er proaktivt i kontakt med dem.

Banksektoren betragtes generelt som risikabel, idet kreditinstitutter ofte er det første indgangspunkt til den samlede finansielle servicesektor, men for tilsynsmyndighederne er koncentrationen af virksomheder, der vurderes at indebære en meget betydelig risiko, relativt lille. Imidlertid har skandaler i europæiske banker i de seneste år vist, at svagheder knyttet til kunder fra tidligere sovjetrepublikker øger sårbarheden over for hvidvask af penge.

c) retsgrundlag og kontroller

Indskud på konti har været omfattet af reglerne om bekæmpelse af hvidvask af penge og bekæmpelse af finansiering af terrorisme siden den første lovgivning herom på EU-plan i 1991. Eksisterende kontroller betragtes som effektive, men det kan være nødvendigt at udføre tematiske tilsyn for at kontrollere effektiviteten af de overvågningssystemer, der bruges til at afsløre mistænkelige pengetransaktioner, især når juridiske enheder og juridiske arrangementer er involveret. Tilsynsmyndighederne er også betænkelige mht. kreditinstitutternes kontroller med henblik på styre de risici, der er forbundet med kunder med komplekse offshore konstruktioner. Navnlig anses de kontroller, der iværksættes for at identificere og verificere de egentlige ejere, for ikke at være tilstrækkelig grundige.

Konklusion: kreditinstitutterne har i passende grad begrænset den iboende risiko for hvidvask af penge i forbindelse med indskud. Der er dog stadig visse betænkeligheder med hensyn til kontrollernes effektivitet, især mht. kunder med komplekse offshorekonstruktioner og udenlandske kunder fra højrisikolande. I denne henseende anses sårbarheden over for hvidvask af penge i relation til indskud på konti/detailbankforretning for betydelig (niveau 3).

Risikobegrænsende foranstaltninger:

Kommissionen:

- en grundig kontrol af gennemførelsen af det femte direktiv om bekæmpelse af hvidvask af penge med fokus på bestemmelserne vedrørende information om reelt ejerskab), herunder sammenkobling af registre over reelle ejere på EU-niveau

- ensartet praksis inden for e-identifikation for den finansielle sektor og indførelse af standarder for at opfylde kundekendskabskrav med Reg-Tech-virksomheder

- fremme samarbejdet mellem retshåndhævende myndigheder og finansielle institutioner med henblik på at øge effektiviteten af alarmsystemer for terrorfinansiering på supranationalt niveau.

Medlemsstater / kompetente myndigheder:

· offentligt-privat samarbejde om udveksling af oplysninger vedrørende terrorfinansiering

· tematiske inspektioner med fokus på:

  - vurdering af effektiviteten af systemer til overvågning af kontanttransaktioner og anbringelse af midler på bankkonti med tilknytning til samtidig overførsel af midler til højrisikolande uden for EU

  - effektiviteten af kundekendskabskrav og udvidede kundekendskabskrav for juridiske enheder, og juridiske arrangementer.

2. Den institutionelle Investeringssektor – bankvirksomhed

Produkt
Indskud på konti

Sektor
Kreditinstitutter – institutionel investering

Generel beskrivelse af den pågældende sektor og det/den relevante produkt/aktivitet

Sektoren for porteføjleadministration i EU er sammensat af to komplementære søjler. Den første søjle omfatter branchen for investeringsforeninger, de såkaldte "UCITS"-fonde (forvalter aktiver for 9,7 billioner EUR i 2017). Den anden søjle omfatter alternative investeringsfonde (branchen for alternative investeringsfonde havde en nettoværdi af 4,9 billioner EUR ved udgangen af 2017), f.eks. hedgefonde (11 %), private equity (4 %), funds of funds (16 %) og ejendomsfonde (11 %). Porteføljer forvaltet i EU passerede 15 billioner EUR-tærskelen ved udgangen af 2017. Branchen for porteføjleadministration i EU betjener både detailkunder – normalt bestående af husholdninger og formuende enkeltpersoner — og institutionelle kunder. Institutionelle kunder omfatter f.eks. forsikringsselskaber og pensionskasser, som tegnede sig for hhv. 25 % og 28 % af den samlede formue under forvaltning i EU ved udgangen af 2016.

Beskrivelse af risikoscenariet

Der er flere scenarier, hvor lovovertrædere kan misbruge investorer og finansielle markeder, f.eks. gennem integration af udbyttet ved adkomst til aktier for at skjule det reelle ejerforhold. Gennem svig eller gennem markedsmisbrug (der omfatter insiderhandel, kursmanipulation og ulovlig videregivelse af intern viden, som alle er omfattet af EU's forordning om markedsmisbrug[36] og EU's direktiv om strafferetlige sanktioner for markedsmisbrug[37]), mæglerkonti, investeringer for at legitimere kriminelle udbytter som overskud, underliggende investeringssvig eller placering af provenu hos specialiserede finansielle tjenester, der giver højt afkast.

Generel bemærkning

Dette risikoscenarie kan ses som knyttet til scenariet for investering, som foretages af mæglere. Det er blevet antaget, at for så vidt angår sårbarheden over for hvidvask er risikoniveauet højere for mæglere.

[36] Europa-Parlamentets og Rådets forordning (EU) nr. 596/2014 af 16. april 2014 om markedsmisbrug (forordningen om markedsmisbrug) og om ophævelse af Europa-Parlamentets og Rådets direktiv 2003/6/EF og Kommissionens direktiv 2003/124/EF, 2003/125/EF og 2004/72/EF EØS-relevant tekst, EUT L 173 af 12.6.2014, s. 1.
[37] Europa-Parlamentets og Rådets direktiv 2014/57/EU af 16. april 2014 om strafferetlige sanktioner for markedsmisbrug (direktivet om markedsmisbrug) EUT L 173 af 12.6.2014, s. 179.

Trussel

Finansiering af terrorisme

Truslen om terrorfinansiering i relation til institutionelle investorer kan være betydelig, hvis store mængder lovlige midler investeres for at finansiere terrorisme, men når der er tale om at fremskaffe småbeløb til at begå terrorangreb, er truslen om terrorfinansiering ikke betydelig i forhold til dette produkt/i denne sektor.

Konklusion: vurderingen af truslen om finansiering af terrorisme i relation til institutionelle investeringer gennem banker anses for mindre betydelig (niveau 1).

Hvidvask af penge

Den stigende betydning af formidlere i forbindelse med systemer til hvidvask af penge kan gøre sektoren mere udsat for de pågældende trusler, selvom viden og teknisk sagkundskab er nødvendig for at udføre dem. Kriminelle organisationer vil kunne benytte disse formidlere til at hvidvaske udbyttet af ulovlige aktiviteter. Selvom der kan samles store midler gennem denne proces, er det ikke nemt at få adgang til den, den er ikke økonomisk rentabel (afhænger af investeringernes kvalitet) og kræver under alle omstændigheder viden og teknisk sagkundskab. Derfor foretrækker kriminelle organisationer ikke denne form for risikoscenarie, mens rollen som formidlere er væsentlig, når der skal opbygges uigennemsigtige strukturer for at skjule udbyttet af kriminelle aktiviteter.

Imidlertid har man inden for de seneste par år opdaget et par metoder til flytning af store ulovlige pengestrømme, som er udarbejdet af højt kvalificerede formidlere:

- råvarekunder på kapitalmarkeder, der gennemfører over-the-counter future swaps via børser og bruger ulovlige midler til at afvikle, når de er udløbet
- samtidige køb, overførsel og salg af værdipapirer mellem lande gennemført af to enheder, der tilsyneladende er uden indbyrdes forbindelse, men er gensidigt kontrolleret
- kunder på det fast forrentede kapitalmarked gennemfører obligationshandler på vegne af organiserede kriminelle under anvendelse af ulovlige penge til køb af obligationer, og indfører derefter midler i finansielle institutioner efter salget af disse obligationer.

Konklusion: i denne henseende anses truslen om hvidvask af penge i relation til institutionelle investeringer gennem banker for betydelig (niveau 3).

Sårbarhed

Finansiering af terrorisme

Sårbarhed over for terrorfinansiering i relation til institutionelle investeringer udgør en mindre betydelig generel risiko. Risikofaktorer (produkter, kunder, geografiske forhold og fordelingskanaler) taler ikke til fordel for brugen af dette produkt/denne sektor til terrorfinansiering. Lovovertrædere har sædvanligvis ikke ekspertisen til at få adgang til sektoren, og de små pengebeløb, der anvendes til terrorangreb, gør andre sektorer mere attraktive for deres formål.

Konklusion: set i lyset af ovenstående anses truslen om finansiering af terrorisme i relation til institutionelle investeringer gennem banker for mindre betydelig (niveau 1).

Hvidvask af penge

Vurderingen af sårbarhed over for hvidvask af penge i relation til institutionelle investeringer — banker har vist følgende resultater:

a) risikoeksponering

Den vigtigste faktor, der mindsker risikoen for hvidvask af penge, er det lave niveau af kontantbaserede transaktioner, på trods af det forhold, at sektoren er udsat for højrisikokunder, herunder politisk eksponerede personer, og mængden og omfanget af grænseoverskridende transaktioner er høj. For at have adgang til sektoren skal lovovertræderne indføre penge gennem banksystemet, og det kræver en høj grad af ekspertise at skjule ulovlige penge gennem uigennemsigtige strukturer. Derfor er bankerne en første barriere, der begrænser den iboende risiko for hvidvask af penge.

b) risikobevidsthed

Risikobevidstheden i sektoren er ikke høj, når transaktionerne gennemføres uden for banksektoren. Det skyldes, at selskaberne normalt overlader det til bankerne at gennemføre kundekendskabsprocedurer og at kontrollere, når penge går ind på bankkonti.

Tilsynsmyndigheder anser den samlede risiko for sektoren for i moderat grad betydelig; men risikoprofilen på selskabsniveau viser, at en betydelig del af selskaberne er klassificeret som en mindre betydelig risiko. Trods dette anser de fleste tilsynsmyndigheder denne sektor for at udgøre en meget betydelig grænseoverskridende risiko. En anden væsentlig risiko, der er knyttet til denne sektor, er at forene standarderne for bekæmpelse af hvidvask af penge i henholdsvis hjemlandet værtslandene, når der er afdelinger af en koncern i forskellige lande.

Ifølge de finansielle efterretningsenheder er antallet af rapporter om mistænkelige transaktioner ret lavt i sammenligning med omfanget af de pågældende transaktioner, på grund af at sektoren er mere vant til at opdage svig, f.eks. insiderhandel og markedsmisbrug end at få mistanke om hvidvask af penge. Samtidig er de pågældende

finansielle transaktioner mere komplekse, og de mistænkelige af dem er antagelig ikke så lette at afsløre for de forpligtede enheder.

Sektoren oplever også en betydelig interessekonflikt mellem betænkeligheder i forhold til hvidvask af penge og behovet for at tiltrække kunder, nogle med en høj profil for hvidvask af penge, f.eks. politisk eksponerede personer, kunder fra tredjelande med højrisiko og kunder med høj indkomst. I den henseende påvirker det forhold, at tjenesteydelsen stilles til rådighed af en mægler, sårbarhedsniveauet over for hvidvask af penge og gør det højere end sårbarheden mht. kreditinstitutter.

c) retsgrundlag og kontroller

Institutionelle investeringer gennem banker er omfattet af krav om bekæmpelse af hvidvask af penge og af finansiering af terrorisme på EU-plan. På investeringsområdet har kunderådgiveren en materiel interesse i at administrere den pågældende forretningsforbindelse (goder/løn), og dette kan gøre ham/hende mere afslappet i forbindelse med gennemførelsen af kundekendskabsprocedurer.

Tilsynsmyndighederne mener, at dårlig kontrol begrænser effektiviteten af rapporteringen af mistænkelige transaktioner og effektiviteten af den løbende overvågning af retningslinjer og procedurer, herunder transaktionsovervågning. I modsætning hertil blev de fleste af de tilsidesættelser, som blev konstateret ved inspektioner, anset for at være mindre. Den mest almindelige konstatering var, at kontrollerne var af dårlig kvalitet mht. politisk eksponerede personer.

Konklusion: risikoeksponeringen er generelt meget høj på grund af kunderes art og de store beløb, der er knyttet til transaktionerne. Den iboende risiko begrænses af et lavt niveau af kontantbaserede transaktioner og af bankernes hvidvaskkontrol, når investeringsservice ydes ydes af kreditinstitutter. Alligevel kan brugen af uigennemsigtige strukturer eller komplekse projekter øge sårbarheden, hvis forpligtede enheder ikke har ressourcerne til at afsløre og rapportere til finansielle efterretningsenheder. I lyset heraf betragtes sårbarheden over for hvidvask af penge i relation til institutionel investering, der sker via banker, som i moderat grad betydelig/betydelig (niveau 2/3).

Risikobegrænsende foranstaltninger:

Kommissionen:

- en grundig kontrol af gennemførelsen af det femte direktiv om bekæmpelse af hvidvask af penge med fokus på bestemmelserne vedrørende information om reelt ejerskab, herunder sammenkobling af registre over reelle ejere på EU-niveau

- ensartet praksis inden for e-identifikation for den finansielle sektor og indførelse af standarder for at opfylde kundekendskabskrav med Reg-Tech-virksomheder.

Medlemsstater / kompetente myndigheder:

- direktiv 2018/822/EU får virkning fra 2020, og i medfør af direktiver skal mellemmænd indgive oplysninger om indberetningspligtige grænseoverskridende skatteordninger til deres nationale myndigheder

- uddybe og forbedre gennemførelsen af registre over reelle ejere og sammenkobling som beskrevet i det femte direktiv om hvidvask af penge

- samarbejde mellem den private og den offentlige sektor om udveksling af oplysninger vedrørende terrorfinansiering

- tematiske inspektioner for at vurdere

  · effektiviteten af kundekendskabskrav og udvidede kundekendskabskrav, idet de finder anvendelse på juridiske enheder og juridiske arrangementer, samt hvordan identifikationskrav mht. reelle ejere gennemføres.

3. Den institutionelle investeringssektor – mæglere

Produkt
Indskud på konti

Sektor
Investeringsselskaber – institutionel investering

Generel beskrivelse af den pågældende sektor og det/den relevante produkt/aktivitet

Sektoren for porteføjleadministration i EU er sammensat af to komplementære søjler. Den første søjle omfatter branchen for investeringsforeninger, de såkaldte "UCITS"-fonde (forvalter aktiver for 9,7 billioner EUR i 2017). Den anden søjle omfatter alternative investeringsfonde (branchen for alternative investeringsfonde havde en nettoværdi af 4,9 billioner EUR ved udgangen af 2017), f.eks. hedgefonde (11 %), private equity (4 %), funds of funds (16 %) og ejendomsfonde (11 %). Porteføljer forvaltet i EU passerede 15 billioner EUR-tærskelen ved udgangen af 2017. Branchen for porteføjleadministration i EU betjener både detailkunder – normalt bestående af husholdninger og formuende enkeltpersoner – og institutionelle kunder. Institutionelle kunder omfatter f.eks. forsikringsselskaber og pensionskasser, som tegnede sig for hhv. 25 % og 28 % af den samlede formue under forvaltning i EU ved udgangen af 2016.

Beskrivelse af risikoscenariet

Der er flere scenarier, hvor lovovertrædere kan misbruge investorer og finansielle markeder, f.eks. gennem integration af udbyttet ved adkomst til aktier for at skjule det reelle ejerforhold. Gennem svig eller gennem markedsmisbrug (der omfatter insiderhandel, kursmanipulation og ulovlig videregivelse af intern viden, som alle er omfattet af EU's forordning om markedsmisbrug og EU's direktiv om strafferetlige sanktioner for markedsmisbrug), mæglerkonti, investeringer for at legitimere kriminelle udbytter som overskud, underliggende investeringssvig eller placering af provenu hos specialiserede finansielle tjenester, der giver højt afkast.

Generel bemærkning

Dette risikoscenarie kan ses som knyttet til scenariet for investering, som foretages af mæglere. Det er blevet antaget, at for så vidt angår sårbarheden over for hvidvask er risikoniveauet højere for mæglere.

Trussel

Finansiering af terrorisme

Truslen om terrorfinansiering i relation til institutionel investering — mæglere (værdipapirer, kapitalforvaltning og investering) kunne være relevant, hvis store mængder af lovlige midler investeres i finansiering af terrorisme, men når der er tale om småbeløb til at begå terrorangreb, er truslen om terrorfinansiering ikke betydelig i forhold til dette produkt/i denne sektor.

Konklusion: vurderingen af truslen om finansiering af terrorisme i relation til institutionelle investeringer gennem mæglere anses for mindre betydelig (niveau 1).

Hvidvask af penge

Den stigende betydning af formidlere i forbindelse med systemer til hvidvask af penge kan gøre sektoren mere udsat for de pågældende trusler, selvom viden og teknisk sagkundskab er nødvendig for at udføre dem. Kriminelle organisationer vil kunne benytte disse formidlere til at hvidvaske udbyttet af ulovlige aktiviteter. Selvom der kan samles store midler gennem denne proces, er det ikke nemt at få adgang til den, den er ikke økonomisk rentabel (afhænger af investeringernes kvalitet) og kræver under alle omstændigheder viden og teknisk sagkundskab. Derfor foretrækker kriminelle organisationer ikke denne form for risikoscenarie, mens rollen som formidlere er væsentlig, når der skal opbygges uigennemsigtige strukturer for at skjule udbyttet af kriminelle aktiviteter.

Imidlertid har man inden for de seneste par år opdaget et par metoder til flytning af store ulovlige pengestrømme, som er udarbejdet af højt kvalificerede formidlere:

- råvarekunder på kapitalmarkeder, der gennemfører over-the-counter future swaps via børser og bruger ulovlige midler til at afvikle, når de er udløbet
- samtidige køb, overførsel og salg af værdipapirer mellem lande gennemført af to enheder, der tilsyneladende er uden indbyrdes forbindelse, men er gensidigt kontrolleret
- kunder på det fast forrentede kapitalmarked gennemfører obligationshandler på vegne af organiserede kriminelle under anvendelse af ulovlige penge til køb af obligationer, og indfører derefter midler i finansielle institutioner efter salget af disse obligationer.

Konklusion: i denne henseende anses truslen om hvidvask af penge i relation til institutionelle investeringer gennem mæglere for betydelig (niveau 3).

Sårbarhed

Finansiering af terrorisme

Sårbarhed over for terrorfinansiering i relation til institutionel investering — mæglere (værdipapirer, kapitalforvaltning og investering) udgør generelt en beskeden risiko. De forskellige risikofaktorer, produkter, kunder, geografi og fordelingskanaler i sektoren taler ikke til fordel for brugen af den til terrorfinansiering. I den henseende har lovovertrædere sædvanligvis ikke ekspertisen til at få adgang til sektoren, og de små pengebeløb, der anvendes til terrorangreb, gør andre sektorer mere attraktive for deres formål.

Konklusion: set i lyset af ovenstående anses sårbarheden over for finansiering af terrorisme i relation til institutionelle investeringer gennem mæglere for mindre betydelig (niveau 1).

Hvidvask af penge

Vurderingen af sårbarheden over for hvidvask af penge i relation til institutionel investering — mæglere (værdipapirer, kapitalforvaltning og investering) har vist følgende resultater:

a) risikoeksponering

Den vigtigste faktor, der mindsker risikoen for hvidvask af penge, er det lave niveau af kontantbaserede transaktioner, på trods af at sektoren er udsat for højrisikokunder, herunder politisk eksponerede personer, og mængden og omfanget af grænseoverskridende transaktioner er høj. For at have adgang til sektoren skal lovovertræderne indføre penge gennem banksystemet, og det kræver en høj grad af ekspertise at skjule ulovlige penge gennem uigennemsigtige strukturer. Derfor er bankerne en første barriere, der begrænser den iboende risiko for hvidvask af penge.

b) risikobevidsthed

Risikobevidstheden i sektoren er ikke høj, når transaktionerne gennemføres uden for banksektoren. Det skyldes, at selskaberne normalt overlader det til bankerne at gennemføre kundekendskabsprocedurer og at kontrollere, når penge kommer fra bankkonti.

Tilsynsmyndigheder anser den samlede risiko for sektoren for i moderat grad betydelig; men risikoprofilen på selskabsniveau viser, at en betydelig del af selskaberne er klassificeret som en mindre betydelig risiko. Trods dette anser de fleste tilsynsmyndigheder denne sektor for at udgøre en meget betydelig grænseoverskridende risiko. En anden væsentlig risiko, denne sektor er udsat for, er at forlige standarderne for bekæmpelse af hvidvask af penge i hjemlandet hhv. i værtslandene, når der er afdelinger af en koncern i forskellige lande.

Ifølge de finansielle efterretningsenheder er antallet af rapporter om mistænkelige transaktioner ret lavt i sammenligning med omfanget af de pågældende transaktioner, på grund af at sektoren er mere vant til at opdage svig, f.eks. insiderhandel og markedsmisbrug end at få mistanke om hvidvask af penge. Samtidig er de pågældende

finansielle transaktioner mere komplekse, og de mistænkelige af dem er antagelig ikke så lette at afsløre for de forpligtede enheder.

Sektoren oplever også en betydelig interessekonflikt mellem betænkeligheder i forhold til hvidvask af penge og behovet for at tiltrække kunder, nogle med en høj profil for hvidvask af penge, f.eks. politisk eksponerede personer, kunder fra tredjelande med højrisiko og kunder med høj indkomst. I den henseende påvirker det forhold, at tjenesteydelsen stilles til rådighed af en mægler, sårbarhedsniveauet over for hvidvask af penge og gør det højere end sårbarheden mht. kreditinstitutter.

c) retsgrundlag og kontroller

Institutionelle investeringer gennem mæglere er omfattet af krav om bekæmpelse af hvidvask af penge og af finansiering af terrorisme på EU-plan. Men kvaliteten af gennemførelsen af denne retlige ramme er tvivlsom. På investeringsområdet har kunderådgiveren en materiel interesse i at administrere den pågældende forretningsforbindelse (goder/løn), og dette kan gøre ham/hende mere afslappet i forbindelse med gennemførelsen af kundekendskabsprocedurer.

Tilsynsmyndighederne mener, at dårlig kontrol begrænser effektiviteten af rapporteringen af mistænkelige transaktioner og effektiviteten af den løbende overvågning af retningslinjer og procedurer, herunder transaktionsovervågning. I modsætning hertil blev de fleste af de tilsidesættelser, som blev konstateret ved inspektioner, anset for at være mindre. Den mest almindelige konstatering var, at kontrollerne var af dårlig kvalitet mht. politisk eksponerede personer.

Konklusion: risikoeksponeringen er generelt meget høj på grund af kunderes art og de store beløb, der er knyttet til transaktionerne. Den iboende risiko begrænses imidlertid af et lavt niveau af kontantbaserede transaktioner. Når mæglere ydet investeringsservice er sårbarheden over for hvidvask højere, end når disse tjenesteydelser leveres af banker. Manglende ressourcer til at anvende grundige kundekendskabsprocedurer og en vis grad af interessekonflikt i forhold til at tiltrække kunder med en højrisikoprofil for hvidvask af penge kan øge sårbarheden. Konklusion: i denne henseende anses truslen om hvidvask af penge i relation til institutionelle investeringer gennem mæglere for betydelig (niveau 3).

Risikobegrænsende foranstaltninger:

Kommissionen:

- en grundig kontrol af gennemførelsen af det femte direktiv om bekæmpelse af hvidvask af penge med fokus på bestemmelserne vedrørende information om reelt ejerskab, herunder sammenkobling af registre over reelle ejere på EU-niveau

- direktiv 2018/822/EU får virkning fra 2020, og i medfør af direktiver skal mellemled indgive oplysninger om indberetningspligtige grænseoverskridende skatteordninger til deres nationale myndigheder

- ensartet praksis inden for e-identifikation for den finansielle sektor og indførelse af standarder for at opfylde kundekendskabskrav med Reg-Tech-virksomheder.

De europæiske tilsynsmyndigheder:

- Retningslinjer for bedste tilsynspraksis for investeringssektoren. Konstatere de vigtigste risikoscenarier og produkter for hvidvask af penge sideløbende med de mest effektive måder til at gennemføre inspektioner på stedet og eksternt.

Medlemsstater / kompetente myndigheder:

- uddybe og forbedre gennemførelsen af registre over reelle ejere og sammenkobling som beskrevet i det femte direktiv om hvidvask af penge

- samarbejde mellem den private og den offentlige sektor om udveksling af oplysninger vedrørende terrorfinansiering

    - tematiske inspektioner for at vurdere

    - effektiviteten af kundekendskabskrav og udvidede kundekendskabskrav, idet de finder anvendelse på juridiske enheder og juridiske arrangementer, samt hvordan identifikationskrav mht. reelle ejere gennemføres.

4. Corporate banking-sektoren

Produkt
Indskud på konti

Sektor
Kreditinstitutter – corporate banking

Beskrivelse af risikoscenariet

Lovovertrædere benytter dækvirksomheder med kontanter til at indskyde provenuet i det legale økonomiske kredsløb ved hjælp af virksomhedskonti med flere underskriftsberettigede.

Trussel

Finansiering af terrorisme

Corporate banking kan tilvejebringe store mængder lovlige midler til at finansiere terrorvirksomhed eller til at sende penge til konfliktområder. Risikoscenariet er imidlertid ikke sandsynligt, idet der bruges små pengebeløb i terrorangreb, og idet der er andre produkter/brancher, der er mindre sporbare i forhold til at sende penge til risikoområder. Lovovertrædere foretrækker ikke den slags produkter til finansiering af terroristvirksomhed, så truslen om terrorfinansiering er ikke betydelig i forhold til dette produkt/denne sektor.

Konklusion: vurderingen af truslen om finansiering af terrorisme i relation til corporate banking anses for mindre betydelig (niveau 1).

Hvidvask af penge

Vurderingen af truslen om hvidvask af penge i relation til corporate banking viser, at dette risikoscenarie gennemgående er blevet brugt til sådanne ordninger. At bruge corporate banking til hvidvask af penge kræver et mere avanceret niveau end i den finansielle detailsektor, men afhængig af den finansielle tjenesteydelse, der er tale om, kan det krævede niveau være lavere: f.eks. kræves der kun personlig legitimation, hvis der skal anmodes om et lån. Men på grund af det avancerede niveau, corporate netbank kræver, ville brugen heraf til hvidvask af penge forudsætte, at der indskydes økonomiske/juridiske mellemled, som skal betales for deres "ydelser". Dette er et parameter, der kan have indflydelse på hensigtskomponenten.

Retshåndhævende myndigheder har bevis for, at professionelle pengevaskere, der fungerer som mellemled for andre organiserede kriminelle grupperinger, som opretter bankkonti for dæk- eller skuffeselskaber. Disse corporate bankkonti benyttes til fiktive handelstransaktioner, back-to-back lån med andre selskabsenheder samt investeringer i fast ejendom.

Konklusion: denne metode benyttes af organiserede kriminelle grupperinger, og mellemled spiller en stigende rolle. Efter de retshåndhævende myndigheders opfattelse kræver denne metode kun et moderat niveau af viden og ekspertise. I denne henseende anses truslen om hvidvask af penge i relation til corporate banking for betydelig (niveau 3).

Sårbarhed

Finansiering af terrorisme

Den iboende risiko for sårbarhed over for terrorfinansiering i corporate banking-sektoren er af mindre betydning. De forskellige risikofaktorer, produkter, kunder, geografi og fordelingskanaler i sektoren taler ikke til fordel for brugen af den til terrorfinansiering. Lovovertrædere har sædvanligvis ikke ekspertisen til at få adgang til sektoren, og de små pengebeløb, der anvendes til terrorangreb, gør andre sektorer mere attraktive for deres formål.

Konklusion: set i lyset af ovenstående anses truslen om finansiering af terrorisme i relation til institutionel investering gennem banker for mindre betydelig (niveau 1).

Hvidvask af penge

Vurderingen af sårbarhed over for hvidvask af penge i relation til corporate banking har vist følgende resultater:

a) risikoeksponering

Den iboende risiko er potentielt høj på grund af kundernes art, og på grund af, at der er tale om mere komplekse transaktioner end i detailbanker. Identifikation af den egentlige ejer af nogle virksomheder er en af de største svagheder i dette produkt. Nogle handelsbaserede transaktioner, der er knyttet til corporate bankkonti kan øge risikoen for hvidvask af penge, især når højrisikolande er impliceret. Den risiko, der er forbundet med forfalsket dokumentation, påvirker også niveauet for risikoeksponering, mens den stigende rolle, som mellemled og formidlere, der arbejder for organiserede kriminelle grupperinger, spiller, kan også påvirke den iboende risiko ved disse produkter. Nogle kontantbaserede transaktioner kan afvikles ved at bruge disse produkter, når virksomheder, der er involveret i corporate banking-produkter, er kontantintensive virksomheder.

Desuden kan den iboende risiko i forbindelse med disse bankprodukter blive øget gennem brugen af nye teknologier og forretningsrelationer, der ikke sker ansigt til ansigt.

For tilsynsmyndigheder for bekæmpelse af hvidvask af penge giver forskellene i organiseringen og arten af medlemsstaternes kreditinstitutsektorer sig udslag i vurderinger i den generelle risiko, som spænder fra "betydelig" og "meget betydelig" til "i moderat grad betydelig" og endda "mindre betydelig". På den anden side anser de fleste tilsynsmyndigheder den udbredte brug af kontanter i nogle undersektorer og i nogle medlemsstater for at være en af de medvirkende faktorer, der gør sektoren sårbar over for hvidvask, navnlig hvor sektoren består af mange detailbanker. Tilsynsmyndighederne anser også grænseoverskridende aktiviteter for udsat for en betydelig og meget betydelig

risiko for hvidvask af penge, navnlig i de medlemsstater, der er kendt som internationale finanscentre. Udenlandske kunder fra højrisiko-lande og off-shore virksomheder bidrager også til den forhøjede iboende risiko i denne sektor.

a) risikobevidsthed

Sektorens risikobevidsthed er høj, og sektoren har udviklet værktøjer til at udløse relevante advarselssignaler. Normalt udløses advarselssignaler som reaktion på højrisikokunder og højrisikolande samt eksistensen af grænseoverskridende transaktioner. Finansielle efterretningsenheder har bekræftet dette element og nævner, at der er modtaget et stort antal rapporter om mistænkelige transaktioner på dette område. Sektoren klager imidlertid over manglende tilbagemeldinger fra de finansielle efterretningsenheder. Det begrænser sektorens mulighed for at forbedre sine overvågningssystemer.

I de fleste medlemsstater udsender tilsynsmyndighederne for bekæmpelse af hvidvask af penge vejledninger for at hjælpe kreditinstitutterne med at afsløre potentielt mistænkelige corporate banking-transaktioner.

b) retsgrundlag og kontroller

Corporate banking er omfattet af krav om bekæmpelse af hvidvask af penge og af finansiering af terrorisme på EU-plan. Denne ramme anses som ligeså tilfredsstillende som de rammer, der dækker kreditinstitutternes andre finansielle aktiviteter.

De fleste tilsynsmyndigheder vurderede de kontroller, som kreditinstitutter har indført for at begrænse risikoen for hvidvask, som "gode" eller "rigtig gode". På trods af dette vurderer de effektiviteten af disse retningslinjer og procedurer, især dem, der vedrører løbende overvågning af transaktioner og rapportering af mistænkelige transaktioner, som ringe eller meget ringe.

Konklusion: corporate banking udviser nogen sårbarhed pga. de risikofaktorer, der er forbundet med kunder. De eksisterende retlige rammer anses imidlertid for at være tilpasset til disse sårbarheder, og kreditinstitutter, der har corporate banking aktiviteter, er bevidst om risiciene for hvidvask af penge og er udstyret til at tage sig dem. I denne henseende anses niveauet af sårbarhed over for hvidvask af penge i relation til corporate banking for i moderat grad betydelig/betydelig (niveau 2/ 3).

Risikobegrænsende foranstaltninger:

Kommissionen:

- en grundig kontrol af gennemførelsen af det femte direktiv om bekæmpelse af hvidvask af penge med fokus på bestemmelserne vedrørende information om reelt ejerskab, herunder sammenkobling af registre over reelle ejere på EU-niveau
- ensartet praksis inden for e-identifikation for den finansielle sektor og indførelse af standarder for at opfylde kundekendskabskrav med Reg-Tech-virksomheder

- direktiv 2018/822/EU får virkning fra 2020, og i medfør af direktivet skal mellemmænd indgive oplysninger om indberetningspligtige grænseoverskridende skatteordninger til deres nationale myndigheder

De europæiske tilsynsmyndigheder:

- I forbindelse med ajourføringen af den fælles udtalelse fra Det Blandede Udvalg for de europæiske tilsynsmyndigheder om risikoen for hvidvask af penge og finansiering af terrorisme bør de europæiske tilsynsmyndigheder udarbejde en analyse af operationelle risici for hvidvask af penge og terrorfinansiering knyttet til forretningen/forretningsmodellen i corporate banking-sektoren.

Medlemsstater / kompetente myndigheder:

- Myndighederne bør sørge for undervisning og vejledning om risikofaktorer med særligt fokus på relationer, der ikke foregår ansigt til ansigt, professionelle offshore formidlere, kunder eller lande og på komplekse strukturer/skuffe-konstruktioner.
- tematiske inspektioner for at vurdere:
    - effektiviteten af kundekendskabskrav og udvidede kundekendskabskrav, idet de finder anvendelse på juridiske enheder og juridiske arrangementer, samt hvordan identifikationskrav mht. reelle ejere gennemføres.

5. Private banking-sektoren

Produkt
Indskud på konti

Sektor
Kreditinstitutter – private banking og formueforvaltning

Beskrivelse af risikoscenariet
Private banking er en service, der ydes af kreditinstitutter og investeringsselskaber til meget velhavende enkeltpersoner, deres familier og selskabsenheder. Generelt tilpasses disse tjenester til hver enkelt kunde ved at kombinere flere bank- og andre finansielle tjenesteydelser i én pakke. For eksempel kan private banking-ydelser omfatte en blanding af bankydelser (løbende konti, realkreditlån og valutaveksling), investeringsstyring og -rådgivning, forvaltningsydelser, depotydelser, forsikring, regnskab, skatte- og ejendomsplanlægning og tilknyttede tjenester, f.eks. retshjælp.

Lovovertrædere benytter private banking og formueforvaltning til investere i aktier for at indføre udbytte fra strafbare forhold. På grund af kombinationen af sofistikerede finansielle produkter og tjenester og et velhavende kundegrundlag, der undertiden er politisk eksponerede personer med ofte komplekse ejerskabsstrukturer, kan sektoren også misbruges til skatteunddragelse.

Generel bemærkning

I dette risikoscenarie angår de finansielle ydelser investeringer af stor værdi og ikke investeringer foretaget af personer i detailbankerne.

Trussel

Finansiering af terrorisme

Vurderingen af truslen om terrorfinansiering i relation til private banking (formueforvaltning) er ikke blevet anset for at være relevant. Derfor er truslen fra terrorfinansiering ikke en del af vurderingen.

Konklusion: ikke relevant

Hvidvask af penge

Vurderingen af truslen om hvidvask af penge i relation til private banking (formueforvaltning) viser, at denne sektor bruges i forbindelse med følgende prædikat forbrydelser: korruption og narkohandel, bedrageri og skatteunddragelse. Dette reducerer "omfanget" af organiserede kriminelle organisationer, som kan bruge dette risikoscenarie. Det kræver også et vist niveau af ekspertise, hvilket gør det vanskeligere at få adgang til og ikke særlig attraktivt (ikke rentabelt). I private banking er servicen ganske "bekostelig" (behov for tilstrækkelige midler til at få adgang til ydelserne), og forretningsforbindelsen vanskeligere at etablere. Nogle grupperinger kan imidlertid bruge formidlere til at opnå adgang til private banking gennem strømænd eller juridiske personer.

Konklusion: på baggrund af ovenstående anses truslen om hvidvask af penge i relation til private banking for betydelig/meget betydelig (niveau 3/4).

Sårbarhed

Finansiering af terrorisme

Vurderingen af sårbarheden over for terrorfinansiering i relation til private banking (formueforvaltning) er ikke blevet anset for at være relevant. I denne henseende er sårbarheden over for terrorfinansiering ikke en del af vurderingen.

Konklusion: ikke relevant

Hvidvask af penge

Vurderingen af sårbarhed over for hvidvask af penge i relation til private banking (formueforvaltning) har vist følgende resultater:

a) risikoeksponering

Kombinationen af sofistikerede finansielle produkter og tjenester og et velhavende kundegrundlag (undertiden politisk eksponerede personer) med ofte komplekse ejerskabsstrukturer gør i høj grad denne sektor sårbar over for hvidvask af penge. Nogle af de tilbudte produkter og ydelse anses også for at være sårbare over for hvidvask af penge, især dem der er forbundet med overholdelse af skatteregler og skatteplanlægning. "Aggressiv" skatteplanlægning ser ud til at være en sådan type ydelse. Endvidere udgør sektoren en større geografisk risiko på grund af etableringen af filialer i nogle lande uden for EU, der ikke nødvendigvis har ordninger for bekæmpelse af hvidvask af penge og af finansiering af terrorisme, der svarer til EU's ramme for bekæmpelse af hvidvask af penge og af finansiering af terrorisme.

b) risikobevidsthed

Ifølge finansielle efterretningsenheder er private banking kendetegnet ved et meget lavt (næsten ikke eksisterende) niveau for indberetning af mistænkelige transaktioner. Hvad angår investeringsservice står institutterne nogle gange over for en konflikt mellem deres kommercielle mål og behovet for at bekæmpe hvidvask af penge. Konkurrencekomponenten er ikke ubetydelig. Men for private banking er risikovurderingen ikke altid tilstrækkeligt præcis til at sikre, at sektoren er klar over de risici, den står overfor, især risici i forbindelse med bedrageri og skatteunddragelse. Tilsynsmyndighederne mener, at virksomhederne inden for denne sektor ikke i tilstrækkelig grad reducerer risikoen for, at sektoren misbruges til skatteunddragelse.

c) retsgrundlag og kontroller

Private banking er omfattet af krav om bekæmpelse af hvidvask af penge og af finansiering af terrorisme på EU-plan. De fleste kompetente myndigheder, som har inspiceret udbydere af private banking-ydelser, har anset niveauet af kontroller for "utilstrækkeligt" som kundekendskabskrav (verifikation af kundens identitet, oplysninger om midlernes oprindelse, verifikation af af de reelle ejerforhold — særligt for så vidt angår juridiske

personer), overvågning af transaktioner og compliance-funktionen. De forklarer denne svaghed gennem: i) det forhold, at kvaliteten af de finansielle kontroller afhænger af et lands økonomiske kultur, og ii) at forståelsen af de risici, der udgår fra denne sektor, ikke er den samme fra den ene medlemsstat til den anden.

Konklusion: Høj generel risiko på grund af de store beløb, der er involveret, højrisikokunder (politisk eksponerede personer) og potentielt højrisikolande. Betænkeligheder angående sektorens risikobevidsthed på grund af konkurrencen mellem udbyderne om at tiltrække højrisikokunder, mens resultaterne af tematiske undersøgelser har vist utilstrækkelige kontroller på visse områder. Endvidere er niveauet for indberetninger af mistænkelige transaktioner lavt. I denne henseende anses niveauet af sårbarhed over for hvidvask af penge i relation til private banking for betydeligt/meget betydeligt (niveau 3/4).

Risikobegrænsende foranstaltninger:

Kommissionen:

- en grundig kontrol af gennemførelsen af det femte direktiv om bekæmpelse af hvidvask af penge med fokus på bestemmelserne vedrørende information om reelt ejerskab, herunder sammenkobling af registre over reelle ejere på EU-niveau
- ensartet praksis inden for e-identifikation for den finansielle sektor og indførelse af standarder for at opfylde kundekendskabskrav med Reg-Tech-virksomheder
- direktiv 2018/822/EU får virkning fra 2020, og i medfør af direktivet skal mellemmænd indgive oplysninger om indberetningspligtige grænseoverskridende skatteordninger til deres nationale myndigheder

De europæiske tilsynsmyndigheder:

- Europæiske tilsynsmyndigheder sørger for kurser til de kompetente myndigheder med fokus på en fælles metode til inspektioner samt de vigtigste risikoområder.

Medlemsstater / kompetente myndigheder:

- tematiske inspektioner for at vurdere:
  - effektiviteten af kundekendskabskrav og udvidede kundekendskabskrav, idet de finder anvendelse på juridiske enheder og juridiske arrangementer, samt hvordan identifikationskrav mht. reelle ejere gennemføres.
- Risici forbundet med denne sektor bør klart fremgå af de kompetente myndigheders risikovurdering vedrørende hvidvask/terrorfinansiering. De kompetente myndigheder bør udstede retningslinjer om bedste praksis og sørge for uddannelse til sektoren.

- De kompetente myndigheder bør sikre, at der indføres systemer og kontroller med henblik på at begrænse selskabernes mulighed for at udforme eller anbefale produkter og ydelser, der hjælper deres kunder med at begå skattekriminalitet.

6. Crowdfunding

Produkt
Crowdfunding

Sektor
Platforme for crowdfunding

Generel beskrivelse af den pågældende sektor og det/den relevante produkt/aktivitet

Crowdfunding er en åben opfordring til offentligheden om at tilvejebringe midler til et konkret projekt. Crowdfunding-platforme er websteder, der muliggør interaktion mellem fundraisere og enkeltpersoner, der er interesseret i at bidrage økonomisk til projektet. Økonomiske tilsagn gives og indhentes via platformen.

Typen af fundraising-aktiviteter varierer meget mellem de forskellige crowdfunding-modeller. Der er også forskelle i deltagernes motivationen og type samt den heraf følgende forbindelse mellem investorer/långivere og lånesøgende/lånere. Der findes forskellige modeller af crowdfunding-platforme og enhver kategorisering er foreløbig, da markedet udvikler sig og integrerer nye teknologier i leveringen af ydelser. De fem hovedkategorier af crowdfunding-platforme er:

- investeringsbaseret crowdfunding: virksomheder udsteder aktier eller gældsinstrumenter til crowd-investorer via en platform
- lånebaseret crowdfunding (også kendt som crowdlending, peer-to-peer eller markedspladslån): virksomheder eller enkeltpersoner søger at skaffe midler fra offentligheden via platforme i form af en låneaftale
- fakturahandel-crowdfunding: en form for aktivbaseret finansiering, hvor virksomheder sælger ubetalte fakturaer eller tilgodehavender, individuelt eller i et bundt, til en pool af investorer via en online platform,
- belønningsbaseret crowdfunding: enkeltpersoner donerer til et projekt eller en forretning med forventning om at modtage en ikke-økonomisk belønning, f.eks. varer eller ydelser på et senere tidspunkt til gengæld for deres bidrag
- donationsbaseret crowdfunding: enkeltpersoner donerer beløb for at opfylde et konkret velgørende projekts større finansieringsmål uden at modtage økonomisk eller materielt afkast.

Der findes en række platforme, som kombinerer forskellige modeller eller benytter en model, der ikke umiddelbart kan henføres til disse fem kategorier ("hybridmodeller -

crowdfunding"). De er imidlertid normalt af en meget mindre størrelsesorden end hovedmodellerne.

En anden relevant klassificering af crowdfunding-platforme afhænger af, om de er godkendt eller ej:

- Regulerede crowdfunding-platforme, der er omfattet af anvendelsesområdet for eksisterende lovgivning om finansielle tjenesteydelser (dvs. Investeringsbaserede og lånebaserede platforme), og som dermed er godkendt.
- Uregulerede crowdfunding-platforme, som falder uden for anvendelsesområdet for lovgivningen om finansielle tjenesteydelser (dvs. donationsbaseret, belønningsbaseret, forbrugslånsbaseret crowdfunding). Dette omfatter også websteder, dvs. sociale medieplatforme, messaging apps eller blogs med en potentielt stor rækkevidde, som gør det muligt for deres brugere at udsende en offentlig opfordring til indsamling af midler, men hvor selve platformen ikke faciliterer denne proces.

Det bør også tages i betragtning, at platformene præsenterer de relevante parter for hinanden og knytter dem sammen, men de faktiske pengetransaktioner udføres normalt af godkendte udbydere af betalingstjenester, der er omfattet af anvendelsesområdet for lovgivning om bekæmpelse af hvidvask af penge. Der bør derfor yderligere ske en sondring mellem reguleret crowdfunding, hvor transaktioner sker via godkendte betalingsudbydere (dvs. ved forbindelse til PayPal eller ved at henvise til personlige bankkonti) på regulerede crowdfunding-platforme, der er omfattet af supplerende oplysningskrav, og ureguleret crowdfunding, som for tiden ikke er omfattet af lovgivning om finansielle tjenesteydelser. Navnlig på det uregulerede område kan betalinger også finde sted på mindre gennemsigtige måder, dvs. krypto-aktiver eller forudbetalte simkort tokens.

Det europæiske marked for alternativ finansiering som helhed rejste 10,44 mia. EUR i 2017, en stigning på 36 % i forhold til året før. Markedet er stærkt domineret af Det Forenede Kongerige, der havde en markedsandel på 68 % med 7,07 mia. euro i 2016, hvilket var et fald fra 75 % året før. Resten af det europæiske marked rejste i alt 3,37 mia. EUR og voksede med 63 % det år. Dette gør crowdfunding til det vigtigste delmarked i sektoren for alternativ finansiering. Bortset fra Det Forenede Kongerige var de lande, der havde det største samlede markedsvolumen i 2016, Frankrig, Tyskland, Nederlandene, Italien og Finland.

En mere detaljeret undersøgelse af markedsandele viser, at peer-to-peer forbrugerudlån har den største markedsandel med 41 %, efterfulgt af fakturahandel (16 %), peer-to-peer erhvervsudlån (14 %), fast ejendom crowdfunding (8 %) og aktiebaseret crowdfunding (6 %).

Beskrivelse af risikoscenariet

Lovovertrædere kan oprette platforme med henblik på at indsamle/akkumulere midler og overfører dem til udlandet med henblik på hvidvask af penge eller finansiering af terrorangreb. Dette kan gøres ved at oprette en reguleret crowdfunding-platform, der er

direkte knyttet til en finansiel institution [38] eller ved at oprette en platform uden for et reguleret miljø og ikke knyttet til en finansiel institution, hvor betalinger kan ske i virtuel valuta, e-pengekort mv. ... Ikke autoriserede crowdfunding-platforme kan oprettes i forhold fiktive projekter med henblik på at modtage midler, der så hæves inden for EU eller overføres til udlandet. Denne metode kan enten bruges til at modtage midler fra legitime kilder til finansiering af terrorisme eller til at modtage ulovlige midler fra kriminelle aktiviteter ved hjælp af anonyme produkter.

Misbrug af sociale medier ("crowdsourcing") er en anden slags risikoscenarie. Især har terrorgrupper gjort brug af sociale medier og andre online og mobile platforme til at skaffe midler, som derefter bliver kanaliseret afsted gennem forskellige betalingsmidler. Denne type crowdsourcing analyseres ikke nærmere her.

Trussel

Finansiering af terrorisme

Terrorgrupper kan have til hensigt at bruge crowdfunding-teknikker til at modtage midler. Samlet set har der været få tilfælde af (uregulerede) donationsplatforme, hvor disse teknikker er blevet anvendt, og i de tilfælde har det sædvanligvis været for at rejse mindre beløb. Derudover er mistænkelige aktiviteter noget lettere at afsløre, og det kan afholde terrorgrupper fra at bruge denne metode, da den ikke er den sikreste løsning. Men hvis lovovertræderne er mere systematiske i deres planlægning, vil dette sætte dem i stand til at oprette indsamlingsplatforme med mulighed for mere anonyme aktiviteter (brug af strømænd eller pårørende), hvilket ville gøre denne metode mere attraktiv. Retshåndhævende myndigheder har afsløret nogle tilfælde af crowdfunding-opfordringer til at donere, hvor man har anført "støtte til enker, martyrer, religiøse grupper" i et forsøg på at undgå en klar sammenkædning med finansiering af terrorisme. Værdien af donationerne er lav (10, 20, 50 USD, de fleste beløb i US-dollar). Det er svært for de retshåndhævende myndigheder at finde frem til de endelige modtagere samt brugen af donationerne (bevis for terrorfinansiering).

Konklusion: Retshåndhævende myndigheder har bevis for, at terroristgrupper bruger uregulerede donationsbaserede crowdfunding-platforme. Det er imidlertid ikke rentabelt at rejse eller kanalisere store beløb på denne måde. Det kan også være noget usikkert sammenlignet med andre typer ydelser, og det kræver mere planlægning at skjule den ulovlige hensigt. I denne henseende anses truslen om terrorfinansiering i relation til crowdfunding som i moderat grad betydelig (niveau 2).

Hvidvask af penge

Vurderingen af truslen om hvidvask af penge i relation til crowdfunding viser, at der er få eller ingen beviser på eller indikationer af, at kriminelle har brugt det til at hvidvaske udbytte fra kriminalitet. Der er dog tilfælde, hvor et selskab er oprettet med det formål at

[38] Knyttet til en bankkonto eller med et bankpartnerskab.

blive anvendt til kriminelle aktiviteter i forbindelse med crowdfunding, men det kræver en vis ekspertise og kan være bekosteligt. Et enkelt tilfælde, man har fundet, var et komplekst pyramidespil med brug af svig og falske projekter. Det tyder på, at dette scenarie kan være vanskeligt tilgængelig og kræver, at man har adgang til betalingsprocedurer. Det betyder, at brug af kriminelle mellemled kunne gøre sektoren mere attraktiv med henblik på hvidvask af penge. Imidlertid mener de retshåndhævende myndigheder, at sektoren stadig bruges mere til svigagtige indsamlinger og bedrageri snarere end til at hvidvaske ulovlige midler.

Konklusion: kriminelle kan have vage intentioner om at udnytte denne metode, som ikke nødvendigvis er attraktiv og kan være bekostelig. Under alle omstændigheder kræver metoden nogen ekspertise for at være rentabel. Der er kun få beviser for, at den er blevet brugt, selvom der ikke kan ses bort fra formidlernes rolle. I denne henseende anses truslen om pengevask i relation til crowdfunding som i moderat grad betydelig (niveau 2)

Sårbarhed

Finansiering af terrorisme

Vurderingen af sårbarhed over for terrorfinansiering i relation til crowdfunding viser, at sektoren ikke kan vurderes isoleret.

a) risikoeksponering

Niveauet for risikoeksponering varierer afhængigt af, om crowdfunding-platformen er under tilsyn som udbyder af finansielle tjenester eller er ureguleret (private initiativer på internettet). Ligeledes afhænger risikoen for terrorfinansiering også af, hvilken type platform der er tale om. Uregulerede donationsbaserede platforme udgør en højere generel risiko for misbrug til finansiering af terrorisme, idet disse platforme falder uden for området for finansielle institutioner og tilsynsmyndigheder vedrørende hvidvask. Den iboende risiko i forbindelse med crowdfunding er højere, hvis crowdfunding-platforme tillader brug af virtuelle valutaer eller (anonyme) elektroniske penge. Den iboende risiko er også højere, hvis lovovertrædere opretter donationsbaserede crowdfunding-platforme, der muliggør brug af stråmænd, familie eller enkeltpersoner uden for anvendelsesområdet for sanktionslister.

b) risikobevidsthed

Selv når en crowdfunding-platform er reguleret som finansiel tjenesteudbyder, kan der være en mangel på viden om kilderne til midler samt formålet. Når de stilles til rådighed gennem uregulerede platforme, befinder crowdfunding-tjenester sig uden for anvendelsesområdet for overvågning til bekæmpelse af hvidvask af penge og af finansiering af terrorisme. Kompetente myndigheder, herunder på EU-niveau, er opmærksomme på, at der er risici mht. finansiering af terrorisme, men risikovurderingen er stadig ufuldstændig i de fleste medlemsstater. Det skal imidlertid understreges, at hvis platformene er optaget på listen over forpligtede enheder, vil finansielle efterretningsenheder modtage indberetninger om mistænkelige transaktioner.

c) retsgrundlag og kontroller

EU's regelværk om bekæmpelse af hvidvask af penge og af finansiering af terrorisme gælder generelt ikke for crowdfunding-platforme som sådan, men gælder for særlige typer af crowdfunding-ydelser afhængigt af forretningsmodellen. Der er derfor ingen tværgående rammer, der fastsætter forpligtelser mht. bekæmpelse af hvidvask af penge og af finansiering af terrorisme for disse ydelser.

Crowdfunding-platforme er særligt reguleret i nogle medlemsstater, navnlig for værdipapirer og lån, hvilket betyder, at donationsplatforme ikke er omfattet af forpligtelserne vedrørende bekæmpelse af hvidvask af penge og af finansiering af terrorisme. Nogle medlemsstater har medtaget crowdfunding-platforme i deres lovgivning til gennemførelse af det andet direktiv om betalingstjenester. De kompetente myndigheder skønner imidlertid, at kontrollerne og tilsynsvirksomheden er svage, især da mange platforme ikke er fysisk etableret i det område, hvor de arbejder, hvilket skader kontrollernes effektivitet. Hvor kredit- og finansielle institutioner er impliceret, er de forpligtede enheders kontroller mindre mindre effektive, idet de forpligtede enheder kun kan støtte sig på mere begrænsede oplysninger med henblik på overvågning af transaktioner og anvendelse af advarselssignaler.

Konklusion: sektoren er ikke homogen, og sammenhængen med andre sektorer kan påvirke sårbarhedsniveauet. Eksisterende kontroller er ikke harmoniseret, fordi der ikke er nogen tværgående rammer, der beskæftiger sig med dette spørgsmål, selvom den nye forordning om europæiske crowdfunding-tjenesteudbydere for erhvervslivet vil forbedre denne ramme. Der er en vis bekymring med hensyn til sektorens bevidsthed. I denne henseende anses sårbarhedsniveauet over for terrorfinansiering i relation til crowdfunding for i moderat grad betydeligt (niveau 2)

Hvidvask af penge

Vurderingen af sårbarheden over for hvidvask af penge i relation til crowdfunding svarer til vurderingen af sårbarheden over for terrorfinansiering.

a) risikoeksponering

Niveauet for risikoeksponering varierer afhængigt af, om crowdfunding-platformen er direkte knyttet til finansieringsinstitutter eller er overladt til private initiativer på internettet. I begge tilfælde kan brugen af virtuelle valutaer øge den iboende risiko for hvidvask af penge. Afhængig af platformstypen kan tjenesterne muligvis lette anonyme transaktioner. På låne- og værdipapirplatforme er det muligt at rejse større beløb, hvilket gør den iboende risiko for hvidvask af penge større end for donationsplatforme. Imidlertid vil disse crowdfunding-platforme normalt være reguleret og således overholde oplysningskravene og samarbejde med betaling- eller kreditinstitutter om at gennemføre betalingstransaktioner.

b) risikobevidsthed

Kriminelle organisationers infiltrering af sådanne platforme bør også betragtes som en yderligere sårbarhedsfaktor. Nogle retshåndhævende myndigheder og finansielle

efterretningsenheder er tilbøjelige til at betragte crowdfunding som en udbredt måde at hvidvaske penge på. Selv når en finansiel institution er involveret, er der mangel på viden om kilderne til midlerne, omfanget af midlerne og formålet med dem. Når de stilles til rådighed gennem uregulerede enheder, befinder crowdfunding-tjenester sig uden for anvendelsesområdet for overvågning til bekæmpelse af hvidvask af penge og af finansiering af terrorisme. Kompetente myndigheder, herunder på EU-niveau, er opmærksomme på, at der findes risici for hvidvask af penge, men nogle af dem betragter denne sektor som lavrisiko og overvejer ikke at medtage crowdfunding-platforme som forpligtede enheder. Det skal imidlertid understreges, at hvis platformene er optaget på listen over forpligtede enheder, vil finansielle efterretningsenheder modtage indberetninger om mistænkelige transaktioner.

c) retsgrundlag og kontroller

EU's regelværk om bekæmpelse af hvidvask af penge og af finansiering af terrorisme gælder generelt ikke for crowdfunding-platforme som sådan, men gælder for særlige typer af crowdfunding-ydelser afhængigt af forretningsmodellen. Der er derfor ingen tværgående rammer, der fastsætter forpligtelser mht. bekæmpelse af hvidvask af penge og af finansiering af terrorisme for disse ydelser.

Særlige typer crowdfunding-tjenester vil i de fleste tilfælde være omfattet af forpligtelser til bekæmpelse af hvidvask af penge og af finansiering af terrorisme afhængigt af forretningsmodel (f.eks. investeringsbaseret og lånebaseret crowdfunding-baseret). Nogle medlemsstater har medtaget crowdfunding-platforme i deres lovgivning til gennemførelse af andet direktiv om markeder for finansielle instrumenter og andet direktiv om betalingstjenester. På nuværende tidspunkt er det imidlertid ikke alle medlemsstater der overvejer at medtage crowdfunding-platforme som forpligtede enheder.

Selv når crowdfunding platforme anses for forpligtede enheder skønner de kompetente myndigheder, at kontrollerne og tilsynsvirksomheden er svage, især da mange platforme ikke er fysisk etableret i det område, hvor de arbejder, hvilket skader kontrollernes effektivitet. Hvor kredit- og finansielle institutioner er impliceret, kan forpligtede enheders kontroller være mindre intense, hvis de forpligtede enheder kun kan støtte sig på mere begrænsede oplysninger med henblik på overvågning af transaktioner og at anvendelse af advarselssignaler.

Konklusion: risikoeksponeringen er temmelig begrænset, selvom der kan være store summer involveret i visse konkrete forretningsmodeller for crowdfunding. Eksisterende kontroller er ikke harmoniseret, fordi der ikke er nogen tværgående rammer, der beskæftiger sig med dette spørgsmål. Når de er under tilsyn, er man med hensyn til disse platforme udmærket klar over de risici, der er forbundet med dem, og indberetningsniveauet er godt. De eksisterende kontrol er undertiden svag, især når de forpligtede enheder er afhængige af begrænset information med henblik på at udføre kontroller. Den nye forordning om europæiske crowdfunding-tjenesteudbydere vil forbedre denne ramme. I denne henseende anses niveauet af sårbarhed over for hvidvask af penge for i moderat grad betydeligt (niveau 2).

Risikobegrænsende foranstaltninger:

Medlemsstater / kompetente myndigheder:

- Ved anvendelsen af artikel 4 i det femte direktiv om bekæmpelse af hvidvask af penge, der udvider anvendelsesområdet for forpligtede enheder, bør medlemsstaterne overveje behovet for at definere uregulerede crowdfunding-platforme som forpligtede enheder med krav om bekæmpelse af hvidvask af penge og af finansiering af terrorisme.

7. Valutaveksling

Produkt
Omveksling af midler

Sektor
Vekselkontorer

Beskrivelse af risikoscenariet

Lovovertrædere veksler deres midler til en anden valuta for gøre det lettere omveksle, overføre eller hvidvaske penge.

Trussel

Finansiering af terrorisme

Vurderingen af truslen om terrorfinansiering i forbindelse med valutaveksling viser, at denne fremgangsmåde udnyttes af terrorgrupper, især af udenlandske terrorkrigere. EUR/USD-omveksling er særlig attraktiv for disse grupper. At bringe valuta ind i konfliktområder er en af de vigtigste måder til finansiering af udenlandske terrorkrigere på. Fra et teknisk synspunkt kræver veksling af midler ikke nogen særlig planlægning, viden eller ekspertise og er meget let at bruge. Selvom det ikke består i at rejse eller overføre midler, er det et nødvendigt skridt til at flytte fysisk "ren" valuta (for det meste i kontanter). Terrorgrupper kan muligvis anse valutaveksling for lige så attraktivt som at indsamle eller overføre midler til at finansiere deres aktiviteter.

Konklusion: terrorgrupper viser nogen hensigt og kapacitet til at bruge valutaveksling til understøtte/gennemføre deres aktiviteter. Dette scenarie kræver ikke nogen nærmere planlægning eller ekspertise og er allerede blevet brugt. I denne henseende anses trusselsniveauet mht. terrorfinansiering i relation til valutaveksling for betydeligt (niveau 3).

Hvidvask af penge

Vurderingen af truslen om hvidvask i relation til valutaveksling viser, at vekselkontorer i nogle tilfælde er blevet infiltreret af kriminelle organisationer, som driver deres virksomheder. Dette er især udbredt mht. kontorer i lufthavns- og turistområder. Store pengebeløb kan let omveksles, så det bliver let for disse kriminelle organisationer at få adgang til "ren" valuta. Som med hensyn til terrorfinansiering kræver valutaveksling ikke nogen nærmere planlægning eller ekspertise for at hvidvaske penge. Imidlertid er omfanget af mistænkelige transaktioner vanskeligt at vurdere i øjeblikket.

Konklusion: selvom mængden af sager er vanskelig at vurdere for de retshåndhævende myndigheder, viser indikatorerne, at kriminelle organisationer kan bruge valutaveksling til hvidvask af udbyttet af kriminalitet. Dette scenarie kræver ikke nogen nærmere planlægning eller ekspertise og er allerede blevet brugt.

I denne henseende anses trusselsniveauet mht. hvidvask af penge i relation til valutaveksling for betydeligt (niveau 3).

Sårbarhed

Finansiering af terrorisme

Sårbarhed i forbindelse med valutaveksling er knyttet til overførsel af midler. Der er to forskellige måder, hvorpå transaktioner kan udføres:

- brug af kontanter til at veksle og overføre midlerne til en bestemt bank eller betalingskonto
- brug af internettet til at gennemføre valutaveksling og overføre midlerne til en bankkonto eller betalingskonto.

a) risikoeksponering

Det forhold, at hovedparten af transaktionerne sker kontant, øger sektorens sårbarhed. Endvidere involverer transaktioner, der muligvis har forbindelse til finansiering af terrorisme, som regel små beløb i kontanter, hvilket gør dem vanskeligere for vekselkontorerne at afsløre.

b) risikobevidsthed

I nogle risikoscenarier er udbydere af penge- eller værdioverførselstjenester forbundet med vekselkontorer eller opererer endda fra de samme lokaler. I sådanne tilfælde finder de varslingssystemer og advarselssignaler, der benyttes af udbydere af penge- eller værdioverførselstjenester til at afsløre transaktioner med forbindelse til terrorfinansiering, anvendelse på den forudgående valutahandel. Den negative virkning er, at vekselkontorerne er afhængige af de terrorfinansieringskontroller, der foretages af udbyderne af penge- eller værdioverførselstjenester. Vekselkontoret befinder er ikke selv i stand til at følge hele transaktionen, afsløre mistænkelige transaktioner og indgå i en komplet forretningsrelation med sine kunder.

Risikobevidstheden i sektoren er høj, navnlig når vekselkontorer er tæt på penge- eller værdioverførselstjenester, men niveauet for indberetning af mistænkelige transaktioner er fortsat lavt, bortset fra særlige tilfælde, f.eks. anmodning omveksling af USD fra højrisikolande uden for EU (f.eks. Syrien).

c) retsgrundlag og kontroller

Vekselkontorer er omfattet af rammerne for bekæmpelse af hvidvask af penge og af bekæmpelse af terrorisme på EU-plan. Tilsynsmyndighederne mener, at de kontroller, der vedrører effektiviteten af rapporteringen af mistænkelige transaktioner, generelt er ringe eller meget ringe, på linje med kontroller vedrørende til kundeidentifikation og -verifikation. I den henseende kan ny teknologisk udvikling blive en vigtig risikobegrænsende kraft for denne sektor, når henses til stigningen i onlinebetalinger. Tilsynsaktiviteter har for det meste været begrænset til off-site inspektioner, og nogle

tematiske inspektioner er udført som reaktion på identificerede, konkrete risici. Når nogle jurisdiktioner anvender tærskler for lejlighedsvise transaktioner, er sårbarheden større, især for risici for terrorfinansiering, hvor små beløb er normen.

Konklusion: Kontrollerne inden for sektoren er ikke ret effektive og er afhængige af tilknyttede sektorer som f.eks. udbydere af penge- eller værdioverførselstjenester og banker. Tærskler for lejlighedsvise transaktioner kan markant påvirke overvågningssystemerne og kundekendskabskravene, hvilket øger sårbarheden over for finansiering af terrorisme. I denne henseende anses sårbarhedsniveauet for terrorfinansiering i relation til valutaveksling for betydeligt (niveau 3).

Hvidvask af penge

Vurderingen af sårbarhed over for hvidvask af penge i relation til valutaveksling har vist følgende resultater:

a) risikoeksponering

Det forhold, at størstedelen af transaktionerne sker kontant, påvirker sårbarheden. Den virkning er mere udtalt, når kunden anvender pengesedler med pålydende høj pålydende værdi, som ikke overvåges godt. Andre faktorer, som øger den sektorspecifikke risiko, er politisk eksponerede personers brug af disse tjenester, eller at vekselkontorerne ligger i grænseområder. Den største risikofaktor er kriminelle organisationers infiltration af vekselkontorer eller -agenturer. Den iboende risiko øges, hvis virksomhederne har utilstrækkelige værktøjer til at afsløre potentielt dårlige valutavekslingsagenter.

b) risikobevidsthed

I nogle risikoscenarier er udbydere af penge- eller værdioverførselstjenester forbundet med vekselkontorer eller opererer endda fra de samme lokaler. I sådanne tilfælde finder de varslingssystemer og advarselssignaler, der benyttes af udbydere af penge- eller værdioverførselstjenester til at afsløre transaktioner med forbindelse til pengevask, anvendelse på den forudgående valutahandel. Den negative virkning er, at vekselkontorerne bruger de kontroller af hvidvask af penge, der foretages af udbyderne af penge- eller værdioverførselstjenester. I forhold til bekæmpelse af hvidvask af penge er indberetningsniveauet uensartet fra den ene medlemsstat til den anden, og består ikke nødvendigvis af indberetninger om mistænkelige transaktioner (mest indberetninger om valutatransaktioner).

Tilsynsmyndighedernes vurderinger af den iboende risiko for valutavekslingssektoren er forskellige og spænder fra meget betydelig til mindre betydelig. De konstaterende aktuelle risici omfatter: transaktionernes anonymitet, nærhed til grænseregioner og vandrende samfundsgrupper (migranter, grænseoverskridende arbejdstagere, asylansøgere, turisme) og udbredelsen af kontanttransaktioner. Forskellige kompetente myndigheder har identificeret disse som kilden til den største bekymring.

c) retsgrundlag og kontroller

Vekselkontorer er omfattet af rammerne for bekæmpelse af hvidvask af penge og af bekæmpelse af terrorisme på EU-plan. Tilsynsmyndighederne betragter ikke

valutasektoren som højrisiko generelt. Ifølge denne vurdering er ressourcerne til at føre tilsyn med denne sektor mere begrænsede end i andre sektorer. Derudover nævnte mange kompetente myndigheder som konstante risikofaktorer dårlig intern kontrol, manglende opmærksomhed om den relevante lovgivningsmæssige kontekst og ringe rapporteringspraksis om mistænkelig aktivitet, selvom der gennemføres kontrol.

En anden faktor, der er til hinder for korrekt kontrol i valutavekslingskontorer, er den begrænsning, der kan fastsættes i forskellige lande, så kundekendskabskravene kun anvendes på lejlighedsvise transaktioner; under alle omstændigheder anvender de fleste medlemsstater tærskler under 15 000 EUR.

Konklusion: Bevidstheden i sektoren er temmelig ujævn, og eksisterende kontroller er ikke effektive, når henses til det lave rapporteringsniveau. De kompetente myndigheder mener ikke, at reglerne og tilsynet fungerer effektivt. I denne henseende anses trusselsniveauet for hvidvask af penge i relation til valutaveksling for betydeligt (niveau 3).

Risikobegrænsende foranstaltninger:

Medlemsstater / kompetente myndigheder

- Kompetente myndigheder bør foretage et antal tematiske inspektioner på stedet med fokus på de risici, agenter udgør. Omfanget af disse tematiske inspektioner bør omfatte kontrol af, at selskaber, der driver penge- eller værdioverførselstjenester, har en dækkende funktion vedrørende tilsyn med agenter, herunder effektive overvågningssystemer, revisioner på stedet og uddannelse.
- Medlemsstaterne bør afskaffe tærsklerne for anvendelse af kundekendskabs krav på lejlighedsvise transaktioner i valutasektoren for at forbedre overvågningen af mistænkelige transaktioner.

8. E-pengesektoren

Produkt
E-penge

Sektor
Kredit- og finansielle institutioner

Generel beskrivelse af den pågældende sektor og det/den relevante produkt/aktivitet

"Elektroniske penge" er defineret i det andet e-pengedirektiv (2009/110/EF) som en elektronisk eller magnetisk lagret pengeværdi som repræsenteret ved et krav på udstederen, der er udstedt efter modtagelse af midler med henblik på at gennemføre betalingstransaktioner, og som accepteres af en anden fysisk eller juridisk person end udstederen af elektroniske penge.

Et karakteristisk egenskab ved e-penge er, at de er forudbetalt. Dette betyder, at en konto, et kort eller en enhed skal krediteres en pengeværdi, for at denne værdi kan udgøre e-penge. E-penge kan for eksempel lagres på kort, på mobile enheder og på onlinekonti. Afhængig af, hvordan e-penge lagres, kan de klassificeres som "hardwarebaserede" eller "serverbaserede". Visse e-pengeprodukter kræver identifikation af ejeren; andre tillader ejere at forblive anonyme.

E-pengetypologi

En første klassificering af e-pengeprodukter afhænger af den teknologi, der bruges til at lagre den monetære værdi. Produkter kan være hardwarebaserede eller softwarebaserede.

For så vidt angår hardwarebaserede produkter findes købekraften i en fysisk enhed, f.eks. et chipkort med hardwarebaserede sikkerhedsfunktioner. Pengeværdier overføres typisk ved hjælp af enhedslæsere, der ikke kræver netværksforbindelse i realtid til en ekstern server.

Softwarebaserede produkter har specialiseret software, der fungerer på almindelige enheder, f.eks. computere eller tablets. For at muliggøre overførsel af pengeværdier skal enheden typisk etablere en onlineforbindelse med en fjernserver, der kontrollerer brugen af købekraften. Ordninger, der blander både hardware- og softwarebaserede funktioner findes også.

Andre mulige sondringer mellem forskellige e-pengeprodukter kan omfatte den måde, hvorpå e-penge skabes eller udstedes. Den vigtigste sondring vedrører spørgsmålet om, hvorvidt e-penge kan forudbetales af brugeren (betaleren) eller af en tredjepart på vegne af eller til fordel for betaleren (f.eks. af en virksomhed i forhold til business-to-businesskort eller af en handlende i loyalitetsordninger med flere handlende).

Nogle e-pengeprodukter kan tankes op (for at tilføje mere værdi efter udstederens første udstedelse af e-penge), andre ikke.

Hvordan e-pengeprodukter klassificeres afhænger af, om produktet er multifunktionelt eller er knyttet til en platform. Begge typer kan bruges online, men sidstnævnte tillader kun køb på én enkelt platform og tillader ikke peer-to-peer-overførsler. I begge tilfælde er der behov for en bankkonto til optankning af e-pengeprodukterne. En anden kategori omfatter forudbetalte kort eller værdikuponer med undtagelser fra kundekendskabskravene. Disse produkter kan bruges online eller offline og kan købes kontant.

Ikke al pengeværdi, der gemmes elektronisk, kan betragtes som e-penge i det andet e-pengedirektivs forstand. Begrænsede netværksprodukter som f.eks. gavekort og offentlige transportkort, der kun kan bruges hos en bestemt forhandler, eller en bestemt kæde af definerede detailhandlere, falder uden for det andet e-pengedirektivs anvendelsesområde. Virtuelle valutaer som bitcoin betragtes heller ikke som e-penge, da de ikke udstedes på grundlag af modtagelse af midler.

Beskrivelse af sektoren

En systematisk undersøgelse af markedet med hensyn til mængden og værdien af e-pengetransaktioner er mere kompliceret. Den Europæiske Centralbank (ECB) fungerer som central kilde til statistiske data om værdien og omfanget af e-penge-transaktioner, men der er adskillige datahuller. Ifølge ECB skyldes dette hovedsagelig, at det kun er medlemsstater i euroområdet, der skal rapportere statistiske oplysninger, mens de resterende medlemsstater gør dette frivilligt.

Selvom eksisterende ECB-statistikker ikke giver et fuldstændigt billede af størrelsen på e-pengemarkedet, giver de nogle indikationer af størrelsesordener vedrørende markedsstørrelsen samt ændringer over tid.

Ifølge ECB-data om e-pengemarkedet i 2014 udgjorde betalingstransaktioner med e-penge for de 22 medlemsstater, der leverede data, 73 mia. EUR svarende til betalingstransaktioner med e-penge udstedt af betalingstjenesteudbydere med hjemsted i EU. Disse 73 mia. EUR omfatter 57 mia. EUR i Luxembourg (PayPal, Amazon) og 13 mia. i Italien. Antallet af transaktioner var 2,09 mia. (inklusive 1,5 mia. i Luxembourg og ca. 300 mio. i Italien). Disse data er ikke komplette, da de ikke omfatter flere markeder uden for euroområdet og derfor undervurderer EU-markedets faktiske størrelse. Den gennemsnitlige transaktionsværdi på dette grundlag var 35 EUR. E-pengebetalinger udgjorde 3% af det samlede antal elektroniske betalingstransaktioner i euroområdet (EU-18). I femårsperioden 2010-2014 steg antallet af e-pengetransaktioner i EU 2 gange og deres værdi 2,5 gange.

På baggrund af ECB's statistikker skal markedet for forudbetalte instrument i 2014 have udgjort 19,3 mia. EUR, hvoraf 13 mia. kan henføres til italienske forudbetalte kort, som i det væsentlige distribueres af et offentligt organ, *Poste Italiane*, og 3,2 mia. til markedet i Det Forenede Kongerige, som er det næststørste i EU. ECB's statistikker dækker ikke afgrænsede netværksmarkeder, herunder gavekortmarkedet. Disse kort falder imidlertid uden for rammerne for lovgivningen om bekæmpelse af hvidvask af penge og af finansiering af terrorisme på EU-plan og nationalt plan, idet anvendelsen af dem er begrænset til afgrænsede net af detailhandlere eller benzinstationer (mht. brændstofkort),

og derfor indebærer de pågældende kort beskedne risici i forhold til hvidvask af penge og finansiering af terrorisme.

Relevante aktører

Elektroniske penge kan udstedes af kreditinstitutter, institutter for elektroniske penge og postgiroinstitutioner, der i henhold til national lov har ret til at udstede elektroniske penge. E-penge kan også udstedes af Den Europæiske Centralbank og de nationale centralbanker, når de ikke handler som monetær myndighed eller anden form for offentlige myndighed. Medlemsstater og deres regionale eller lokale myndigheder kan, når de handler i deres egenskab af offentlige myndigheder, kan også udstede elektroniske penge.

Hovedparten af udstederne af e-penge har base i Det Forenede Kongerige og Belgien samt i CZ, DK, LV og NL.

Med hensyn til de forskellige forretningsmodeller anerkendes tre typer aktører i det andet e-pengedirektiv:

- udsteder: enhed, der "sælger" e-penge til kunden (det være sig en forbruger eller en virksomhed) i bytte for en betaling. Det er også den enhed, der anmoder om tilladelse til at udstede elektroniske penge, og som er reguleret af det andet e-pengedirektiv
- distributøren: en anden enhed end udstederen, der kan distribuere eller indløse e-penge på vegne af udstederen (dvs. den videresælger de e-penge, der er udstedt af udstederen, f.eks. en detailhandler, der sælger forudbetalte kort)
- agenten: enhed, der handler på vegne af udstederen af e-penge, og som gør det muligt for udstederen at udføre betalingstjenesteaktiviteter (bortset fra at udstede e-penge) i en anden medlemsstat uden at oprette en filial der.

I praksis ser denne sondring ud til af de konsulterede e-pengeudstedere at blive brugt primært i forbindelse med grænseoverskridende levering af e-pengetjenester, hvor valgte udstedere bruger "distributionspartnere" til at drive virksomhed i andre medlemsstater[39].

Beskrivelse af risikoscenariet

Lovovertrædere bruger karakteristika og funktioner i nogle af nye betalingsmetoder "direkte" ved hjælp af rigtigt anonyme produkter (dvs. uden nogen kundeidentifikation) eller "indirekte" ved at misbruge ikke-anonyme produkter (dvs. omgåelse af verifikationsforanstaltninger ved hjælp af falske eller stjålne identiteter eller ved at bruge strømænd eller proformaaktører mv.). Men sidstnævnte mulighed er bekostelig, og det er en lettere mulighed for lovovertrædere at håndtere formidlere i fordelingskanalen.

[39] Opinion of the European Banking Authority on the nature of passport notifications regarding agents and distributors under Directive (EU) 2015/2366 (PSD2), Directive 2009/110/EC (EMD2) and Directive (EU) 2015/849 (AMLD) https://eba.europa.eu/documents/10180/2622242/EBA+Opinion+.pdf

Lovovertrædere kan optanke flere kort efter modellen med anonyme forudbetalte kort. Denne optankning af mange kort kan føre til betydelige værdier, som derefter kan bruges i udlandet med begrænset sporbarhed. Det er kun når penge, der er lagret på kort, bruges, at udstedere af e-penge har chancen for at spore eller overvåge transaktioner

Trussel

Finansiering af terrorisme

E-pengeprodukter giver visse fordele frem for kontanter mht. onlinebetalinger, og brugen af disse produkter kræver ikke stor ekspertise. Når henses til de små pengebeløb, der er nødvendige til terrorangreb, kan det undertiden være lettere at betale for nogle produkter eller tjenester (hoteller, billeje) med e-pengeprodukter end med kontanter, selvom lovovertræderne skal gennem kundekendskabsprocedurer, fordi betalingerne ligger over tærsklerne. På den anden side er e-pengeprodukter lettere at spore end kontanter.

Når lovovertrædere sender penge til konfliktzoner kan e-pengeprodukter være sikrere at anvende, men at bruge dem som betalingsmiddel i disse lande kan være mere kompliceret end at bruge kontanter.

Retshåndhævende myndigheder har samlet bevis for, at e-penge, der er tanket på forudbetalte kort, er blevet brugt til at finansiere terroraktiviteter, især til at bidrage til, at terrorister kan gennemføre angreb (f.eks. hotel eller biludleje). Truslen fra at bruge forudbetalte kort eller e-pengeprodukter til dette formål er imidlertid uafhængig af behovet for at komme igennem kundekendskabsprocedurer for at få adgang til e-penge-produkter.

Sammenfattende indebærer e-pengeprodukter visse fordele for dem, der finansierer terror, sammenlignet med kontanter. Sådanne produkter giver mulighed for mere diskrete betalinger end kontanter, men de medfører ulemper, når e-pengeprodukter bruges i konfliktzoner eller for at undgå, at betalingerne kan spores. Trusselsniveauet er uafhængigt af tærsklerne for anvendelse af kundekendskabskrav, hvis lovovertræderne ikke er opført på sanktionslister.

Konklusion: e-penge, navnlig i forudbetalte kort, er attraktive for terrorgrupper, fordi det er en enkel måde at finansiere deres aktiviteter på. I betragtning af de små pengebeløb, der bruges, er det en diskret måde at foretage betalinger på. Imidlertid er kontanter stadig en foretrukken måde til at sende penge til konfliktzoner eller undgå sporbarhed. Retshåndhævende myndigheder har bevis for, at denne fremgangsmåde er blevet brugt, men truslen er uafhængig af tærsklerne for at anvende kundekendskabskrav. I denne henseende anses trusselsniveauet for terrorfinansiering i relation til e-penge for betydeligt (niveau 3).

Hvidvask af penge

Vurderingen af truslen om hvidvask af penge er knyttet til visse kontantbaserede produkter, der kan bruges af kriminelle organisationer, herunder fra steder uden for EU, gennem distributører af disse produkter. E-pengeprodukter har visse fordele i forhold til kontanter, når der er tale om at flytte pengene ud af EU eller til forskellige medlemsstater. Ikke desto mindre er kontanter stadig det foretrukne valg for disse grupper.

Finansielle efterretningsenheder har opdaget flere tilfælde af misbrug af e-penge (skattesvindel, narkotikahandel, prostitution) gennem købet af mange forudbetalte kort. Retshåndhævende myndigheder har fundet tilfælde, hvor fortjeneste fra narkotikahandel blev hvidvasket med forudbetalte kort. Med forudbetalte kort kan man muliggøre, at store beløb let kan flyttes rundt. Med da brugen af strømænd er bekostelig, når tærskler for kundekendskabskrav skal omgås og store pengebeløb skal hvidvaskes, er det lettere at bruge agenter i fordelingskanalen for e-pengeprodukter.

Konklusion: I modsætning til i forhold til finansiering af terrorisme er e-penge attraktive for kriminelle organisationer på grund af de store pengebeløb, der bruges, især når de tankes på forudbetalte kort eller værdikuponer, som er undtaget fra kundekendskabskravene, og som kan bruges online eller offline og kan købes for kontanter. På grund af de lavere tærskler er der dog brug for nogen forbindelse med e-pengeudstedernes agenter eller distributører i disses fordelingskanaler. Ikke desto mindre foretrækker kriminelle organisationer at bruge kontanter frem for e-pengeprodukter. I lyset af dette anses trusselsniveauet fra hvidvask af penge i relation til e-penge som betydeligt (niveau 3).

Sårbarhed

Finansiering af terrorisme

Vurderingen af sårbarhed over for finansiering af terrorisme i relation til e-penge har vist følgende resultater:

a) risikoeksponering

E-pengesektoren er ikke homogen, hvilket skyldes den brede vifte af produkter med vidt forskellige niveauer af finansiering af terrorisme og hvidvask af penge. Nogle e-pengeprodukter, der ikke er knyttet til en løbende konto (kontantbaserede produkter[40]), har anonym karakter på tilsvarende måde som kontanter, idet de er undtaget fra kundekendskabsprocedurer. Den iboende risiko for terrorfinansiering kan være betydelig mht. disse særlige e-pengeprodukter på grund af de små beløb, der bruges i terrorangreb, og fordi de tilbyder en diskret måde til at foretage små betalinger i sammenligning med kontanter. Ikke desto mindre betragter lovovertrædere stadig brugen af kontanter som en foretrukken mulighed på grund af den fuldstændige anonymitet.

Den iboende risiko for terrorfinansiering mht. e-pengeprodukter, der ikke er kontantbaserede, kan betragtes som svarende til den, der gælder for andre bankprodukter eller kreditkort. På trods af, at midlernes oprindelse er kendt, og at betalingernes sporbarhed er fuldstændig, kan lovovertrædere bruge disse produkter som betalingsmiddel, selvom de skal igennem kundekendskabsprocedurer. Det skyldes, at lovovertræderne for det meste ikke er omfattet af sanktionsordninger.

[40] E-pengeprodukter, der optankes kontant, ikke via en bankkonto eller et kreditkort.

Med hensyn til finansiering af terrorisme giver e-pengeprodukter en mere sikker måde til at flytte penge til konfliktzoner til terrorfinansiering, men det kan være vanskeligere at bruge de pågældende produkter som betalingsmiddel i disse områder.

Den iboende risiko afhænger hovedsagelig af produktets struktur, men selv e-pengeprodukter, der ikke er kontantbaserede, kan udgøre en betydelig risiko, hvis midlerne er lovlige, lovovertræderne ikke er på sanktionslisterne, og de pengebeløb, der er behov for, er små. Det er bemærkelsesværdigt, at økonomiske sanktioner rettes mod enkeltpersoner eller grupper, som man allerede ved, udgør en trussel, men risikoen udgår ofte fra personer, som ikke bliver opfanget af sanktionssystemet. I den henseende er den iboende risiko for terrorfinansiering uafhængig af tærsklerne eller de anvendte forholdsregler mht. kundekendskabskrav.

b) risikobevidsthed

Sektorens bevidsthed kan anses for høj, især efter nogle terrorangreb, hvor der blev brugt e-pengeprodukter. Der er dog stadig nogle bekymringer blandt tilsynsmyndighederne om, hvorvidt e-pengeselskaber, der sælger produkter med undtagelse fra kundekendskabskravene, er i stand til at gennemføre effektiv overvågning og rapportering af mistænkelige transaktioner. På den anden side har resultaterne af tematiske inspektioner i sektoren i sektoren vist et godt niveau af kontrol og risikovurdering i de inspicerede selskaber. De fleste tilsynsmyndigheder klassificerer sektorens samlede risiko som "i moderat grad betydelig" eller "betydelig".

Der er et stigende antal initiativer, der sigter mod at samarbejde med kompetente myndigheder og retshåndhævende myndigheder; dette kan bidrage til at øge risikobevidstheden i sektoren og til at forbedre effektiviteten.

c) retsgrundlag og kontroller

E-penge er omfattet af krav om bekæmpelse af hvidvask af penge og af finansiering af terrorisme på EU-plan. Ifølge det femte direktiv om bekæmpelse af hvidvask af penge er e-pengeprodukter omfattet af en undtagelsesordning, hvilket betyder, at kundekendskabskrav ikke behøver at blive opfyldt, når nærmere bestemte betingelser er opfyldt. Derudover er tærsklerne lavere end i det fjerde direktiv om bekæmpelse af hvidvask af penge, der begrænser anonymiteten af visse produkter. På den anden side kræver direktiverne, at udstedere af e-penge gennemfører tilstrækkelig overvågning af transaktionerne, for at de kan anvende undtagelserne vedrørende kundekendskabskrav.

At have effektive kontroller i relation til finansiering af terrorisme kan kræve en mange ansatte til bekæmpelse af hvidvask af penge og af finansiering af terrorisme, hvilket kan påvirke forretningsmodellen for små e-pengevirksomheder og reducere effektiviteten af deres overvågningssystemer, selv når de har gode softwareværktøjer til at overvåge transaktioner. I den henseende, dvs. når der er tale om risiko for terrorfinansiering, er kontrollernes effektivitet ikke afhængig af de gennemførte kundekendskabsprocedurer og afhænger i højere grad af kvaliteten af de undersøgte databaser, dvs. om disse kan afsløre transaktioner og kunder, der er knyttet til terrorfinansiering. Sektorens samarbejde med kompetente myndigheder og retshåndhævende myndigheder er afgørende for at forbedre effektiviteten og begrænse disse risici.

Konklusion: De lavere tærskler, der er anført i det femte direktiv om bekæmpelse af hvidvask af penge, reducerer de mest risikable produkters anonymitet og dermed sektorens sårbarhed. Risikobevidstheden er forbedret, hvilket er blevet bekræftet af nogle tilsynsmyndigheder, men der er stadig visse betænkeligheder ved effektiviteten af sektorens systemer til at overvåge og rapportere mistænkelige transaktioner med forbindelse til terrorfinansieringsaktiviteter. I denne henseende anses niveauet for sårbarhed over for terrorfinansiering i relation til e-penge for betydeligt (niveau 3).

Hvidvask af penge

Vurderingen sårbarhed over for hvidvask af penge i relation til e-penge har vist følgende resultater:

a) risikoeksponering

Blandt det store udvalg af e-pengeprodukter er de produkter, der er mest udsat for risici for hvidvask af penge, dem, der kan købes for kontanter. Brugen af disse produkter i enkelttilfælde til hvidvask af penge er bekostelig på grund af de lavere tærskler og omkostningerne ved at ansætte strømænd til at omgå tærsklerne for anvendelsen af kundekendskabskrav. Når nogle formidlere handler i fordelingskanalen for e-pengeproduktet (distributører, agenter), kan dette imidlertid være den svageste del af forebyggelsessystemet til bekæmpelse af hvidvask af penge, hvis selskaberne ikke er i stand til at gennemføre effektiv overvågning af deres distributørers net.

Lovovertrædere eller formidlere kan have en ekstern aftale med disse agenter eller distributører om at købe store beløb på forudbetalte kort og flytte disse midler til forskellige medlemsstater eller ikke-EU-lande eller endog at sælge de pågældende beløb på forudbetalte kort til tredjepart med rabat. Hvis e-pengeselskaber ikke har grundig kontrol med deres distributørs net og kan afsløre mulige useriøse distributører, vil de pågældende distributører kunne undgå at anvende kundekendskabsprocedurer korrekt og bringe falske dokumenter ind i systemet på en måde, der ligner den som forekommer med useriøse agenter for pengeoverførselsselskaber. Som følge heraf bestemmes risikoen i distributionsmodeller primært af, i hvilket omfang e-penge distribueres af andre end e-pengeudstederen.

Den iboende risiko for hvidvask af penge er betydeligt mindre for de resterende e-pengeprodukter, der er knyttet til en bankkonto eller en betalingskonto.

b) risikobevidsthed

Sektoren har tillid til brugen af teknologi til kontrol med e-pengeprodukter og vurderer, at den risiko for hvidvask af penge, som dens produkter, endog forudbetalte kort eller kontantbaserede værdikuponer, udgør, er "mindre betydelig" eller "i moderat grad betydelig". Udstederen af e-penge har på ethvert tidspunkt adgang til produktet og har ressourcerne til at deaktivere kort i tilfælde af mistænkelige transaktioner. De fleste tilsynsmyndigheder har vurderet sektorens samlede risikoprofil til at være "i moderat grad betydelig" eller "betydelig". Forskellen i opfattelse i forholdet mellem sektoren og tilsynsmyndighederne stammer hovedsagelig fra forskellige opfattelser af, i hvilket omfang e-pengeudstederes kontroller mht. bekæmpelse af hvidvask af penge og af

finansiering af terrorisme er effektive. På den anden side har tilsynsmyndigheden i en EU-medlemsstat, hvor der er udstedt mange licenser, for nylig foretaget en tematisk inspektion i sektoren og har fundet et godt niveau af kontrol og risikovurdering i de inspicerede selskaber.

c) retsgrundlag og kontroller

E-penge er omfattet af krav om bekæmpelse af hvidvask af penge og af finansiering af terrorisme på EU-plan. Ifølge det femte direktiv om bekæmpelse af hvidvask af penge er e-pengeprodukter omfattet af en undtagelsesordning, hvilket betyder, at kundekendskabskrav ikke behøver at blive opfyldt, når nærmere bestemte betingelser er opfyldt. Derudover er tærsklerne lavere end i det fjerde direktiv om bekæmpelse af hvidvask af penge, der begrænser anonymiteten af visse produkter. På den anden side kræver direktiverne, at udstedere af e-penge gennemfører tilstrækkelig overvågning af transaktionerne, for at de kan anvende undtagelserne vedrørende kundekendskabskrav.

Tilsynsmyndighederne konstaterede svagheder især mht. overvågningens effektivitet, identificering af mistænkelige transaktioner samt interne kontroller og det interne opsyn. Sektoren er dog stærkt afhængig af transaktionsovervågning som et værktøj til risikobegrænsning, hvilket omfatter effektivt opsyn med distributørernes net. Det er dog værd at bemærke, at opsyn med større distributørnetværk ud over teknologi kan nødvendiggøre ekstra personale, og at det øger sårbarheden i små e-pengeselskaber.

Konklusion: kontantbaserede e-pengeprodukter er mere sårbare end andre bankkontobaserede e-pengeprodukter på grund af det højere anonymitetsniveau. Bevidsthedsniveauet om hvidvask af penge i sektoren er højt, men der er stadig nogen tvivl blandt tilsynsmyndighederne om overvågningssystemerne, særlig i forbindelse med store distributørnetværk og kontantbaserede e-pengeprodukter. I denne henseende anses niveauet af sårbarhed over for hvidvask af penge i relation til e-penge for i moderat grad betydeligt/betydeligt (niveau 2/3).

Risikobegrænsende foranstaltninger:

Medlemsstater / kompetente myndigheder:

- gennemførelse af bestemmelserne i det femte hvidvaskdirektiv vedrørende e-penge
- tematiske inspektioner på stedet med fokus på den risiko, distributører udgør.

9. Overførsler af midler

Produkt
Overførsler af midler

Sektor
Kredit- og finansielle institutioner – penge- eller værdioverførselstjenester

Generel beskrivelse af den pågældende sektor og det/den relevante produkt/aktivitet
Pengeoverførsel defineres i det andet betalingstjenestedirektiv som en betalingstjeneste, hvor der modtages midler fra en betaler, uden at der oprettes en betalingskonto i betalerens eller betalingsmodtagerens navn, alene med det formål at overføre et tilsvarende beløb til en betalingsmodtager eller en anden betalingstjenesteudbyder på betalingsmodtagerens vegne, og/eller hvor sådanne midler modtages på betalingsmodtagerens vegne og stilles til rådighed for denne.

Et vigtigt eksempel på pengeoverførsel er de overførselstjenester, der tilbydes af store netværksagenturer (penge- eller værdioverførselssystemer), hvor betaleren giver kontanter til en betalingstjenesteudbyders agent med henblik på at stille dem til rådighed for betalingsmodtageren gennem en anden agent.

Statistikker
Pengeoverførsel er en betalingstjeneste, der kan leveres af betalingstjenesteudbydere, herunder kreditinstitutter, e-pengeinstitutter og autoriserede betalingsinstitutter. Pengeoverførsel er den betalingstjeneste, som autoriserede betalingsinstitutter oftest har tilladelse til.

I følge de generelle ECB-statistikker udgjorde det samlede beløb for overførsler sendt i 2017 fra EU's medlemsstater 270 mia. EUR, men dette tal inkluderer ikke Det Forenede Kongerige, Luxembourg, Polen, Slovakiet, Danmark, Cypern og Finland. Dette tal viser kun en mindre stigning sammenlignet med 2016 (240 mia. EUR).

Markedslandskabet viser, at der findes forskellige typer udbydere af penge- eller værdioverførselstjenester. Dette fremgår af direktivet om betalingstjenester, der indeholder bestemmelser om "registrerede penge- eller værdioverførselstjenester" og "autoriserede penge- eller værdioverførselstjenester".

Beskrivelse af risikoscenariet

Finansiering af terrorisme

Lovovertrædere bruger finansielle institutioner penge- eller værdioverførselstjenester til at placere og/eller overføre midler, der foreligger kontant eller i anonyme e-penge (ikke-kontobaserede transaktioner). De bruger penge- eller værdioverførselstjenester til hurtigt at overføre beløb til forskellige lande og foretrækker normalt en lang række transaktioner med lav værdi for at undgå, at viser sig faresignaler.

Hvidvask af penge

Lovovertrædere kan bruge penge- eller værdioverførselstjenester til at gennemføre en række ulovlige aktiviteter. De er opregnet nedenfor.

- Overførsel af penge fra legitime og illegitime kunder. Useriøse agenter udfører normalt transaktioner ved hjælp af falske ID'er og falske fakturaer.
- Udbytte af kriminalitet hvidvaskes gennem afviklingssystemer i et land uden for EU (ved brug af pas). Udbydere af penge- eller værdioverførselstjenester kanaliserer midler gennem meget komplekse betalingskæder med et stort antal mellemled og lande i betalingskredsløbet, hvorved sporbarheden af de ulovlige midler vanskeliggøres. Udbydere af penge- eller værdioverførselstjenester, der opererer langs betalingskæden, etablerer ofte formelle og/eller uformelle afviklingssystemer (ofte sammen med handelsbaserede teknikker til pengehvidvask), hvilket også vanskeliggør sporbarhed af ulovlige midler.
- Store pengesummer opdeles i mindre beløb, der ligger under de tærskler, for hvilke der kræves skærpet kundeidentifikation.
- Udbytte fra kriminalitet placeres i det finansielle system gennem en lovreguleret penge- eller værdioverførselstjeneste, der tilbyder betalingskonti eller lignende produkter. Lovovertrædere kan også bruge de pågældende lovregulerede udbydere af penge- eller værdioverførselstjenester til at kanalisere deres midler.
- Midler placeres og/eller overføres via pengeoverførselstjenester. Risikoen for hvidvask af penge/finansiering af terrorisme kan være særlig stor, når midler, der skal overføres, modtages kontant eller i anonyme e-penge.

Trussel

Finansiering af terrorisme

Vurderingen af truslen om terrorfinansiering i relation til penge- eller værdioverførselstjenester viser, at terrorgrupper gennemgående bruger denne metode. Retshåndhævende myndigheder og finansielle efterretningsenheder har indsamlet stærke beviser for, at disse tjenester bruges til at modtage og overføre midler, der bruges til at støtte finansieringen af terroraktiviteter i EU og navnlig til at overføre midler fra/til udenlandske terrorkrigere, der rejser til/fra konfliktzoner.

Udbydere af penge- eller værdioverførselstjenester er, afhængigt af deres organisation, lette at få adgang til, og terrorister behøver ikke særlig ekspertise eller teknikker for at misbruge denne tjeneste til finansiering af terroraktiviteter. Terrorister kan muligvis være mere tiltrukket af store udbydere af penge- eller værdioverførselstjenester på grund af deres globale net af agenter, mens mindre udbydere af penge- eller værdioverførselstjenester måske ikke er så attraktive, da de sædvanligvis driver virksomhed i et begrænset antal lande. De særlige karakteristika hos udbydere af penge- eller værdioverførselstjenester (se sårbarhedsafsnit) betyder, at de opfattes som attraktive og sikre.

Konklusion: Udbydere af penge- eller værdioverførselstjenester bruges ofte til at finansiere terroraktiviteter og behøver ikke særlig viden eller planlægning. I lyset af dette anses trusselsniveauet for finansiering af terrorisme i relation til penge- eller værdioverførselstjenester for meget betydeligt (niveau 4).

Hvidvask af penge

Organiserede kriminelle grupperinger bruger gennemgående denne metode. Retshåndhævende myndigheder og finansielle efterretningsenheder har samlet stærke beviser for, at disse tjenester bruges til at modtage og overføre midler, der bruges til at understøtte hvidvask af penge. Udbydere af penge- eller værdioverførselstjenester er, afhængigt af deres organisation, lette at få adgang til, og der behøves ikke særlig ekspertise eller særlige teknikker for at misbruge denne tjeneste til at hvidvaske udbyttet af kriminalitet. De særlige karakteristika hos udbydere af penge- eller værdioverførselstjenester betyder, at de opfattes som attraktive og sikre. Sædvanligvis tager lovovertrædere kontakt til agenter med henblik på at hvidvaske penge fra en organiseret kriminel gruppering til gengæld for en procentdel af det pengebeløb, der hvidvaskes. Agenter, der er knyttet til disse lovovertrædere, gennemfører sædvanligvis falske transaktioner med falske kunde-ID'er, hvis de er opmærksomme på svage kundekendskabskrav hos den virksomhed, der udbyder penge- eller værdioverførselstjenester. Ellers kan de bruge reelle kundeformularer til at tilføje nye transaktioner.

På grundlag af princippet om ikke-eksklusivitet kan agenter arbejde for forskellige virksomheder samtidig. Dette betyder, at når de er forbundet med lovovertrædere, kan agenter let opdele transaktioner mellem virksomheder med henblik på at hvidvaske store beløb; sådanne aktiviteter er vanskelige at afsløre for de enkelte virksomheder og kompetente myndigheder.

Konklusion: Udbydere af penge- eller værdioverførselstjenester bruges ofte til at hvidvaske penge, og der behøves ikke særlig viden eller planlægning. I lyset af dette anses trusselsniveauet over hvidvask af penge i relation til penge- eller værdioverførselstjenester som meget betydeligt (niveau 4).

Sårbarhed

Finansiering af terrorisme

a) risikoeksponering

Brugen af kontantbaserede transaktioner og den gennemgående brug af disse tjenester i områder med høj risiko fører til en høj risikoeksponering. Når penge bruges til terrorangreb i EU, er der en højere generel risiko ved forsendelsen af små beløb fra betalere, der ikke er opført på sanktionslister.

Sektoren er sårbar over for grænseoverskridende misbrug til terrorfinansieringsformål. Retshåndhævende myndigheders efterforskning efter nylige terrorangreb i for eksempel Paris og Det Forenede Kongerige har bekræftet, at terrorister brugte pengeoverførsel til at skaffe og flytte midler. I modsætning til pengehvidvaskere søger personer, der vil

finansiere terrorisme ikke nødvendigvis at skjule deres identitet og kan bruge lovlige finansieringskilder, ofte med små beløb. Hertil kommer, at risikoen fra terrorfinansiering ofte udgår fra personer, som ikke bliver opfanget af sanktionssystemet.

Den betydelige risiko for hvidvask af penge og finansiering af terrorisme i sektoren for penge- eller værdioverførselstjenester har ført til, at bankerne har gennemført retningslinjer for nedbringelse af risikoen i forhold til pengeoverførselstjenester i visse regioner med højere risiko. Denne tendens giver anledning til bekymring, da nedbringelse af risikoen i sidste ende kan føre til, at pengeoverførselstjenester presses til at gå under jorden (dvs. uformelle tjenesteudbydere som hawala-tjenester). Der opstår også problemer med økonomisk inklusion, idet pengeoverførselstjenester spiller en vigtig rolle for kunder, der har begrænset eller ingen adgang til andre regulerede finansielle tjenester.

b) risikobevidsthed

Ifølge de kompetente myndigheder er risikobevidstheden i sektoren høj (på grund af de nylige terrorangreb), men de forholdsregler, virksomhederne har truffet med henblik på at at identificere deres kunder og verificere deres identiteter, vejer muligvis ikke så tungt i forbindelse med bekæmpelse af terrorfinansiering som effektiv løbende overvågning af transaktioner. Retshåndhævende myndigheder anfører, at de større spillere oftere misbruges af terrorister end de mindre på grund af deres større agentnet i forskellige lande.

Kampen mod finansiering af terrorisme er fortsat hæmmet, når virksomheder ikke har adgang til relevant information, som de retshåndhævende myndigheder ofte ligger inde med, og som ville bidrage til, at de kunne identificere risici for terrorfinansiering, før de bliver til virkelighed. Tilsvarende kan de retshåndhævende myndigheders bestræbelser på at forpurre terroristernes aktiviteter og net blive vanskeliggjort, når de ikke er i stand til at indhente oplysninger om finansielle strømme, som kun virksomheder kan give.

Størstedelen af tilsynsmyndighederne anser den samlede risikoprofil for sektoren for at være betydelig eller meget betydelig, og mere end 50% af virksomhederne i sektoren vurderes til at udgøre en meget betydelig risiko.

c) retsgrundlag og kontroller

Registrerede og autoriserede udbydere af penge- eller værdioverførselstjenester er omfattet af krav om bekæmpelse af hvidvask af penge og af finansiering af terrorisme på EU-niveau. Tilsynsmyndighederne anser effektiviteten af de eksisterende kontroller som i alt væsentligt ringe. Virksomheder i sektoren, især store virksomheder, er afhængige af deres kundekontroller og varslingssystemer for at begrænse risiciene.

Effektiviteten af de nuværende systemer i forhold til at afsløre mistænkelige transaktioner i tilknytning til finansiering af terrorisme er ikke stor, selvom de er personaleintensive. Som den iboende risiko udgår risikoen fra terrorfinansiering ofte fra personer, som ikke bliver opfanget af sanktionssystemet. Resultatet er, at der er behov for tættere samarbejde mellem virksomhederne og de retshåndhævende myndigheder, så de bliver mere effektive til at finde kunder, der er involveret i terrorhandlinger.

Konklusion: Sårbarheden over for terrorfinansiering i relation til penge- eller værdioverførselstjenester er høj. Det skyldes, at de transaktionerne i tilknytning til terrorfinansiering har karakteristika, som ikke er lette af afsløre, på trods af de menneskelige og tekniske ressourcer, virksomhederne lægger i det. Effektiviteten af kontrollen afhænger af de informationskilder, der bruges til at kontrollere transaktioner og kunder. Det er nødvendigt, at virksomheder og retshåndhævende myndigheder forbedrer udvekslingen af oplysninger til at styrke afsløringen af mistænkelige transaktioner i tilknytning til finansiering af terrorisme. I lyset af dette anses sårbarhedsniveauet for finansiering af terrorisme i relation til penge- eller værdioverførselstjenester for betydeligt/meget betydeligt (niveau 3/ 4).

Hvidvask af penge

Sårbarhed over for hvidvask af penge i relation til penge- eller værdioverførselstjenester kan ikke vurderes uden hensyntagen til, at de fleste udbydere af penge- eller værdioverførselstjenester benytter agenter. Agenter udgør derfor hovedfaktoren i risikoeksponering i forhold til udbydere af penge- eller værdioverførselstjenester.

a) risikoeksponering

Penge- eller værdioverførselstjenester er i nogle tilfælde kontantbaserede og gør det muligt at foretage hurtige transaktioner. På grund af deres særlige karakteristika og navnlig det forhold, at de benytter agenter, kan penge- eller værdioverførselstjenester leveres i højrisikolande uden for EU og kan bruges af højrisikokunder, som burde være underlagt konkret tilsyn og kontrol. Derfor er de mest fremherskende risici i sektoren for penge- eller værdioverførselstjenester deres kontantintensive karakter, overførslernes høj hastighed og store volumen, (selvom de enkelte transaktioner sædvanligvis er små) samt overførslerne til højrisikoområder.

At gennemføre konsekvente kundekendskabsprocedurer kan være problematisk på grund af karakteren af kunderne, der sædvanligvis gennemfører enkeltstående transaktioner, og pga. risikoen for, at der vil blive brugt stråmænd til at gennemføre transaktionerne (selvom dette er en dyrere metode at hvidvaske penge på). Men den iboende risiko er større, når pengeoverførselsvirksomheder ikke har grundige overvågningssystemer til at kontrollere detailagenternes net, især i virksomheder med store net af detailagenter.

Den betydelige risiko for hvidvask af penge og finansiering af terrorisme i sektoren for penge- eller værdioverførselstjenester har navnlig ført til, at bankerne har gennemført retningslinjer for nedbringelse af risikoen i forhold til pengeoverførselstjenester i visse regioner med højere risiko. Denne tendens giver anledning til bekymring, da nedbringelse af risikoen i sidste ende kan føre til, at pengeoverførselstjenester presses til at gå under jorden (dvs. til uformelle tjenesteudbydere som hawala-tjenester). Der opstår også problemer med økonomisk inklusion, idet pengeoverførselstjenester spiller en vigtig rolle for kunder, der har begrænset eller ingen adgang til andre regulerede finansielle tjenester.

b) risikobevidsthed

Risikobevidstheden kan anses for høj i sektoren. Kontrollerne er generelt effektive, når de er fokuseret på kunderisiko, men for så vidt angår risikoen for hvidvask af penge

hidrørende fra useriøse agenter er kontrollerne ikke så effektive rundt omkring i EU. Endvidere har visse lande tærskler for kundekendskabskrav, der gør det vanskeligere at holde ordentligt opsyn med agenter. I den henseende er det også værd at bemærke, at sektoren er meget konkurrencepræget, og at der er lave avancer, således at der somme tider bliver tale om et kompromis mellem rentabilitet og regeloverholdelse. Agenter, der har forbindelse til hvidvask af penge er sædvanligvis de mest profitable. Hvis således virksomhederne ikke er i stand til at påvise en klar forbindelse med de pågældende aktiviteter, foretrækker de at beholde agenten i deres net, men under opsyn (og almindeligvis fastsættes kvantitative lofter for deres transaktioner), i stedet for at indberette agenten til den finansielle efterretningsenhed og dermed afbryde forretningsforbindelsen.

Tilsynsmyndighedernes bevidsthed om de pågældende risici er høj. I deres risikovurderinger har nogle tilsynsmyndigheder nævnt de følgende risici, der er forbundet med agentnet: utilstrækkelig styring, uddannelse og overvågning af agenter. I modsætning hertil opfatter de fleste tilsynsmyndigheder branchens bevidsthed som ringe eller meget ringe.

Indberetningen af mistænkelige transaktioner til finansielle efterretningsenheder er ikke altid effektiv, hvis virksomhederne rapporterer store mængder af enkeltstående kundetransaktioner i stedet for at rapportere agenter eller grupper af agenter, der gennemfører disse transaktioner.

c) retsgrundlag og kontroller

Registrerede og autoriserede udbydere af penge- eller værdioverførselstjenester er omfattet af krav om bekæmpelse af hvidvask af penge og af finansiering af terrorisme på EU-niveau. På grund af den udbredte brug af agenter er tilsyn med sektoren en stor udfordring. Virksomhederne bruger nye teknologier og software til at gennemføre grundige kundekendskabskrav og agentkundekontrol, men på grund af de særlige karakteristika ved deres kunder er de pågældende foranstaltninger er ikke altid effektive. Udbydere af penge- eller værdioverførselstjenester har brug for uddannelse for at kunne gennemføre kundekendskabskravene ordenligt, men uddannelsen har ingen effekt, når der er tale om at håndtere den risiko, useriøse agenter udgør.

I øjeblikket virker det grænseoverskridende samarbejde ikke ordenligt, og tilsynsmyndighederne er ikke i stand til at gennemføre passende kontrolforanstaltninger og et passende sanktionssystem. Men et af målene for det fjerde og det femte hvidvaskdirektiv er netop at styrke samarbejdet mellem tilsynsmyndigheder inden for bekæmpelse af hvidvask af penge. På baggrund heraf kan oprettelsen af et "kollegium af tilsynsmyndigheder for bekæmpelse af hvidvask af penge", når forpligtede enheder opererer i forskellige lande, forbedre tilsynet i EU.

Konklusion: Den iboende risiko er høj, men risikobevidstheden i virksomhederne er voksende. Tilsynsmyndigheder og virksomheder tager sig af risikoen for hvidvask af penge, fokuserer deres indsats på områder med højere sårbarhed, herunder opsyn med agenter. Men for at mindske sårbarheden er der stadig behov for visse forbedringer, f.eks. forbedret tilsynssamarbejde og mere effektivt gennemførte kundekendskabskrav og opsyn med agenter. I denne henseende anses sårbarhedsniveauet for hvidvask af penge i relation til penge- eller værdioverførselstjenester for betydeligt (niveau 3).

Risikobegrænsende foranstaltninger:

Medlemsstater / kompetente myndigheder:

- Medlemsstaterne bør fjerne tærskler for lejlighedsvise transaktioner og gennemføre kundekendskabskrav for alle transaktioner, således at virksomheder, der driver penge- eller værdioverførselstjenester, effektivt kan overvåge og afsløre mistænkelige transaktioner og mistænkelige agenter knyttet til hvidvask af penge.
- Etablere og støtte et system, hvor mistænkelige agenter, der indberettes af virksomheder, som driver penge- eller værdioverførselstjenester, registreres i en database, hvortil alle virksomheder i sektoren har adgang. Dette vil begrænse eller eliminere mistænkelige agenters aktiviteter.
- Kompetente myndigheder bør foretage et antal tematiske inspektioner på stedet med fokus på de risici, agenter udgør. Omfanget af disse tematiske inspektioner bør omfatte kontrol af, at selskaber, der driver penge- eller værdioverførselstjenester, har en dækkende funktion vedrørende tilsyn med agenter, herunder effektive overvågningssystemer, revisioner på stedet og uddannelse.

De europæiske tilsynsmyndigheder:

- Tilskynde kompetente myndigheder til at afsætte passende ressourcer, der står i forhold til risikoniveauet, til inspektioner af penge- eller værdioverførselstjenester med fokus på opsyn med agenter.

Kommissionen:

Fremme samarbejdet mellem retshåndhævende myndigheder og finansielle institutioner med henblik på at øge effektiviteten af alarmsystemer for terrorfinansiering på supranationalt niveau.

10. Ulovlige overførsler af midler – hawala

Produkt
Ulovlig/uformel overførsel af midler gennem hawala

Generel beskrivelse

Hawala er et system af pengeoverførselstjenester, som sørger for overførsel og modtagelse af penge eller tilsvarende værdier. Det hviler ofte på bånd inden for bestemte geografiske områder eller etniske befolkningsgrupper. Disse bevægelser af værdier kan afvikles gennem handel eller kontantbaserede virksomheder, der deltager i overførselsaktiviteter. De drives ofte i områder med befolkningsgrupper, der bor i udlandet. *Hawaladarer* (de, der driver hawala-virksomhed) driver ofte parallelle forretninger, især med valutaveksling, rejsebureauer eller telefonbutikker, eller arbejder endda som agenter for officielle udbydere af pengeoverførsler. Udtrykket hawala bruges ofte til at beskrive en række forskellige uformelle værdioverførselssystemer, som har ensartede egenskaber og fungerer på samme måde, selvom de ikke er hawala i snæver forstand. Sådanne pengeoverførsler betragtes som uregulerede betalingstjenester i EU, hvilket betyder at de er ulovlige i EU. Uformelle værdioverførselssystemer som *Hawala* kan bruges til lovlige formål som pengeoverførsler, men også med ulovlige formål.

I 2013 fremkom Den Finansielle Aktionsgruppe (FATF) med det bredere begreb "Hawala og andre lignende tjenesteydere" eller "HOSSP'er" for at beskrive denne aktivitet. HOSSP'er er en underafdeling af de uformelle værdioverførselstjenester. Andre former end hawala omfatter hundi, kinesisk uofficiel bankvirksomhed og Black Market Peso Exchange (konvertering af peso på det sorte marked). Uformelle værdioverførselssystemer drejer sig om flytning af værdi, uden at der er behov for, at penge bliver flyttet fysisk eller elektronisk.

Medlemmer af diasporaer og migrantsamfund bruger vid udstrækning HOSSP'er til at sende legitime pengeoverførsler til deres oprindelseslande. Samtidig har gennemførelsen af strengere regler til bekæmpelse af hvidvask af penge i de almindelige finansieringsinstitutter også i tiltagende grad gjort uformelle værdioverførselssystemer og HOSSP'er tillokkende for organiserede kriminelle grupperinger, der ofte bruger dem til ulovlige overførsler, dvs. til at overføre store beløb i udbytte fra lovovertrædelser eller til at hvidvaske kriminelle udbytter og derved skabe slørings- og overførselstjenester i og uden for EU.

Hawala-betalinger er uformelle pengeoverførsler, der foretages uden at inddrage autoriserede finansielle institutioner. I princippet flytter pengene sig ikke fysisk fra betaleren til betalingsmodtageren. I stedet, som det også ofte sker i forbindelse med pengeoverførsler, gøres dette ved at modregne saldoen mellem betalerens hawaladar og betalingsmodtagerens hawaladar. Til illustration af denne metode: en hawaladar fra land A (HA) modtager et beløb i én valuta fra betaleren og giver til gengæld betaleren en kode til brug for identifikation. Han instruerer derpå sin korrespondent i land B (HB) om at udbetale et tilsvarende beløb i lokal valuta til en udpeget modtager, der skal oplyse koden for at kunne modtage pengene. Efter overførslen har HA en gæld til HB, og afviklingen af

deres mellemværender sker på forskellige måder, enten økonomisk eller med varer og tjenesteydelser.

Ifølge reglerne burde alle operatører, der udbyder betalingstjenester som defineret i bilag I, nr. 6, i det andet direktiv om betalingstjenester (PSD2), være behørigt registreret og under tilsyn. Disse udbydere burde søge status som autoriserede betalingsinstitutter. Den seneste og betydelige indsats fra retshåndhævende myndigheders side har ud over enhver tvivl bevist, at den uregulerede og hemmelige karakter af HOSSP'ers uformelle overførselssystemer har gjort dem til det foretrukne valg for kriminelle mht. hvidvask af penge.

Selvom hawaladarer skal registreres og have behørig tilladelse i henhold til betalingstjenestedirektivet, vælger disse udbydere af betalingstjenester ofte at gennemføre de pågældende overførsler ulovligt, uden om det konventionelle banksystem og uden korrekt tilladelse. Det betyder, at de omgår deres forpligtelser til bekæmpelse af hvidvask af penge og undgår obligatorisk tilsyn efter forordningerne om bekæmpelse af hvidvask af penge. Myndighederne savner ofte midlerne til at afsløre disse net og håndhæve anvendelsen af PSD2 og forpligtelserne til bekæmpelse af hvidvask af penge over for disse udbydere.

Beskrivelse af risikoscenariet

I modsætning til alle andre overførselssystemer bygger hawala på et net af nøgleaktører (hawaladarer) bundet sammen af tillid som følge af tilhørsforholdet til særlige geografiske områder, familier, stammer, etniske grupper, nationaliteter, forretningsaktiviteter osv. Hawaladarer afviklinger transaktioner indbyrdes over lang tid ved nettoafvikling vha. bankkanaler, handel eller kontanter. Det betyder, at i modsætning til alle andre overførselssystemer overføres der ikke penge for hver enkelt transaktion. I stedet bruger de hver dag en lokal kontantpulje med penge, som allerede var i systemet, til at betale modtageren. Efter en given periode (normalt efter 2-3 måneder) er det kun et eventuelt nettobeløb, der afregnes. Hawaladarer samler måneders modtagne midler fra individuelle afsendere og foretager derefter afvikling. Det skal understreges, at lovlige værdioverførselstjenester med tilladelse sædvanligvis også fungerer på denne måde.

Hawalanettet bruger også visse unikke teknikker:

- bilateral afvikling: "omvendt hawala" mellem to hawaladarer
- multilateral afvikling: "trekantet", "firkantet" eller andre arrangementer mellem flere hawaladarer i samme net
- afvikling af værdi gennem handelstransaktioner, sædvanligvis under anvendelse af handelsbaserede teknikker til hvidvask af penge (forsendelse af tilsvarende værdi gennem handelstransaktioner, f.eks. varer, betaling af en gældspost eller faktura med samme værdi, som de skylder. Overfakturering eller underfakturering. Dobbelt fakturering. Black Market Peso Exchange (konvertering af peso på det sorte marked mv.)
- kontant afvikling via pengekurerer over grænserne, bank- og pengeforretningskanaler.

Der er skabt særlige hawala-net til udelukkende at imødekomme kriminelle behov; de placerer og slører kriminelle penge og betaler efter anmodning modværdien andre steder i verden. Disse net er kendt for at anvende de teknikker, der er beskrevet ovenfor. For at beskytte sig selv bruger hawala-net herudover følgende teknikker:

- hurtige kontantpick-ups
- autentificering via et tegn (et fast bestanddel af kriminelle kontantoverleveringer er brugen af det unikke serienummer på en pengeseddel, der fungerer som et middel til identifikation og en rudimentær kvittering for overleveringen)
    - placering via cuckoo smølfing (en form for hvidvask af penge knyttet til alternative overførselssystemer, hvor kriminelle midler overføres via konti tilhørende uvidende personer, der forventer lovlige midler eller betalinger fra udlandet).

Alle disse teknikker er særlige for hawala-systemet og er allesammen kendte fareindikatorer for hawala-aktiviteter for EU's retshåndhævende myndigheder.

Sådanne kriminelle hawala-net følger også en særlig struktur, der består af:

- controllers eller vekselerer — de indgår aftalen med organiserede kriminelle grupperinger om modtagelse af ulovlige kontanter og leveringen af værdien af dem på en valgt destination.
- koordinatorer — de er formidlere, der arbejder for controlleren med at styre og lede forskellige opsamlere
- opsamlere — de samler ulovlige kontanter fra kriminelle og skaffer dem af vejen
- afsendere — modtager og afsender de penge, opsamleren har modtaget (sædvanligvis en, der driver pengeforretninger).

Trussel

Omfanget af *Hawala* i EU er ukendt.

Det vides, at *Hawala* er knyttet til visse forretningsvirksomheder blandt visse etniske grupper (Indien, Afghanistan, Pakistan, Iran, Forenede Arabiske Emirater, Somalia og Kina), som er almindelige i EU. Eksempler på den type forretning, der er tale om, er rejsebureauvirksomhed, pantelånere, mobiltelefon- og SIM-kortsalg, toptankning af mobilkort, købmandsbutikker, import-/eksportforretninger samt forskellige forretninger af nabolagstypen som neglesaloner, frisører, skønhedssaloner, blomsterbutikker.

Europol er også bekendt med flere verserende undersøgelser af hvidvask i mange millioner euro-klassen med fokus på kriminelle *Hawala*.

Der er ingen direkte penge/værdistrømme mellem afsender og modtager, som retshåndhævende myndigheder kan følge eller spore. Dette gør det nærmest muligt at spore penge-/værdistrømmen i et hawala-net, selv hvis regnskaberne bliver beslaglagt — de er sædvanligvis krypteret, og oftere og oftere befinder de sig på cloud-servere placeret i lande, der ikke er samarbejdsvillige. Denne uigennemsigtighed gør det attraktivt for lovovertræderne.

Retshåndhævende myndigheder har afsløret en overlapning mellem officielle og uformelle værdioverførselssystemer, bl.a. gennem "cuckoo smølfing". Til gengæld kan *hawaladarer* hvidvaske store summer i kontanter fra forskellige typer udbytte af kriminalitet (f.eks. narkotikahandel, skatteunddragelse, terrorfinansiering mv.). En opsamler/hawaladar modtager kommission med fra 2 % til 10 %.

Sårbarhed

Sådanne pengeoverførsler betragtes som uregulerede betalingstjenester i EU, hvilket betyder at de er ulovlige i EU. Der er ingen konkret vurdering af sårbarhed over for ulovlige tjenesteydelser i forbindelse med den supranationale risikovurderingsrapport.

Risikobegrænsende foranstaltninger:

Medlemsstater / kompetente myndigheder:

- Oprette fælles efterretningstaskforce vedrørende hvidvask af penge. Sikre samarbejdet mellem den finansielle sektor og offentlige institutioner om udveksling af efterretningsoplysninger for at forhindre hvidvask af penge (som også kan udvides til at gælde hawala-tjenester).
- Gennemføre tilsynstiltag for at kontrollere, at forpligtede enheder, navnlig pengeoverførselsvirksomheder, har indført kontroller til afsløring af hawaladarer, som bruger registrerede agenter som camouflage med henblik på at tiltrække kunder for at tilbyde dem hawala.

11. Betalingstjenester

Produkt
Betalingstjenester

Sektor
Kredit- og finanssektoren

Generel beskrivelse af den pågældende sektor og det/den relevante produkt/aktivitet

Betalingstjenesteprodukter

Betalingstjenester reguleres af det reviderede direktiv om betalingstjenester (2015/2366). De er opført i bilag I til det andet betalingstjenestedirektiv og dækker en bred vifte af tjenester, herunder:

- tjenester, der muliggør, at kontantbeløb indsættes på eller hæves fra en betalingskonto (kontante indskud behandles i et særskilt afsnit i denne rapport)

- pengeoverførselsvirksomhed (også dækket i et særskilt afsnit i denne rapport)

- gennemførelse af betalingstransaktioner, herunder kreditoverførsler eller direkte debiteringer

- gennemførelse af betalingstransaktioner via betalingskort eller lignende anordninger

- udstedelse af betalingsinstrumenter

- indløsning af betalingstransaktioner.

En "betalingstransaktion" er defineret som en handling, der initieres af en betaler eller på dennes vegne eller af en betalingsmodtager med henblik på at indbetale, overføre eller hæve midler uden hensyn til eventuelle underliggende forpligtelser mellem betaleren og betalingsmodtageren

Det andet betalingstjenestedirektiv omfatter yderligere betalingstjenester, som er opstået i de seneste år i slipstrømmen af digitaliseringen af tjenesterne. Disse tjenester betegnes betalingsinitieringstjenester og kontooplysningstjenester. I forbindelse med vurderingen af den relevante risiko for hvidvask, er det kun betalingsinitieringstjenester der er relevante.

Betalingsinitieringstjenester giver forbrugerne mulighed for at betale for deres køb af en kreditoverførsel i stedet for en kreditkortbetaling (ca. 60 % af EU's befolkning har ikke noget kreditkort). Betalingsinitieringstjenesten kan kontrollere, om der er tilstrækkelige midler på kundens konto til at gennemføre betalingen. Den oplyser den handlende om, at betalingsordren er blevet iværksat. På den baggrund kan den webhandlende eventuelt beslutte at afsende varen eller levere tjenesteydelsen, før beløbet er bogført på hans konto. Det andet betalingstjenestedirektiv dækker disse nye betalinger og beskæftiger sig med

potentielle problemer med fortrolighed, ansvar og sikkerhed i forbindelse med sådanne transaktioner.

Det andet betalingstjenestedirektiv fandt anvendelse fra den 13. januar 2018. Pr. 8. februar 2019 havde 25 medlemsstater givet underretning om fuldstændig gennemførelse af direktivet, to (Malta og Spanien) om delvis gennemførelse, og i Rumænien er direktivet endnu ikke blevet gennemført.

Det andet betalingstjenestedirektiv regulerer ikke alle betalinger. Betalinger med kontanter eller betaling med papircheck er ikke omfattet. Betalingstransaktioner gennemført af en udbyder af elektroniske kommunikationsnetværk under en vis værdi er også undtaget fra direktivets anvendelsesområde.

Langt størstedelen af betalingerne foregår elektronisk. Det samlede antal ikke-kontante betalinger i EU steg med 7,9 % til 134 mia. EUR i 2017 sammenlignet med året før:

- betalinger med kredit- og debetkort udgjorde 52 % af alle transaktioner
- kreditoverførsler udgjorde 24 % og direkte debiteringer 19 %
- antallet af kreditoverførsler steg med 5,5 % til 32,1 mia. EUR

Antallet af kort med en betalingsfunktion i EU steg i 2017 med 2,0 % til 812 mio. Med en samlet EU-befolkning på 513 millioner svarede dette til ca. 1,6 betalingskort EU pr. indbygger. Antallet af transaktioner steg med 11,2 % til 69,2 milliarder euro, hvilket svarer til en samlet værdi af 3,1 billion EUR. Det svarer til en gennemsnitsværdi på omkring 44 EUR pr. korttransaktion.

SEPA

Det fælles eurobetalingsområde (SEPA) har til formål at harmonisere og integrere betalingmarkederne i Europa med ét sæt betalingsinstrumenter i EUR: kreditoverførsler, direkte debiteringer og betalingskort, fælles standarder og praksis samt et harmoniseret retsgrundlag. SEPA dækker mere end 520 millioner mennesker i 28 EU-medlemsstater og seks ikke-EU-lande (Island, Liechtenstein, Monaco, Norge, San Marino og Schweiz).

Detailbetalingssystemer

Detailbetalingssystemer i EU tager sig af betalinger, der foretages af offentligheden, med en relativt lav værdi, høj volumen og begrænset tidskritikalitet. I 2017 fandtes der 43 detailbetalingssystemer i EU som helhed. I det pågældende år blev omkring 57 mia. transaktioner behandlet af de pågældende systemer, hvilket omfattede 44,0 billioner EUR. Ca. 22 af disse systemer er placeret i euroområdet, hvor de behandlede næsten 42 mia. transaktioner i 2017 (dvs. 73 % af det samlede antal i EU), hvilket omfattede en værdi på 31,6 billioner EUR (dvs. 72 % af det samlede beløb i EU).

Betalingssystemer for store betalinger

Betalingssystemer for store betalinger er primært udformet med henblik på at behandle hastende eller værdimæssigt store interbankbetalinger, men nogle af dem kan også afvikle en stor mængde detailbetalinger. I løbet af 2017 afviklede 12 systemer 842 millioner

betalinger til en samlet værdi af 702 billioner EUR i EU. De to største systemer til store betalinger i euroområdet (TARGET2 og EURO1/STEP1) afviklede 143 millioner transaktioner til et beløb af 528 billioner EUR i 2017, dvs. 75 % af den samlede værdi.

Udbydere af betalingstjenester

Bankerne er aktører i de nationale og internationale betalingssystemer. Der blev i 2016 på EU-28 niveau foretaget ca. 122 milliarder kontantfrie betalinger af ikke-monetære finansielle institutioner. Mere end halvdelen (60 mia. EUR) af disse var kortbetalinger, mens ca. en fjerdedel var pengeoverførsler (31 mia.) eller betalingsservice (25 mia.).

I EU er det ikke kun kreditinstitutter, der har tilladelse til at udbyde betalingstjenester. De kan også udbydes af e-pengeinstitutter og postgirokontorer samt regionale eller lokale myndigheder, hvor de ikke handler i deres egenskab af offentlige myndigheder. Hertil kommer, at med vedtagelsen af det første direktiv om betalingstjenester i 2007 blev der indført en ny enhed, "betalingsinstitutter". Disse kan kun udbyde betalingstjenester; de må ikke tage mod indlån eller udstede e penge. I det andet betalingstjenestedirektiv blev der indført nye kategorier af betalingstjenesteudbydere, nemlig udbydere af betalingsinitieringstjenester og kontooplysningstjenester. De kan alene levere hhv. betalingsinitieringstjenester og kontooplysningstjenester.

Indførelsen af betalingsinstitutter har siden 2009 øget konkurrencen på betalingsmarkedet.

Flertallet af betalingstjenesteudbydere består stadig af kreditinstitutter.

Hvad angår de mindre aktører var der i hele EU (status i 2012):

- 568 autoriserede betalingsinstitutter
- 2.203 små betalingsinstitutter (betalingsinstitutter, som kun har lov til at yde betalingstjenester i det land, hvor de har fået en tilladelse), og
- 71 e-pengeinstitutter.

Fordelingen af betalingsinstitutter (autoriserede betalingsinstitutter og små betalingsinstitutter) er stærkt koncentreret, i begge tilfælde tegner nogle få lande sig for langt størstedelen af disse institutter i EØS. Det Forende Kongerige tegner sig for 39,4 % af alle autoriserede betalingsinstitutter i EØS, og Det Forenede Kongerige tegner sig sammen med Spanien (8,1 %), Italien (7,9 %), Tyskland (6,5 %), Nederlandene (4,9 %) og Sverige (4,3 %), for 71 % af alle autoriserede betalingsinstitutter i EØS. Hvad angår små betalingsinstitutter var 44,8 % registreret i Polen og 43,6 % var registreret i Det Forenede Kongerige. Det Forenede Kongerige tegnede sig også for 42,2 % af alle e-pengeinstitutter i EØS.

Flere generelle oplysninger om antallet af finansielle institutioner, der udbyder betalingstjenester i EU findes i ECB betalingsbalancestatistikken rapport 2017: http://sdw.ecb.europa.eu/servlet/desis?node=1000001384.

Beskrivelse af risikoscenariet

Lovovertrædere benytter banksystemet og det finansielle system til kanalisering af deres midler gennem bankkonti, kredit- og debetoverførsler, (peer-to-peer) mobilbetalinger og internetbaserede betalingstjenester.

Trussel

Finansiering af terrorisme

Vurderingen af truslen om terrorfinansiering i relation til betalingstjenester viser, at kontobaserede transaktioner bruges af terrorister til at gemme og overføre penge og til at betale for de tjenester eller produkter, der er nødvendige for at udføre deres operationer, især når det sker gennem internettet. Ifølge en undersøgelse om finansieringen af europæiske jihadist-terrorceller er det formelle banksystem en af de seks mest almindeligt brugte metoder for terrorgruppernes vedkommende. De fleste terrorgrupper i Europa har en vis indkomst stammer fra lovlige kilder — som regel modtaget gennem det formelle banksystem — og bruger bankkonti og kreditkort både til deres daglige økonomiske aktiviteter og til angrebsrelaterede omkostninger. På grund af de kontobaserede elementer er terrorgruppers tilbøjelighed til at sætte deres lid til dette risikoscenarie mere begrænset. Deres kapacitet til at bruge det er imidlertid ganske stor. Betalingstjenester muliggør grænseoverskridende transaktioner, der kan hvile på forskellige identifikationsmekanismer (afhængigt af national lovgivning), som kan medføre, at terrorister bruger en falsk identitet. Det betyder, at de retshåndhævende myndigheder ikke kan spore afsenderen eller modtageren af transaktionen. Brugen af betalingstjenester kræver bestemte færdigheder, men ifølge de retshåndhævende myndigheder er disse færdigheder almindeligt udbredt blandt terrorgrupper og udgør ikke en forhindring (mobil-/internetbetalinger er ganske let). De pågældende beløb synes imidlertid at være ganske begrænsede.

Konklusion: terrorister bruger betalingstjenester til finansiering af terrorvirksomhed. De bruger IT-færdigheder til at omgå legitimationskravene og har ikke behov for særlig viden for at få adgang til denne kanal, som er ganske attraktiv og sikker. De pågældende beløb synes imidlertid at være ret begrænsede. I denne henseende anses trusselsniveauet for terrorfinansiering i relation til betalingstjenester for betydeligt (niveau 3).

Hvidvask af penge

Vurderingen af truslen om hvidvask af penge i relation til betalingstjenester anses for at have ligheder med indskud på en konto. Dette risikoscenarie angår både indsættelse og hævning af midler (dvs. indestående på en konto og brug af denne konto). Det bruges hyppigt af kriminelle, men også af slægtninge/nære forretningspartnere, hvilket udvider anvendelsesområdet for hensigts- og kapacitetsanalysen.[41] De midler, der anvendes i betalingstjenesterne er af ulovlig oprindelse. Det kræver nogen planlægning og viden om, hvordan banksystemerne fungerer.

[41] Om hensigt og kapacitet se fodnote 34.

Ifølge de retshåndhævende myndigheder kan betalingstjenesteydere anvendes af pengeskurerer eller kan være kontrolleret af kriminelle:

> For eksempel er en betalingstjenesteudbyder blevet undersøgt af flere EU-medlemsstater. Betalingstjenesteudbyderen, der var registreret i én EU-medlemsstat, lod sig registrere som e-pengeudsteder i et andet land og fik dermed en paslicens. Betalingstjenesteudbyderen blev kontaktet af en kriminel struktur, der påstod at drive onlinehandel. Betalingstjenesteudbyderen forsynede kunden med salgsterminaler. Terminalerne blev bragt ud af Europa og brugt i "swipe out"-konvertering af peso på det sorte marked. De oplysninger, der blev indsamlet i forbindelse med efterforskningen, viste, at betalingstjenesteyderen ikke foretog nogen form for kontrol af kunden, hvilket ville have resulteret i konstatering af risikoen, idet den erklærede lille onlineforretning førte til, at der inden for et begrænset tidsrum kunne akkumuleres flere millioner euro. Salgsterminalerne blev heller ikke overvåget, idet de ikke var fysisk til stede i EU, da ordren blev afgivet. Den samme betalingstjenesteudbyder blev også kontaktet af en kriminel struktur i en anden EU-medlemsstat. Den kriminelle struktur kontrollerede dækturistvirksomheder, der blev anvendt til kontante indskud af kokainudbytte. Disse virksomheder blev kunder hos betalingstjenesteudbyderen og krævede at få udstedt bankkort (da betalingstjenesteudbyderen er udsteder af Visa og Mastercard). Kortene blev bragt ud af Europa og kontanterne blev hævet i Colombia.

Konklusion: organiserede kriminelle grupper bruger denne metode ret hyppigt, da den er let tilgængelig, på trods af at det kræver nogen viden og planlægning at skjule midlernes oprindelse. Men når kriminelle strukturer overtager betalingstjenesteudbydere, kan risiko hvidvask være højere. I denne henseende anses trusselsniveauet for hvidvask af penge i relation til betalingstjenesteudbydere for betydeligt (niveau 3).

Sårbarhed

Finansiering af terrorisme

Vurderingen af sårbarheden over for finansiering af terrorisme i relation til betalingstjenester har visse træk til fælles med vurderingen af sårbarheden over for terrorfinansiering mht. detailbetalingssystemer.

a) risikoeksponering

Risikoeksponeringen er generelt meget høj på grund af de særlige karakteristika ved betalingstjenester, idet der er tale om meget store mængder produkter og serviceydelser. Selvom betalingerne normalt ikke er anonyme (da de er knyttet til en bestemt konto), kan de interagere med meget betydelige mængder af højrisikokunder eller -lande, herunder grænseoverskridende overførsler af midler. De spiller også sammen med nye betalingsformer (mobil/internet), hvilket kan øge niveauet for risikoeksponering, fordi de indebærer et forretningsforhold, der ikke er ansigt til ansigt.

b) risikobevidsthed

Risikobevidstheden er generelt god, fordi sektoren har indført vejledning i at opdage de relevante advarselssignaler om terrorfinansiering. Dette bekræftes af et godt rapporteringsniveau, idet sektoren synes at have de fornødne værktøjer til at opdage disse risici. Men kundekendskabskrav og risikoindikatorer er ikke altid tilstrækkeligt til at påvise en forbindelse til terrorisme, hvilket skyldes midlernes lovlige oprindelse. Kompetente myndigheder er også bevidst om sektorens sårbarheder og er proaktivt i kontakt med den.

c) retsgrundlag og kontroller

Betalingstjenester er omfattet af retsreglerne om bekæmpelse af hvidvask af penge og af finansiering af terrorisme på EU-niveau. Denne ramme har eksisteret i mange år, og kontrollerne anses overordnet set som tilfredsstillende. For så vidt angår den retlige ramme så dækker den ligeledes kredit- og betalingsinstitutter. På lignende måde som mht. indskud på konti anses de eksisterende kontroller generelt for at være effektive, men sanktionsscreening ikke er en erstatning for effektive kontroller i forbindelse med bekæmpelsen af finansiering af terrorisme. Økonomiske sanktioner rettes mod enkeltpersoner eller grupper, som man allerede ved, udgør en trussel, men risikoen fra terrorfinansiering udgår ofte fra personer, som ikke bliver opfanget af sanktionssystemet. Derfor er risikobaserede kontroller i forbindelse med bekæmpelse af hvidvask af penge og af terrorfinansiering samt især transaktionsovervågning nøglen til en effektiv bekæmpelse af terrorfinansiering.

Almindeligvis har banker og betalingsinstitutter ikke adgang til relevant efterretningsinformation, som de retshåndhævende myndigheder ofte ligger inde med, og som ville bidrage til, at de kunne identificere risici for terrorfinansiering, før de bliver til virkelighed. Tilsvarende kan de retshåndhævende myndigheders bestræbelser på at forpurre terroristernes aktiviteter og net blive vanskeliggjort, når de ikke er i stand til at indhente oplysninger om finansielle strømme, som kun virksomheder kan give. Der pågår for tiden initiativer på nationalt og supranationalt niveau, der er udformet med henblik på at finde ud af, hvordan retshåndhævende myndigheder kan give virksomhederne mere konkrete og væsentlige oplysninger om konkrete personer af interesse, som kan give virksomhederne mulighed for at fokusere deres transaktionsovervågning på disse personer.

Konklusion: Risikoeksponeringen kan betragtes som ganske høj (stort antal transaktioner). Sektoren udviser et godt niveau af bevidsthed omkring sårbarheden mht. risikoen og er i stand til at opstille de relevante faresignaler. De retsgrundlag og kontroller er grundlaget for et godt rapporteringsniveau. Men residualrisikoen er høj på grund af afhængigheden af de løbende kontroller vedrørende bekæmpelse af terrorfinansiering, som er baseret på sanktionsscreening. I denne henseende anses sårbarhedsniveauet over for terrorfinansiering i relation til betalingstjenester for betydeligt (niveau 3).

Hvidvask af penge

Vurderingen af sårbarheden over for hvidvask af penge i relation til betalingstjenester har visse fællestræk med vurderingen af sårbarheden over for terrorfinansiering mht. detailbetalingssystemer.

a) risikoeksponering

Risikoeksponeringen er generelt meget høj på grund af de særlige karakteristika ved betalingstjenester, hvor det ofte drejer sig om meget store beløb. Selvom betalingerne normalt ikke er anonyme (da de er knyttet til en bestemt konto), kan de medføre kontakt med højrisikokunder eller -lande, navnlig hvor ved grænseoverskridende overførsler af midler. De gør også brug af nye betalingsformer (mobil/internet), hvilket kan øge risikoen, fordi de indebærer , et forretningsforhold, der ikke er ansigt til ansigt.

b) risikobevidsthed

Kompetente myndighederne har konstateret forskelle mellem banker og betalingsinstitutter, hvor de sidstnævnte er mindre bevidste om risikoen for hvidvask af penge. De fleste kompetente myndigheder så den overordnede risikoprofil for betalingsinstitutter som enten betydelig eller meget betydelig. Dette gælder særligt for de myndigheder, der fører tilsyn med det største antal betalingsinstitutter. Det potentielle misbrug af nye teknologier som f.eks. mobilbetalinger for at lette peer-to-peer pengeoverførsler blev af de kompetente myndigheder generelt anset for at være en ny og voksende risiko (se afsnittet om virtuelle valutaer). Der er i øjeblikket utilstrækkelig overvågning, både når en betalingskonto åbnes (indgangspunkt), og når transaktionen behandles.

c) retsgrundlag og kontroller

Betalingstjenester er omfattet af retsreglerne om bekæmpelse af hvidvask af penge og af finansiering af terrorisme på EU-niveau. For så vidt angår den retlige ramme så dækker den ligeledes banker og betalingsinstitutter. Brugen af kontobaserede transaktioner indebærer, at de retlige rammer generelt finder anvendelse på banksektoren og på sektoren for betalingsinstitutter). Denne ramme har eksisteret i mange år, og kontrollerne anses overordnet set som tilfredsstillende. Betalingsinstitutter er afhængigt af bankkontroller for at begrænse deres iboende risiko for hvidvask af penge, men nogle alarmsystemer i bankerne er ikke grundige nok til at opspore mistænkelige kontanttransaktioner overført efterfølgende af betalingsinstitutter.

Konklusion: Sektorens risikoeksponering og risikobevidsthed er meget lig dem, der gælder for indskud på konti. For så vidt angår den retlige ramme så dækker den ligeledes banker og betalingsinstitutter. De eksisterende kontroller er imidlertid mindre effektive, når det drejer sig om betalingsinstitutter. I denne henseende anses sårbarhedsniveauet over for hvidvask af penge i relation til betalingstjenester for betydeligt (niveau 3).

Risikobegrænsende foranstaltninger:

Kommissionen:

- afklare og etablere en fælles ramme for elektronisk identifikation og kundekendskabskrav
- identificere risici forbundet med Fin-Tech og fastlægge standarder for at begrænse disse risici

- gennemføre en undersøgelse med henblik på kortlægning og analyse af bankpraksis i hele EU vedrørende accept af kunder og vurdere de eventuelle næste trin
- fremme samarbejdet mellem retshåndhævende myndigheder og finansielle institutioner med henblik på at øge effektiviteten af alarmsystemer for terrorfinansiering på supranationalt niveau.

Medlemsstater / kompetente myndigheder:

- Medlemsstaterne bør sikre, at tilsynsmyndighederne gennemfører en række tematiske undersøgelser på stedet med fokus på risikovurderinger af betalingsinstitutter, og sikre, at deres alarmsystemer er effektive.
- Derudover bør de kompetente myndigheder sørge for yderligere risikobevidsthed og risikoindikatorer vedrørende finansiering af terrorisme.
- Medlemsstaterne bør fjerne tærskler for lejlighedsvise transaktioner og gennemføre kundekendskabskrav for alle transaktioner, således at betalingsinstitutter effektivt kan overvåge og afsløre mistænkelige transaktioner.

12. Virtuelle valutaer og andre virtuelle aktiver

Produkt
Virtuelle valutaer og andre virtuelle aktiver

Sektor
Virtuelle valutaer og andre virtuelle aktiver – tjenesteudbydere

Generel beskrivelse af den pågældende sektor og det/den relevante produkt/aktivitet

Definitioner

Med det femte direktiv om bekæmpelse af hvidvask af penge blev der for første gang i EU-retten indført en definition af virtuel valuta, som beskrives som "et digitalt udtryk for værdi, som ikke er udstedt eller garanteret af en centralbank eller en offentlig myndighed, ikke nødvendigvis er bundet til en lovligt oprettet valuta og ikke har samme retlige status som valuta eller penge, men som accepteres af fysiske eller juridiske personer som betalingsmiddel, og som kan overføres, lagres og handles elektronisk".[42] I det femte hvidvaskdirektiv er med henblik på bekæmpelse af hvidvask af penge og af finansiering af terrorisme som forpligtede enheder angivet udbydere af valutaveksling mellem virtuelle valutaer og fiatvalutaer samt udbydere af virtuelle tegnebøger med virtuel valuta. I oktober 2018 ændrede FATF sine standarder, idet man udvidede sin henstilling 15 (ny teknologi) med "virtuelle aktiver" og "udbydere af tjenesteydelser vedrørende virtuelle aktiver". Den ændrede henstilling 15 kræver, at landene opstiller regler for tjenesteudbydere af virtuelle aktiver i forhold til bekæmpelse af hvidvask af penge og af finansiering af terrorisme, godkender eller registrerer dem og underkaster dem effektive systemer til overvågning og sikring af overholdelse af de relevante forholdsregler, der kræves i FATF's henstillinger.

Endvidere er virtuelle aktiver nu defineret i FATF's ordliste som "en digital repræsentation af værdi, som kan sælges eller overføres digitalt og kan bruges til betalings- eller investeringsformål, og som ikke omfatter digitale repræsentationer af fiatvalutaer, værdipapirer og andre finansielle aktiver, der allerede er omhandlet andetsteds i FATF's henstillinger".

Den nye FATF-definition er bredere end definition af "virtuel valuta" i det femte hvidvaskdirektiv.

Som følge af ændringerne blev det anbefalet landende at lade forpligtelserne til bekæmpelse af hvidvask af penge og af finansiering af terrorisme omfatte enhver fysisk eller juridisk person (der ikke er omhandlet andetsteds i FATF's henstillinger), som erhvervsmæssigt udøver en eller flere af følgende aktiviteter eller handlinger for eller på vegne af en anden fysisk eller juridisk person:

- veksling mellem virtuelle aktiver og fiatvalutaer

[42] I betragtning 10) til det femte hvidvaskdirektiv gøres det klart, at virtuelle valutaer ikke bør forveksles med (blandt andet) elektroniske penge som defineret i det andet e-pengedirektiv eller med midler som defineret i det andet betalingstjenestedirektiv: https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32018L0843&from=DA .

- veksling mellem en eller flere andre former for virtuelle aktiver
- overførsel af virtuelle aktiver
- opbevaring eller administration af virtuelle aktiver eller instrumenter, der giver kontrol over virtuelle aktiver, og
- deltagelse i og levering af finansielle tjenesteydelser i forbindelse med en udsteders udbud og/eller salg af et virtuelt aktiv.

Interessenter

På markedet for virtuelle valutaer/virtuelle aktiver deltager forskellige interessenter, og de vigtigste er:

– **leverandører af tegnebøger:** brugere af kryptovaluta kan have konti for virtuelle valutaer-/virtuelle aktivkonti på deres egne enheder eller overdrage det til en leverandør af tegnebøger at besidde og administrere kontiene (i en elektronisk tegnebog) og give en oversigt over brugerens transaktioner (via en web- eller telefonbaseret tjeneste). Der findes tre typer leverandører af tegnebøger:

  - udbydere af hardware til tegnebøger, som forsyner brugerne med konkrete hardwareløsninger til privat opbevaring af deres krypteringsnøgler
  - udbydere af software til tegnebøger, som forsyner brugere med softwareprogrammer, der giver dem mulighed for at få adgang til nettet, sende og modtage kryptovalutaer samt gemme deres krypteringsnøgler lokalt, og
  - udbydere af virtuelle tegnebøger, der tager en brugers kryptografiske nøgler i online forvaring (herunder tegnebøger med mange tegningsberettigede).

  I modsætning til udbydere af software til tegnebøger (som leverer apps eller programmer, der kører på brugernes hardware – computer, smartphone, tablet osv. – og har adgang til offentlige oplysninger fra en distributed ledger og har adgang til nettet), tager udbydere af virtuelle tegnebøger brugerens offentlige og private nøgle i forvaring. Dette svarer til en traditionel bank, der stiller en personlig konto til rådighed.

  Tegnebøger kan gemmes online ("hot storage") eller offline ("cold storage"), hvor sidstnævnte sikrer en bedre beskyttelse.

  Kun udbydere af virtuelle tegnebøger ("enhed[er], som leverer tjenester til at beskytte private kryptografiske nøgler på vegne af [deres] kunder med henblik på at opbevare, lagre og overføre virtuelle valutaer") er forpligtede enheder i det femte hvidvaskdirektivs forstand.

  Udbydere af hardware og software til tegnebøger har ikke nøgler i forvaring på deres kunders vegne, men forsyner dem med redskaber til selv at sikre deres kryptovalutaer; dette skaber rum for hvidvask af penge/finansiering af terrorisme

– **vekslingsplatforme** (en person eller enhed, der er beskæftiget med veksling af virtuelle valutaer/virtuelle aktiver til fiatvaluta, fiatvaluta til virtuelle valutaer/virtuelle aktiver, penge eller andre slags virtuelle valutaer/virtuelle

aktiver): disse platforme (*vekselkontorerne* i de virtuelle valutaers/virtuelle aktivers verden) kan modtage et bredt spektrum af betalingsformer, herunder kontanter, kreditoverførsler, kreditkort og andre virtuelle valutaer/virtuelle aktiver. De omfatter pengeautomater.

Ligesom traditionelle vekselbørser giver store vekselbørser for virtuelle valutaer et samlet overblik over ændringerne i en virtuel valutas vekselkurs og dens bevægelser. Nogle platforme tilbyder tjenester som konverteringstjenester for forretningsdrivende, der accepterer at modtage betalinger i virtuelle valutaer, men er bange for kursfald og straks vil konvertere dem til (nationale) fiatpenge. Femte hvidvaskdirektiv omfatter kun veksling af virtuelle valutaer til fiatvalutaer, ikke til andre virtuelle valutaer/virtuelle aktiver.

- **bruger** (en person eller juridisk enhed, som modtager et beløb i virtuel valuta og bruger det til at købe virkelige eller virtuelle varer eller tjenester eller til som privatperson at sende overførsler til en anden person (til personlig brug), eller som besidder den virtuelle valuta til andre formål som f.eks. investeringer): typisk modtager brugere virtuelle valutaer på én af følgende måder:
    - gennem en vekselbørs (eller for de mest centraliserede virtuelle valutaers vedkommende direkte fra den enhed, der styrer ordningen) ved brug af fiatvalutaer eller anden virtuel valuta
    - gennem konkrete aktiviteter, f.eks. som reaktion på en kampagne, udfyldelse af en onlineundersøgelse og "mining" (anvende særlig software til at løse komplicerede algoritmer for at validere transaktioner i systemet med virtuelle valutaer), og/eller
    - fra den enhed, der styrer ordningen-, udstederen eller andre brugere til andre formål end deres erhvervsmæssige eller forretningsmæssige virksomhed
- **miners:** i decentrale ordninger med virtuelle valutaer løser miners komplekse algoritmer for at få små beløb i virtuel valuta. Miners arbejder ofte anonymt fra et hvilket som helst sted i verden og validere transaktioner med virtuelle valutaer. Når en gruppe miners kontrollerer mere end halvdelen af den samlede computerkraft, der bruges til at skabe virtuelle valutaenheder, er den i stand til at gribe ind i transaktioner, f.eks. ved at afvise transaktioner, der er valideret af andre miners. Miners grupperer sig i pools (Antpool, F2Pool, BitFury BTCC Pool, BTCC, BW:COM osv.). For øjeblikket befinder de fleste sig i Kina, og
- **initial coin offerors (første møntudbydere):** FATF's nyligt vedtagne definition af udbyder af tjenesteydelser vedrørende virtuelle aktiver omfatter "deltagelse i og levering af finansielle tjenesteydelser i forbindelse med en udsteders udbud og/eller salg af et virtuelt aktiv". Coin offerors er de personer eller organisationer, der tilbyder mønter i kryptovaluta til brugere ved møntens første udgivelse, enten mod betaling (f.eks. gennem et crowdsale) eller gratis (f.eks. som led i en bestemt tilmeldingsordning, f.eks. Stellar) normalt med henblik på at finansiere møntens

videreudvikling eller øge dens indledningsvise popularitet. En coin offeror kan være den samme person som møntens opfinder eller en anden person eller organisation.

Det femte hvidvaskdirektiv har udvidet forpligtelser til-bekæmpelse af hvidvask af penge til at omfatte "udbydere af valutaveksling mellem virtuelle valutaer og fiatvalutaer" (vekslingsplatforme) og udbydere af virtuelle tegnebøger, men dækker ikke alle -de aktiviteter vedrørende virtuelle aktiver, der henvises til i den nye FATF-definition af serviceudbydere af virtuelle aktiver, navnlig vekslinger fra virtuelle aktiver til virtuelle aktiver og første møntudbud (se **retsgrundlag og kontroller** nedenfor).

Markedet for virtuelle valutaer/virtuelle aktiver i EU

Det er vanskeligt at sammenstille officielle data om markedet for virtuelle valutaer. Estimaterne nedenfor er baseret på oplysninger fra forskellige websteder, der sporer handelsvoluminer og priser eller udfører forskning. Estimater fra markedsaktørerne har tendens til at være lavere end de statistikker, man finder online. Nedenstående statistikker vise således høje, men afbalancerede estimater:

Samlet antal virtuelle valutategnebøger på verdensplan	13 mio. (4. kvt. 2015)[43] – 7,4 mio. kr. i 4. kvt. 2014
Virtuelle valutategnebøger i EU	Omkring 3 mio.
Brugere af virtuelle valutaer på verdensplan[44]	1-4 mio.
Brugere af virtuelle valutaer i EU	Omkring 500 000
Miners af virtuelle valutaer på verdensplan	100 000[45]
Miners af virtuelle valutaer i EU	10 000 (estimat)
Udbydere af software til virtuelle valutategnebøger på verdensplan	> 500 (estimat)
udbydere af virtuelle valutaer på verdensplan	> 100(estimat)
Udbydere af virtuelle valutaer i EU	> 20 (estimat)
Vekslingsplatforme på verdensplan	> 100
Vekslingsplatforme i EU	> 28
Pengeautomater på verdensplan[46]	571
Pengeautomater i EU	> 100
Daglige virtuelle valutatransaktioner	> 125 000 (kun bitcoin – for 2015)
Forretningsdrivender, der accepteret bitcoins	110 000 (4. kvt. 2015) – 80 000 i 4. kvt. 2014
Markedsværdi af virtuelle valutaer	7 mia. EUR

[43] http://www.coindesk.com/state-of-bitcoin-blockchain-2016/, se slide 8.
[44] Mindst én transaktion pr. måned.
[45] http://bravenewcoin.com/news/the-decline-in-bitcoins-full-nodes/
[46] http://coinatmradar.com/ (efterset den 4. februar 2016).

Beskrivelse af risikoscenariet

Hvidvask af penge: Virtuelle valutaer udgør en markant risiko for hvidvask af penge og terrorfinansiering pga. den lette overførsel af virtuel valuta til forskellige lande, ligesom der ikke er fastlagt ensartede kontroller og forebyggende foranstaltninger på globalt plan. Lovovertrædere bruger virtuelle valuta-/virtuelle aktiv-systemer til at overføre værdier eller købe varer anonymt (pengeindbetaling eller tredjepartsfinansiering via virtuelle børser).

Finansiering af terrorisme: Virtuelle valutaer/virtuelle aktiver indebærer normalt kunderelationer, der ikke er -ansigt-til-ansigt og kan muliggøre anonym finansiering eller anonyme køb (pengeindbetaling eller tredjepartsfinansiering via virtuelle børser, på hvilke finansieringskilden er ikke ordentligt identificeret). De kan desuden muliggøre anonyme pengeoverførsler, hvis afsender og modtager ikke er ordentligt identificeret.

Trussel

Aktiviteter i forbindelse med virtuelle valutaer/virtuelle aktiver udgør en stadig stigende trussel om hvidvask af penge/terrorfinansiering. Finansielle efterretningsenheder i FATF's globale net har oplevet en stigning i antallet af rapporter om mistænkelige transaktioner, der angår virtuelle valutaer/virtuelle aktiver; dette vil sandsynligvis tiltage for de finansielle efterretningsenheder i EU efter gennemførelsesfristen for det femte hvidvaskdirektiv.[47]

Europol anser bitcoin for det foretrukne virtuelle valuta-/virtuelle aktiv-valg for flertallet af kriminelle, men forventer en mere markant forskydning hen imod anonymitetsstyrkede virtuelle aktiver, hvilket giver mere beskyttelse, hurtigere transaktionstider, lavere transaktionsgebyrer og mindre prisudsving.

Brugen af andre mønter med mere beskyttelse vil langsomt fjerne behovet for særlige blandingstjenester. De to største blandingstjenester har allerede indstillet deres aktiviteter (i 2017). Vekslingstjenester kan nu tilbyde transaktioner fra virtuelle valutaer/virtuelle aktiver til virtuelle valutaer/virtuelle aktiver, som tilslører transaktionssporet, og decentrale blandingstjenester har også været anvendt.

Et særligt sæt udfordringer udspringer af ydelser mht. virtuelle valutaer/virtuelle aktiver, der leveres af kriminelle eller enheder, der ikke overholder reglerne:

- aktørerne bruger kriminelle penge til at oprette en virksomhed med virtuelle valutaer/virtuelle aktiver, som deponerer penge erhvervet ved kriminalitet eller ulovligt erhvervede virtuelle valutaer/virtuelle aktiver i en pengeautomat
- enkeltpersoner køber/sælger store mængder virtuelle valutaer/virtuelle aktiver for ethvert aktiv "over the counter" (ingen formidling) uden at være registreret som virtuelle valutaer/virtuelle aktiver-tjenesteudbydere eller reklamere for deres ydelser, og

[47] Den luxembourgske finansielle efterretningsenhed noterede en 70 % stigning i antallet af rapporter om mistænkelige transaktioner i relation til brugen af virtuelle aktiver mellem 2017 og 2018.

– betalingstjenesteudbydere, der tilbyder krypto-kort, blev oprindelig kun tilbudt for bitcoin, men der er sket et skift i retning af understøttelse af flere virtuelle valutaer/virtuelle aktiver. De registreres ofte i lande med "gunstige" tilsynsregler.

Retshåndhævende myndigheder står også over for en særlig udfordring med at indsamle oplysninger, når veksling af virtuelle valutaer/virtuelle aktiver finder sted i et andet land end det, hvor betaleren/betalingsmodtageren befinder sig (som i sig selv kan være overalt i verden).

Mange lande er bekymrede for misbrug af initial coin offerings (ICO'er) og mere generelt for den manglende bevidsthed blandt udstederne af sikkerhedstokens om deres forpligtelser mht. bekæmpelse af hvidvask af penge og af finansiering af terrorisme, især i lande, hvor det ikke kræves, at virksomheder har en fysisk tilstedeværelse for at kunne blive registreret og opnå tilladelse.

Finansiering af terrorisme

Vurderingen viser, at terrorgrupper kan have interesse i at bruge virtuelle valutaer/virtuelle aktiver til finansiering af terroristvirksomhed. Der er rapporteret et begrænset, men voksende antal sager med relation til virtuelle valutaer.[48] Egmont Gruppen af finansielle efterretningsenheder har registreret tilfælde, hvor terrorgrupper har brugt virtuelle valutaer, og grupper vides at have givet instruktioner på internettet (herunder via Twitter) om, hvordan virtuelle valutaer/virtuelle aktiver bruges.

Konklusion: Retshåndhævende myndigheder har oplysninger om, at terrorgrupper kan bruge virtuelle valutaer til at finansiere terroraktiviteter. Truslen om finansiering af terrorisme i relation til virtuelle valutaer anses som følge heraf for betydelig (niveau 3).

Hvidvask af penge

Vurderingen af truslen om hvidvask af penge i relation til virtuelle valutaer/virtuelle aktiver viser, at kriminelle organisationer kan bruge dem til at få adgang til "rene kontanter" (indbetaling og udbetaling). Ikke kun cyberkriminelle bruger virtuelle valutaer/virtuelle aktiver – andre organiserede kriminelle grupper som narkosmuglere bruger dem til at flytte og hvidvaske udbyttet af kriminalitet. Virtuelle valutaer/virtuelle aktiver giver disse grupper mulighed for at få adgang til kontanter anonymt og skjule transaktionssporet. Kriminelle kan erhverve private nøgler til e-tegnebøger eller hæve kontanter fra pengeautomater.

Konklusion: Et stigende antal efterforskninger har angået kriminelle organisationers (ikke kun de cyberkriminelles) brug af virtuelle valutaer og virtuelle aktiver. Trusselsniveauet for hvidvask af penge i relation til virtuelle valutaer anses som følge heraf for betydeligt (niveau 3).

Sårbarhed

Finansiering af terrorisme

[48] Nogle tilfælde af donation gennem crowdfunding opkrævet i bitcoin, idet der anføres "støtte til enker, martyrer, muslimske grupper" i et forsøg på at undgå klar forbindelse til finansiering af terrorisme, og der rådes til brug af bitcoin pengeautomater.

Ved vurderingen af sårbarheden over for terrorfinansiering i relation til udbydere af virtuelle valutaer/virtuelle aktiver skal vi huske på, at nok er EU begyndt at regulere virtuelle valutaer/virtuelle aktiver, men risikoen for, at de bliver misbrugt til finansiering af terrorisme er kun lige i sin vorden.

a) risikoeksponering

Når de bruges anonymt, gør virtuelle valutaer det muligt at udføre transaktioner hurtigt uden at måtte afsløre "ejerens" identitet. De udbydes via internettet, og det grænseoverskridende element er den mest åbenlyse risikofaktor, da det giver mulighed for interaktion med højrisikoområder eller højrisikokunder, der ikke kan identificeres. Dette kan ændre sig, når de nye FATF-standarder gennemføres, da de vil tvinge udbydere af tjenester med virtuelle aktiver til at lade sig registrere det sted, hvor de er oprettet eller indregistreret (juridiske personer), eller i det land, hvor forretningsstedet er beliggende (fysiske personer). Imidlertid spreder brugen af virtuelle valutaer/virtuelle aktiver sig hurtigt, og antallet af transaktioner forventes at stige betydeligt i de kommende år.

b) risikobevidsthed

Denne del af sårbarheden over for terrorfinansiering er vanskelig at vurdere til bunds – "udbydere af valutaveksling mellem virtuelle valutaer og fiatvalutaer" og udbydere af virtuelle tegnebøger er nu forpligtede enheder på EU-niveau, men dette er (endnu) ikke tilfældet for alle udbydere af virtuelle valutaer/virtuelle aktiver. Endvidere har de kompetente myndigheder og de finansielle efterretningsenheder noteret sig i forbindelse med deres kontakter med sektoren, at bevidstheden om risikoen for terrorfinansiering stadig er forholdsvis lav, selvom sektoren kræver vedtagelsen af en passende retlig ramme mht. bekæmpelse af hvidvask af penge og af finansiering af terrorisme.

Virtuelle aktiver er blandt de vigtigste nytilkommende risici inden for næsten alle sektorer, fordi:

- en mangel på viden og forståelse, som forhindrer virksomheder og kompetente myndigheder i at foretage en ordentlig konsekvensanalyse
- lakuner eller uklarheder i anvendelsen af gældende lovgivning
- potentiel eksponering af finansierings- og kreditinstitutter for øget risiko for hvidvask af penge og finansiering af terrorisme i forbindelse med virtuelle valutaer/virtuelle aktiver, hvor de fungerer som mellemled eller vekslingsplatforme mellem virtuelle valutaer/virtuelle aktiver og fiat-valutaer (i fraværet af en egentlig risikovurdering) og
- i investeringsbranchen, onlinebehandling af transaktioner med kun begrænset kundeidentifikation og kontroller.

Sektoren er ikke velorganiseret endnu, og det er vanskeligt at finde egnede værktøjer til at forsyne den med relevant information med henblik på at øge graden af bevidsthed.

c) retsgrundlag og kontroller

Det femte hvidvaskdirektiv har indført en første EU-definition af virtuelle valutaer og udvidet forpligtelserne til bekæmpelse af hvidvask af penge med "udbydere af valutaveksling mellem virtuelle valutaer og fiatvalutaer" og udbydere af virtuelle tegnebøger. Ud over almindelig kundekendskabskrav skal medlemsstaterne sikre, at disse

nye forpligtede enheder registreres. Desuden skal de kræve, at de kompetente myndigheder sikrer, at kun personer, som opfylder kravene til egnethed og hæderlighed, har ledelsesfunktioner i disse enheder eller er deres reelle ejere.

De seneste ændringer af FATF-standarderne om virtuelle aktiver betyder, at det femte hvidvaskdirektivs definition af virtuelle valuta kan blive for snæver, da den ikke dækker andre former for virtuelle aktiver.

Derudover kan der være lakuner, som skal udfyldes med hensyn til forskellige aktiviteter udøvet af udbydere af tjenester med virtuelle aktiver, der ikke er omfattet af EU's regler:

- udbydere af virtuelle tegnebøger, der ikke har nøgler i forvaring på deres kunders vegne, men blot forsyner dem værktøjer til til selv at sikre deres kryptovalutaer, således som udbydere af hardware og software til tegnebøger
- vekslinger fra virtuelle valutaer eller virtuelle aktiver til andre virtuelle valutaer eller virtuelle aktiver, og
- "deltagelse i og levering af finansielle tjenesteydelser i forbindelse med en udsteders udbud og/eller salg af et virtuelt aktiv", navnlig i tilfælde, hvor coin offeror kan være den samme person som møntens opfinder, eller en anden person eller organisation.

Konklusion: Den mest betydelige faktor mht. sårbarhed over for udbydere af virtuelle valutaer og virtuelle aktiver er, at de muligvis ikke er fuldt ud reguleret i EU. Når det er gennemført, vil det femte hvidvaskdirektivs forbedre situationen betydeligt ved at gøre udbydere af virtuelle tegnebøger og udbydere af valutaveksling mellem virtuelle valutaer og fiatvalutaer til forpligtede enheder, hvorved det sikres, at de bliver registreret, og at kun personer, som opfylder kravene til egnethed og hæderlighed, har ledelsesfunktioner i disse enheder eller er reelle ejere. Denne ramme er endnu ikke gennemført, og det vil være nødvendigt at overveje at udvide den til at omfatte andre udbydere af virtuelle aktiver, f.eks. initial coin offerors og udbydere af vekseltjenester mellem virtuelle valutaer. Den iboende risikoeksponering er meget høj på grund af de særlige karakteristika, der er forbundet med virtuelle valutaer (internetbaserede-, grænseoverskridende og anonyme). Endelig er sektoren i dag ikke organiseret godt nok til at modtage vejledning og relevant information om kravene til bekæmpelse af hvidvask af penge og af finansiering af terrorisme. Som følge heraf anses sårbarhedsniveauet for finansiering af terrorisme i relation til virtuelle valutaer for betydeligt/meget betydeligt (niveau 3/4).

Hvidvask af penge

Vurderingen af sårbarheden over for hvidvask af penge i relation til udbydere af virtuelle valutaer starter med samme forbehold som for terrorfinansiering. De er delvis reguleret i EU, og der er få tegn på, at virtuelle valutaer misbruges til hvidvask af penge. Det er dog ikke til hinder for en vurdering af potentielle sårbarheder. Selvom kun få efterforskninger fører til retsforfølgelse, eksisterer risikoen og kan analyseres.

a) risikoeksponering

Som nævnt ovenfor gør virtuelle valutaer, når de bruges anonymt, det muligt at udføre transaktioner hurtigt og uden at måtte afsløre "ejerens" identitet. De udbydes via

internettet, og det grænseoverskridende element er den mest åbenlyse risikofaktor, da det muliggør interaktion med højrisikoområder eller højrisikokunder (det mørke net), der ikke kan identificeres. På konverteringsstadiet bliver brugen af kontanter også et nyt element af sårbarhed. De nye regler i det femte hvidvaskdirektiv vil løse dette ved at udvide reglerne om bekæmpelse af hvidvask af penge og af finansiering af terrorisme til at gælde "udbydere af valutaveksling mellem virtuelle valutaer og fiatvalutaer". Men fordelingskanalerne er fortsat decentraliseret, hvilket øger risikoeksponeringen (navnlig gør pengeautomater det muligt at hæve eller konvertere virtuelle valutaer).

b) risikobevidsthed

Dette er ny teknologi, og niveauet af risikobevidsthed i sektoren har svært ved at holde trit. Sektoren har mere og mere brug for en retlig ramme, hvor virtuelle valutaer er omfattet af krav om bekæmpelse af hvidvask af penge og af finansiering af terrorisme. Finansielle efterretningsenheder kan ikke registrere og analysere risici på grundlag af blockchain alene. De kan ikke fastslå, hvilke beløb der gemmes i e-tegnebøger eller identificere oprindelsen til/modtageren af midlerne.

c) retsgrundlag og kontroller

Det femte hvidvaskdirektivs vil føje vekslingsplatforme for virtuelle valutaer og udbydere af virtuelle tegnebøger til listen over forpligtede enheder og underlægge dem kundekendskabskrav og pligt til registrering. Som med terrorfinansiering kan der være behov for forbedringer for at sikre, at alle udbydere af virtuelle valutaer/virtuelle aktiver lever op til kravene om bekæmpelse af hvidvask af penge og af finansiering af terrorisme.

I begyndelsen af 2019 offentliggjorde Den Europæiske Værdipapir- og Markedstilsynsmyndighed og Den Europæiske Banktilsynsmyndighed i lyset af de seneste ændringer af FATF's henstillinger vedrørende virtuelle aktiver rapporter om tilstrækkeligheden af de nuværende EU-lovrammer med hensyn til initial coin offerings og kryptoaktiver. De opfordrer til, at anvendelsesområdet for hvidvaskdirektivet tages op til fornyet overvejelse i lyset af de nye definitioner af virtuelle aktiver og udbydere af virtuelle aktiver (FATF 2018). De nye internationale standarder kræver, at udbuddet af disse andre ydelser vedrørende virtuelle aktiver reguleres yderligere, og at den nuværende definition af virtuelle valutaer tilpasses til også at omfatte den bredere virkelighed, der er dækket af begrebet "virtuelle aktiver". Anonymitet i nogle transaktioner mht. virtuelle aktiver udgør også fortsat en væsentlig risikofaktor, som man kunne tage fat på.

Konklusion: Det femte hvidvaskdirektiv burde i betydeligt omfang styrke overvågningen af risici knyttet til udbydere af virtuelle aktiver, men det skal først gennemføres. De retlige rammer kunne også udvides til at omfatte udbydere af virtuelle aktiver, som endnu ikke er omfattet (f.eks. initial coin offerors og udbydere af valutaveksling mellem virtuelle valutaer) og rettes ind efter de nye FATF-standarder. Den iboende risikoeksponering bør fortsat anses for meget høj på grund af de særlige karakteristika, der er forbundet med virtuelle valutaer (internetbaserede-, grænseoverskridende og anonyme). Derfor anses sårbarhedsniveauet over for hvidvask af penge i relation til virtuelle valutaer for betydeligt/meget betydeligt (niveau 3/4).

Risikobegrænsende foranstaltninger:

- Kommissionen skal vurdere egnede måder, hvorpå den kan fuldføre sit lovgivningsarbejde, så det sikres, at alle udbydere af virtuelle valutaer/virtuelle aktiver er ordentligt dækket af forpligtelser til bekæmpelse af hvidvask af penge.
- Kompetente myndigheder bør følge udviklingen på dette område tæt og vurdere, om ændringer i de nationale love og bestemmelser om bekæmpelse af hvidvask af penge og af finansiering af terrorisme er påkrævet.
- I 2022 vil Kommissionen udsende en beretning om gennemførelsen af det femte hvidvaskdirektiv og medlemsstaternes indsats for at gennemføre FATF-standarderne.
- Kommissionen er for øjeblikket i færd med at vurdere reglerne om finansielle tjenesteydelser for at sikre, at de faktisk finder anvendelse på de virtuelle aktiver, der er omfattet af dem, samt at undersøge, om der er behov for lovgivningsinitiativer mht. de virtuelle aktiver, som i øjeblikket ikke er omfattet af reglerne om finansielle tjenesteydelser, idet disse i vid udstrækning indebærer de samme risici som dem, der blev påpeget i de råd, der blev givet af EBA og ESMA i januar 2019.
- Kommissionen vil fortsat arbejde for et sammenhængende og koordineret internationalt regelsæt omkring virtuelle valutaer/virtuelle aktiver, som udbygger dens bestræbelser i G20 og internationale standardiseringsorganer. Kommissionen vil fortsat være aktivt involveret i FATF's arbejde og har også tilsluttet sig den seneste FATF-kontaktgruppe med den private sektor, der er nedsat til opfølgning på gennemførelsen af de nye standarder vedrørende virtuelle valutaer/virtuelle aktiver.
- I sammenhæng med den supranationale risikovurderingsrapport vil Kommissionen fortsat overvåge de risici, der er forbundet med Fin-Tech, krypto-til-krypto vekselbørser samt brugen af virtuelle valutaer/virtuelle aktiver til køb af maget værdifulde varer.

13. Erhvervslån

Produkt
Kredit - lån

Sektor
Kredit- og finanssektoren (herunder forsikringsselskaber)

Beskrivelse af risikoscenariet

Lovovertrædere tilbagebetaler erhvervslån med ulovlige midler (evt. med kreditkort for at legitimere kilderne til midlerne). Lån giver kriminelle midler et skær af legitimitet.

Trussel

Finansiering af terrorisme

Vurderingen af truslen om terrorfinansiering i relation til erhvervslån viser, at der kun har været få tilfælde af, at terrororganisationer bruger dem som middel til at skaffe sig midler. Generelt gælder det, at organisationerne ikke opfylder betingelserne for sådanne lån (lønniveau for lavt, midler hidrører fra sociale ydelser). I nogle tilfælde har sanktionerede enheder (organisationer på listen) forsøgt at bruge erhvervslån til at finansiere terroraktiviteter gennem skuffeselskaber, men dette kræver et højt niveau af ekspertise og viden.

Konklusion: Der er ikke meget, der tyder på, at kriminelle har brugt/har til hensigt at anvende denne metode. Truslen om finansiering af terrorisme i relation til erhvervslån anses derfor for mindre betydelig (niveau 1).

Hvidvask af penge

Vurderingen af truslen om hvidvask i relation til erhvervslån er det ikke fundet mange tegn på, at kriminelle vil udnytte dette risikoscenarie, som de ikke opfatter som attraktivt. De fleste falske lån er udtryk for systematiseret bedrageri (f.eks. optager to virksomheder et falsk lån og bruger en bank at overføre midler); de bliver ikke nødvendigvis brugt til at hvidvaske udbytte fra kriminalitet. Man har undersøgt nogle tilfælde af lån mellem sammensvorne virksomheder som en del af et stort system til hvidvask af penge, men de indbefattede i realiteten ikke bistand fra den finansielle sektor.

Konklusion: Der er ikke meget, der tyder på, at kriminelle har brugt/har til hensigt at anvende denne metode. Truslen om hvidvask af penge i relation til erhvervslån anses derfor for i moderat grad betydelig (niveau 2).

Sårbarhed

Finansiering af terrorisme

Vurderingen af sårbarheden over for terrorfinansiering i relation til erhvervslån er blevet overvejet i sammenhæng med systemer til hvidvask af penge i relation til erhvervslån.

Konklusion: Niveauet af sårbarhed over for finansiering af terrorisme anses for mindre betydeligt (niveau 1).

Hvidvask af penge

Vurderingen af sårbarheden over for hvidvask af penge i relation til erhvervslån har vist følgende resultater:

a) risikoeksponering

Den væsentligste risiko ved disse produkter ligger i en mulig førtidsindfrielse fra virksomhedernes side, somme tider kontant (med midler fra kapitalforøgelse af ukendt oprindelse).

b) risikobevidsthed

Finansielle institutioner synes at være tilstrækkeligt orienteret om de risici for svig, der kan forekomme i forbindelse med erhvervslån. De er særligt opmærksomme på risikoen for falsk dokumentation eller falsk identitet, da de også skal sikre sig, at de kan få midlerne igen. Sårbarheden er mindre i tilfælde, hvor kontant indfrielse ikke accepteres. Der kan opstå visse interessekonflikter, hvor misligholdte lån opkøbes.

c) retsgrundlag

Erhvervslån er omfattet af rammerne for bekæmpelse af hvidvask af penge og bekæmpelse af terrorisme på EU-plan. I hvert fald i banksektoren kan de eksisterende kontroller anses for at være forenelige med antallet af transaktioner.

Konklusion: Niveauet af sårbarhed over for hvidvask af penge anses for i moderat grad betydeligt (niveau 2).

Risikobegrænsende foranstaltninger:

Medlemsstater / kompetente myndigheder:

- Tematiske inspektioner af andre virksomheder end banker med fokus på kontrolsystemer til afsløring af førtidsindfrielse af lån.

14. Forbrugerkredit og smålån

Produkt
Kredit - lån

Sektor
Kredit- og finanssektoren

Beskrivelse af risikoscenariet

Terrorister/organiserede kriminelle grupperinger bruger (kortfristede, små, men med høj rente) "lønningsdagslån", forbrugslån eller studielån. Lånene ydes for relativt små beløb, hvilket giver adgang til midler, hvis kilder ikke kan spores, så længe pengene ikke bliver overført.

Terrorister/kriminelle organisationer bruger kreditkort til at hæve kontanter fra pengeautomater, hvorved de oparbejder et negativt indestående på kontoen. De forsvinder med pengene uden at have til hensigt at tilbagebetale den "påtvungne" kredit.

Denne type lån kan også bruges til at hvidvaske udbytte fra kriminel virksomhed. Lånene bruges til at købe maget værdifulde varer (f.eks. biler, smykker) og bliver så indfriet før tid.

Trussel

Finansiering af terrorisme

Vurderingen af truslen om finansiering af terrorisme i relation til forbrugerkredit og smålån viser, at terrorgrupperne bruger denne metode til at finansiere udenlandske terrorkrigeres rejser til højrisikolande uden for EU. Det mest anvendte produkt er forbrugerkredit. Det tiltrækkende ved smålån er, at de ikke nødvendigvis kræver et højt niveau af ekspertise og planlægning. Men større ekspertise kan være involveret, hvis den nationale lovgivning kræver særlig dokumentation, hvilket visse terroristgrupper er i stand til at eftergøre.

Konklusion: Forbrugerkredit og smålån er attraktive for terrorgrupper, der har brugt/bruger denne metode ret ofte. Visse lande kan opstille betingelser for adgang til forbrugslån eller smålån, men dette synes ikke at udgøre en hindring for terrororganisationer. Truslen om finansiering af terrorisme i relation til smålån anses derfor for betydelig (niveau 3).

Hvidvask af penge

Disse produkter indeholder mindre potentiale for hvidvask end andre finansielle produkter, men kriminelle organisationer bruger dem til at finansiere indkøb af varer af høj værdi og indfrir derefter lånene med kontanter.

Konklusion: Forbrugslån og smålån er ikke så attraktive for kriminelle organisationer som andre finansielle produkter, men de kan anvendes indirekte til at hvidvaske udbytte fra kriminel virksomhed. Transaktioner sker normalt med mindre beløb, men nogle kriminelle grupperinger har været i stand til at opdele store beløb på adskillige transaktioner. Truslen om hvidvask af penge i relation til smålån anses derfor for i moderat grad betydelig (niveau 2).

Sårbarhed

Finansiering af terrorisme

Vurderingen af sårbarhed over for finansiering af terrorisme i relation til forbrugerkredit/smålån har vist følgende resultater:

a) risikoeksponering

Produkterne er forholdsvis almindelige, men de omfatter normalt små beløb, de tiltrækker ikke højrisikokunder eller kunder fra højrisikolande, og de er underkastet særlige kontroller fra de finansielle institutioners side. De pågældende beløb kan faciliterer terroraktioner, så risikoeksponeringen i forhold til terrorfinansiering er ikke ubetydelig. Den iboende risiko kan være større i forhold til banker, der har specialiseret sig i hurtige forbrugslån, eller telekommunikationsvirksomheder, som tilbyder disse produkter.

b) risikobevidsthed

Antagelsen om kun ringe risikoeksponering opvejes af, at sektoren på grund af de små beløb er mindre bevidst om risiciene mht. terrorfinansiering. Derudover er der som mht. erhvervslån en højere grad af bevidsthed om risiciene for svig end om terrorfinansiering, således at faresignalerne vedrørende terrorfinansiering ikke nødvendigvis vil blive udløst i sektoren. De eksisterende IT-systemer er ikke nødvendigvis udstyret il at afsløre eftergjorte dokumenter. Hvor der er finansielle institutioner involveret, kan kontrollerne mht. terrorfinansiering betragtes som grundige, men nyere aktører på markedet som f.eks. telekommunikationsvirksomheder, som ikke er omfattet af forpligtelserne vedrørende bekæmpelse af hvidvask af penge og af finansiering af terrorisme, er mindre bevidste om risiciene og har mindre effektive kontrolsystemer. Finansielle efterretningsenheder har bemærket, at rapporter om mistænkelige transaktioner undertiden bliver indgivet for sent, hvilket stort set udelukker en nærmere efterforskning, da sporet af den mulige terrorist allerede er blevet koldt.

c) retsgrundlag og kontroller

Forbrugerkreditter/smålån er dækket af rammerne for bekæmpelse af hvidvask af penge og af finansiering af terrorisme på EU-plan, men de nationale lovgivninger varierer betydeligt, hvad angår kravene til dokumentation. Nogle medlemsstater kræver bestemte dokumenter, mens andre ikke gør. Når et lån bevilges af en bank, er risiciene ikke

nødvendigvis fuldstændig begrænsede, da midler indestående på en bankkonto kan hæves i en pengeautomat uden kontroller. Nye risici kan dukke op, når der bevilges lån med identifikation, der ikke sker ansigt til ansigt.

Som med andre finansielle produkter er sårbarheden over for terrorfinansiering større, hvor kunder med forbindelse til terrorgrupper ikke optræder på sanktionslister og derfor ikke udløser advarsler og faresignaler i banksektoren. Retshåndhævende myndigheder og virksomheder burde arbejde tættere sammen for at afsløre kunder, der potentielt kan udgøre en risiko mht. terrorfinansiering, før de begår terrorhandlinger.

Konklusion: Omfanget af transaktioner og de beløb, der er tale om, er som regel lave, men det reducerer ikke den iboende risiko for terrorfinansiering. De ineffektive varslings- og kontrolsystemer (til trods for eksisterende IT-ressourcer) bidrager yderligere til sårbarhed over for finansiering af terrorisme. Nogle nye markedsaktører er mindre bevidste om risiciene mht. terrorfinansiering end banksektoren. Forskellene mellem de nationale lovgivningsrammer viser, at kapaciteten hos kompetente myndigheder og finansielle efterretningsenheder til at afsløre mistænkelige transaktioner er begrænset, især i tilfælde, hvor lån ydes af ikkefinansielle virksomheder. Niveauet af sårbarhed over for finansiering af terrorisme i relation til smålån anses derfor for betydeligt (niveau 3).

Hvidvask af penge

Vurderingen sårbarhed over for hvidvask af penge i relation til forbrugerkredit/smålån har vist følgende resultater:

a) risikoeksponering

Trods de lave beløb kan sårbarheden være høj, hvis virksomhederne i sektoren ikke har passende overvågningssystemer til afsløring af sammenkædede transaktioner, eller hvis kunderne kan indfri lån med kontanter. Lave solvenstærskler for at kunne optage lån kan påvirke kundekendskabskravene for så vidt angår finansielle institutioner. Risikoen er højere, når lånene kommer fra ikkefinansielle institutioner, der ikke er omfattet af forpligtelserne i forhold til bekæmpelse af hvidvask af penge og af finansiering af terrorisme.

De kompetente myndigheder har identificeret risici mht. svig, der kommer fra distributionskanalerne, og som ofte involverer agenter, som virksomhederne finder det vanskeligt at overvåge. De kompetente myndigheder er også bekymret over risikoen for misbrug af kreditkort, risici mht. pengekurerer og fupkonti samt overførsler af penge fra cyberkriminalitet eller onlinebedrageri.

b) risikobevidsthed

Som mht. terrorfinansiering opvejes antagelsen om kun ringe risikoeksponering af, at sektoren på grund af de små beløb er mindre bevidst om risiciene mht. hvidvask af penge. Også her synes risikobevidstheden mere orienteret mod risikoen for svig end for hvidvask

af penge. Derfor bliver faresignalerne vedrørende hvidvask af penge ikke nødvendigvis udløst i sektoren, især ikke i tilfælde af førtidig indfrielse. Hvor der er finansielle institutioner involveret, kan kontrollerne mht. hvidvask af penge betragtes som grundige, men nyere aktører på markedet som f.eks. telekommunikationsvirksomheder, som ikke er omfattet af forpligtelserne vedrørende bekæmpelse af hvidvask af penge og af finansiering af terrorisme, er mindre bevidste og har mindre effektive kontrolsystemer.

c) retsgrundlag og kontroller

Forbrugerkreditter/smålån er dækket af rammerne for bekæmpelse af hvidvask af penge og af finansiering af terrorisme på EU-plan, men de nationale lovgivninger varierer betydeligt, hvad angår kravene til dokumentation. Nogle medlemsstater kræver bestemte dokumenter, mens andre ikke gør. Når et lån bevilges af en bank, er risiciene ikke nødvendigvis fuldstændig begrænsede, fordi midler indestående på en bankkonto kan hæves i en pengeautomat uden kontroller. Der kan forekomme ekstra risiko, hvor nye Fin-Tech virksomheder er indblandet, på grund af, at kundeforholdet ikke er-ansigt-til-ansigt.

Konklusion: Mens omfanget af transaktioner og de beløb, der er tale om, begrænser sektorens risikoeksponering, er sårbarheden højere, når lån ydes af ikkefinansielle virksomheder. Forskellene mellem de nationale lovgivningsrammer viser, at kapaciteten hos kompetente myndigheder og finansielle efterretningsenheder til at afsløre mistænkelige transaktioner er begrænset, især i tilfælde, hvor lån ydes af ikkefinansielle virksomheder. Niveauet af sårbarhed over for hvidvask af penge i relation til smålån anses derfor for i moderat grad betydelig (niveau 2).

Risikobegrænsende foranstaltninger:

Kommissionen:

- Forbedre samarbejdet mellem forpligtede enheder (primært finansielle institutioner) og retshåndhævende myndigheder med henblik på at forbedre effektiviteten af systemerne til overvågning af terrorfinansiering.

Medlemsstater / kompetente myndigheder:

- Tematiske inspektioner i sektoren med fokus på kontrolsystemer til afsløring af førtidsindfrielse af lån.

15. Realkredit og kreditter sikret ved pant i meget værdifulde

Produkt
Realkredit

Sektor
Kredit- og finanssektoren

Beskrivelse af risikoscenariet

Hvidvask af penge: Lovovertrædere skjuler og investerer udbyttet af kriminalitet ved at investere i fast-ejendom. Provenuet anvendes til deposita, afdrag og førtidsinfrielser.

Finansiering af terrorisme: Lovovertrædere bruger (mellemlange/langfristede, lavt-forrentede) lån med pant i meget værdifulde aktiver/realkreditlån til at finansiere sammensværgelser. Lån optages for relativt store beløb for at få adgang midler, som ikke kan spores, så længe pengene ikke bliver overført.

Trussel

Finansiering af terrorisme

Vurderingen af truslen om finansiering af terrorisme i relation til realkredit viser, at terrorgrupper finder metoden meget vanskelig at bruge og få adgang til. Kun i nogle få foreliggende tilfælde har terrororganisationer brugt den til at samle penge. Den stemmer ikke med deres behov, da den kræver avanceret viden og teknisk ekspertise ved fremskaffelsen af kompleks dokumentation. Hertil kommer, at formålet med realkredit er at give en tredjepart adgang til midler, så den giver ikke terrororganisationer let og hurtig adgang til midler, medmindre de har opbygget en ulovlig samvirken med en sådan tredjepart.

Konklusion: Realkredit kræver et højt niveau af viden og kompetencer for at forstå produktet og tilvejebringe den relevante dokumentation (eftergjorte dokumenter). Den er ikke attraktiv, idet den kræver medvirken af en tredjepart (modtageren af midlerne). Vurderingen af truslen om finansiering af terrorisme i relation til realkreditlån anses derfor for mindre betydelig (niveau 1).

Hvidvask af penge

Vurderingen af truslen om hvidvask i relation til realkredit viser, at organiserede kriminelle ofte har brugt denne metode. De er godt rustet til at tilvejebringe falsk dokumentation, og strukturen i pant i fast ejendom (med indragelse af tredjeparts-) bidrager til at skjule den virkelige modtager af midlerne. Realkredit er en let måde, hvorpå det bliver muligt for lovovertrædere at ejer flere ejendomme og for at skjule det sande omfang af deres aktiver. Denne metode bruges stadig i den indledende fase (mest til mindre beløb, da den ikke kræver sofistikerede operationer). Den anvendes dog oftere i kombination med, at den reelle ejer af den faste ejendom skjules bag en kompleks kæde af ejerskabsforhold.

Konklusion: I forbindelse med hvidvask af penge er realkreditlån et middel, som kriminelle organisationer sætter pris på. Den bidrager til, at de kan skjule omfanget af aktiver og og de reelle ejendomsforhold. Det kræver et moderat niveau af ekspertise. Truslen om hvidvask af penge i relation til realkredit anses derfor for betydelig (niveau 3).

Sårbarhed

Finansiering af terrorisme

Vurderingen af sårbarheden over for terrorfinansiering i relation til realkredit viser, at den ikke er sårbar over for risiciene mht. terrorfinansiering — de retshåndhævende myndigheder har kun konstateret få tilfælde (om overhovedet nogen). Kontrollerne mht. terrorfinansiering og risikobevidstheden er den samme som mht. detailbanker.

Konklusion: Mindre betydelig (niveau 1)

Hvidvask af penge

Vurderingen af sårbarhed over for hvidvask af penge i relation til realkredit viser følgende:

a) risikoeksponering

Den iboende risiko kan være høj på grund af den tætte forbindelse til fast-ejendomssektoren, som kriminelle organisationer foretrækker at bruge til at hvidvaske udbyttet af deres aktiviteter ved hjælp af transaktioner af store beløb-. Når kreditinstitutter deltager kan den iboende risiko være mindre, men sektoren er også udsat for højrisiko-kunder (f.eks. politisk eksponerede personer) og kan indbefatte grænseoverskridende-overførsler af midler.

b) risikobevidsthed

Bevidstheden i kreditinstitutter kan betragtes som høj og kontrollerne er grundigt. Endvidere kan andre aktører i sektoren (f.eks. notarer) bidrage til at begrænse risikoen. Bankerne kan ikke desto mindre stå over for interessekonflikter, hvor lempeligere kontroller tillader højrisikokunder at indløse større panter eller misligholdte lån.

Sårbarheden er højere, hvor handler med fast ejendom og tilhørende panter omfatter overførsler af penge fra en bankkonto i en medlemsstat med en svagere hvidvaskkontroller for højrisikokunder. Denne svaghed er knyttet til horisontale sårbarheder i tilsynet.

Der er et godt rapporteringsniveau og de finansielle efterretningsenheder og retshåndhævende myndigheder er udmærket bekendt med sårbarhederne i sektoren.

c) retsgrundlag og kontroller

Realkredit er omfattet af reglerne om bekæmpelse af hvidvask af penge og af finansiering af terrorisme på EU-niveau. Kontrollerne anses for at være ganske effektive, hvor realkreditlån ydes af kreditinstitutter. Endvidere kan andre deltagere i processen (f.eks. notarer) begrænse risiciene.

Konklusion: Når de udbydes af banker, er lån med pant i fast ejendom lige så sårbare som indskud på konti. Samspillet med ejendomssektoren øger generelt sårbarheden, men andre deltagere i transaktionerne, f.eks. notarer, kan begrænse sårbarheden. Vurderingen af truslen om hvidvask af penge i relation til realkreditlån anses derfor for i moderat grad betydelig (niveau 2).

Risikobegrænsende foranstaltninger:

Medlemsstater / kompetente myndigheder:

- Tematiske undersøgelser i sektoren med fokus på vurdering af kontrolsystemer til afsløring af førtidsindfrielse af lån og på effektiviteten af kundekendskabskrav, navnlig hvor der er højrisiko tredjelandskunder indblandet.

16. Livsforsikring

Produkt
Livsforsikring

Sektor
Forsikringssektoren

Generel beskrivelse af den pågældende sektor og det/den relevante produkt/aktivitet

Livsforsikringsselskaber tilbyder en række investeringsprodukter, med eller uden garantier, og indbefatter livsforsikringsydelser som en komponent. Set i forhold til de tegnede bruttopræmier er den mest dominerende dele af livsforsikringsvirksomheden i EØS livsforsikring tilknyttet investeringsfonde og indeksregulerede forsikringer, anden livsforsikring og gensidig forsikring.

Ifølge ECB's statistiske database udgjorde de samlede rapporterede aktiver tilhørende forsikringsselskaber i euroområdet i 3. kvartal 2018 7 984 mia. EUR, hvoraf ca. 3 305 mia. EUR tilhørte livsforsikringsselskaber (1 125 mia. EUR skadesforsikringsselskaber, 579 mia. EUR genforsikringsselskaber og 2 974 mia. EUR forsikringsselskaber, der tegner flere forsikringsklasser).

Ifølge data offentliggjort af den europæiske tilsynsmyndighed for forsikrings- og arbejdsmarkedspensionsordninger udgjorde livsforsikringspræmier i EU i 2017 876,2 mia. EUR.

I tillæg til reglerne om bekæmpelse af hvidvask af penge og af finansiering af terrorisme gælder der særlige bestemmelser, som har til formål at mindske de risici, der er forbundet med brug af livsforsikringsselskaber som investeringsredskab. Ifølge artikel 59 i direktiv 2009/138/EF (Solvens II) (hhv. art 323 i Kommissionens delegerede forordning (EU) 2015/35) er rimelige grunde til i forbindelse med den påtænkte erhvervelse (hhv. kvalificerede deltagelse af aktionæren eller medlemmet med kvalificeret deltagelse i den pågældende special purpose vehicle) at formode, at der foretages eller har været foretaget hvidvask af penge eller finansiering af terrorisme eller gøres eller har været gjort forsøg herpå, eller at den påtænkte erhvervelse (hhv. kvalificerede deltagelse) vil kunne øge risikoen herfor.

Beskrivelse af risikoscenariet

Lovovertrædere benytter svig med livsforsikringer- til at finansiere deres aktiviteter. Livsforsikingspolicer kan indløses før tid for at opnå udbetaling af tilbagekøbsværdien, navnlig i tilfælde, hvor provenuet kan overføres.

Risici mht. hvidvask af penge og terrorfinansiering i forsikringsbranchen relaterer sig navnlig til livsforsikrings- og kapitalpensionsprodukter. Disse giver en kunde mulighed for at placere midler i det finansielle system og potentielt skjule disses kriminelle oprindelse eller at finansiere illegale aktiviteter. Relevante risikoscenarier omfatter typisk

investeringsprodukter i forbindelse med livsforsikring (og ikke direkte produkter med udbetaling ved dødsfald).

Der kan opstå risiko, når:

1. et forsikringsselskab* accepterer en præmiebetaling i kontanter (dette er ikke almindelig praksis)
2. et forsikringsselskab tilbagebetaler, ved opsigelse eller tilbagekøb af policen, præmierne til anden konto end kilden til den oprindelige indbetaling (som indehaves af en anden part end forsikringstageren)
3. et forsikringsselskab gennemfører ikke "kend din kunde"-kravene generelt eller fastslår navnlig ikke kilden til investeringerne
4. et forsikringsselskab sælger policer, der kan overdrages (disse er usædvanligt)
5. investeringstransaktioner omfatter truster, fuldmagtshavere mv.
6. et forsikringsselskab sælger skræddersyede-produkter, hvor investor dikterer sammensætningen af den underliggende investering eller porteføljen, og/eller
7. et forsikringsselskab sælger i første omgang en lille police med opsparing, og investor foretager efterfølgende store investeringer uden at yderligere at blive omfattet af "kend din kunde"-krav.

I scenarierne 2, 4 og 6 ovenfor er der en direkte og indirekte risiko for finansiering af terrorisme.

Der er en risiko for hvidvask af penge i alle de ovennævnte scenarier. Lovovertrædere bruger risikoscenarierne 1, 6 og 7 til placering, 2 og 4 sløring og 2, 4, 6 og 7 til integration.

** Alle ovenstående scenarier kan angå et forsikringsselskab, dets agent eller mægler. For enkelhedens skyld refererer vi til "forsikringsselskab".*

Trussel

Finansiering af terrorisme

Vurderingen af truslen om terrorfinansiering i relation til livsforsikring viser viser, at terrorgrupper har begrænset interesse i denne metode. Den kræver en særlig viden om produktet og dets særlige karakteristika. Livsforsikringskontrakter er ikke let tilgængelige og forsikringsbegæringer kræver en mængde dokumentation, som let kan afskrække terroristgrupperinger. Udenlandske terrorkrigere kan tegne en livsforsikring og bede om, at pengene bliver udbetalt til fordel for deres familie i tilfælde af selvmord eller død i kamp. Medlemsstaternes lovgivning eller forsikringsselskabernes retningsliner for forsikringstegning tillader ofte ikke denne type klausul, så risikoen er ikke så stor.

Konklusion: Retshåndhævende myndigheder har kun i begrænset omfang dokumentation for, at livsforsikring misbruges til finansiering af terrorisme. Behovet for viden og planlægningsekspertise gør denne metode mindre attraktiv. Truslen om finansiering af terrorisme i relation til livsforsikring anses derfor for i moderat grad betydelig (niveau 2).

Hvidvask af penge

Vurderingen af truslen om hvidvask i relation til livsforsikring viser, at organiserede kriminelle organisationer kan bruge denne metode, men det er nødvendigt med komplekse arrangementer for at skjule udbytte fra kriminalitet (bankkonto i en forsikringspolice, flere konti i tredjelande fyldt med kontanter og anvendt som sikkerhed for et lån, at sende penge til livsforsikringspolice). Tilfælde eksisterer, men de er få og avanceret planlægning og viden er nødvendig for at gøre livsforsikring til en realistisk mulighed.

Konklusion: Der er afsløret nogle tilfælde af, at livsforsikring er blevet misbrugt til hvidvask af penge, men de er generelt et resultat af avancerede arrangementer. Truslen om hvidvask af penge i relation til erhvervslån anses derfor for i moderat grad betydelig (niveau 2).

Sårbarhed

Finansiering af terrorisme

Vurderingen af sårbarhed over for finansiering af terrorisme i relation til livsforsikring viser følgende:

a) risikoeksponering

Misbrug af livsforsikring drejer sig for det meste om anonym anbringelse af midler, ikke hævning af dem. Men risikoeksponeringen synes at være begrænset på grund af de pågældende transaktioners omfang. De fleste kompetente myndigheder vurderer det generelle niveau af risiko for terrorfinansiering som værende af ringe eller moderat betydning. De anser sektorens eksponering mht. risici for terrorfinansiering som følge af grænseoverskridende transaktioner og aktiviteter for ubetydelig.

b) risikobevidsthed

Sektoren synes at være temmelig uopmærksom på risici mht. terrorfinansiering. De fleste indberetninger om mistænkelige transaktioner bliver sendt ret sent i processen, fordi livsforsikringsselskaber har tendens til at vente, inden midlerne hæves, før der tages stilling til, om det er mistænkeligt. Forsikringsselskaber har typisk adgang til langt færre oplysninger om deres kunder end andre sektorer (f.eks. banker), hvilket reducerer deres mulighed for at opbygge omfattende risikoprofiler om kunderne. De manglende

transaktioner betyder, at mistænkelig aktivitet hovedsagelig opdages på grundlag af "usædvanlig adfærd", og risikoen for terrorfinansiering fastlås ved starten af forholdet.

c) retsgrundlag og kontroller

Livsforsikring er omfattet af reglerne om bekæmpelse af hvidvask af penge og af finansiering af terrorisme på EU-niveau.

De kompetente myndigheder vurderer kvaliteten af kontrollerne i denne sektor som overvejende gode eller meget gode. De svagheder, de konstaterede, angik især kvaliteten af både hele branchens og de individuelle risikovurderinger og de dermed forbundne mangler i relation til overvågning og identifikation samt indberetning af mistænkelige transaktioner.

Konklusion: Risikobevidstheden i sektoren er lav, men risikoeksponeringen er også lav. Der er meget få sager på grund af den begrænsede interesse for produktet. Niveauet af sårbarhed over for finansiering af terrorisme i relation til livsforsikring anses derfor for at være mindre/i moderat grad betydelig (niveau 1-2).

Hvidvask af penge

Vurderingen af sårbarhed over for hvidvask af penge i relation til livsforsikring viser følgende:

a) risikoeksponering

Misbrug af livsforsikring drejer sig for det meste om anonym anbringelse af midler, ikke hævning af dem. Men risikoeksponeringen synes at være ret begrænset på grund af de pågældende transaktioners omfang. De fleste kompetente myndigheder vurderer det generelle niveau af risiko for hvidvask af penge som værende af ringe eller moderat betydning. De anser sektorens eksponering mht. risici for hvidvask af penge som følge af grænseoverskridende transaktioner og aktiviteter for ubetydelig.

b) risikobevidsthed

Sektoren er ganske bevidst om risiciene mht. hvidvask af penge. Forsikringsselskaber har imidlertid typisk adgang til langt færre oplysninger om deres kunder end andre sektorer (f.eks. banker), hvilket reducerer deres mulighed for at opbygge omfattende risikoprofiler om kunderne. De manglende transaktioner betyder, at mistænkelig aktivitet hovedsagelig opdages på grundlag af "usædvanlig adfærd", og risikoen for hvidvask af penge fastlås ved starten af forholdet.

c) retsgrundlag og kontroller

Tjenesterne ydes for de meste gennem bankkonti, som generelt er omfattet af effektive kontroller. De kompetente myndigheder vurderer kvaliteten af kontrollerne i sektoren som overvejende gode eller meget gode. De svagheder, de konstaterede, angik især kvaliteten af både hele branchens og de individuelle risikovurderinger og de dermed forbundne mangler i relation til overvågning og identifikation samt indberetning af mistænkelige transaktioner.

Som i andre sektorer er Fin-Tech og Reg-Tech-løsninger ved at bliver mere udbredte i sektoren. Disse anses af adskillige kompetente myndigheder for at udgøre en ny risiko; myndighederne er bekymrede over den manglende opmærksomhed omkring (og til tider mangel på) tilsynskrav vedrørende bekæmpelse af hvidvask af penge og af finansiering af terrorisme mht. Reg-Tech-løsninger og Fin-Tech-ydelser. En hertil knyttet ny risiko, som de kompetente myndigheder har konstateret, er sektorens overgang til webbaserede forsikringsplatforme og de hermed forbundne udfordringer i forbindelse med konti, som åbnes uden kundens fysiske tilstedeværelse.

Konklusion: Livsforsikring er på nuværende tidspunkt godt reguleret, og sektoren synes at være ganske bevidst om risiciene mht. hvidvask af penge. De eksisterende kontroller udføres korrekt. Niveauet af sårbarhed over for hvidvask af penge i relation til livsforsikring anses derfor for mindre/i moderat grad betydelig (niveau 1-2). Når livsforsikringsprodukter bruges som investeringsprodukter til formueforvaltning eller anden investeringsservice, bør det relevante risikoniveau overvejes.

Risikobegrænsende foranstaltninger:

Der forslås ikke yderligere på nuværende tidspunkt.

17. Skadesforsikring

Produkt
Skadesforsikring

Sektor
Forsikringssektoren

Generel beskrivelse af den pågældende sektor og det/den relevante produkt/aktivitet

Skadesforsikringspolicer er almindeligvis korterevarende og tjener til at tilvejebringe beskyttelse mod uventede tab, f.eks. skader på ejendom. De er baseret på bruttopræmier, og de dominerende dele af skadesforsikringsvirksomheden er dem, der er knyttet til ansvarsforsikring af motorkøretøjer, brandforsikring og anden forsikring af fast ejendom samt sundhedsudgifter.

Ifølge ECB's statistiske database udgjorde de samlede rapporterede aktiver tilhørende forsikringsselskaber i euroområdet i 3. kvartal 2018 7 984 mia. EUR, hvoraf ca. 1 125 mia. EUR tilhørte skadesforsikringsselskaber (3 305 mia. EUR skadesforsikringsselskaber, 579 mia. EUR genforsikringsselskaber og 2 974 mia. EUR forsikringsselskaber, der tegner flere forsikringsklasser).

Præmierne på det største skadesforsikringsmarked, motorkøretøjsforsikring, udgjorde ifølge data offentliggjort af Insurance Europe 137,5 mia. EUR i 2017, efterfulgt af præmierne for ejendomsforsikring (101,5 mia. EUR), ulykkesforsikring (36,1 mia. EUR) og almindelig ansvarsforsikring (40,1 mia. EUR); præmierne for sundhedsforsikringer udgjorde 131,5 mia. EUR.

Der gælder der særlige bestemmelser, som har til formål at mindske de risici, der er forbundet med at besidde aktier i forsikringsselskaber. Ifølge artikel 59 i direktiv 2009/138/EF (Solvens II) (hhv. art 323 i Kommissionens delegerede forordning (EU) 2015/35) er rimelige grunde til i forbindelse med den påtænkte erhvervelse (hhv. kvalificerede deltagelse af aktionæren eller medlemmet med kvalificeret deltagelse i den pågældende special purpose vehicle) at formode, at der foretages eller har været foretaget hvidvask af penge eller finansiering af terrorisme eller gøres eller har været gjort forsøg herpå, eller at den påtænkte erhvervelse (hhv. kvalificerede deltagelse) vil kunne øge risikoen herfor.

Beskrivelse af risikoscenariet

Lovovertrædere udøver svig mht. arbejdsplads- og bilforsikring mv. med henblik på at finansiere deres aktiviteter.

Hvidvask af penge kan ske i forbindelse med og som motiv bag forsikringssvig med skadesforsikring, f.eks. hvor dette fører til et krav om at få dækket en del af de investerede illegale midler. Relevante risikoscenarier indeholder typisk højfrekvente-præmier og opsigelser. Der kan opstå risici, eller disse kan blive en realitet, når et forsikringsselskab*:

1. accepterer en præmiebetalinger i kontanter, selvom dette ikke er almindelig praksis, eller
2. tilbagebetaler, ved opsigelse eller tilbagekøb af policen, præmierne til anden konto end kilden til oprindelige indbetaling (som indehaves af en anden part end forsikringstageren)

Hvidvaskere af penge forsøger at bruge scenarie 1 til placering og scenarie 2 til lagring sløring/integration.

** Ovenstående eksempler kan angå et forsikringsselskab, dets agent eller mægler. For enkelhedens skyld refererer vi til "forsikringsselskabet".*

Trussel

Finansiering af terrorisme

Ligeledes angår risikoen vedrørende terrorfinansiering forsikringssvig med henblik på at få adgang til indtægtskilder til brug for terroraktiviteter. Sådanne arrangementer er blevet afsløret i forbindelse med arbejdspladsforsikring og bilforsikring. Det er vanskeligt at sige, at denne metode ikke er relevant, og efter terrorangreb er der indsamlet nogle beviser for dens anvendelse, men den kræver en vis planlægning og meget papirarbejde, hvilket gør den relativt uinteressant for terrorgrupper. Men vi kan for sammenligningens skyld sige, at den er på samme niveau af trussel om terrorfinansiering som livsforsikring.

Konklusion: Retshåndhævende myndigheder har kun i begrænset omfang dokumentation for, at skadesforsikring misbruges til finansiering af terrorisme. Den kræver viden og planlægningsekspertise, hvilket gør den relativt uattraktiv. Truslen om finansiering af terrorisme i relation til skadesforsikring anses derfor for i moderat grad betydelig (niveau 2).

Hvidvask af penge

Vurderingen af truslen om hvidvask af penge i relation til skadesforsikring (f.eks. bil- eller arbejdspladsforsikring) viser, at til forskel fra finansiering af terrorisme kræver hvidvask af penge sofistikerede arrangementer, der gør risikoscenariet utilstrækkeligt sikkert eller attraktivt. Retshåndhævende myndigheder har ingen konkrete beviser for, at skadesforsikring bruges til at hvidvaske udbyttet af kriminalitet.

Konklusion: Skadesforsikring bliver ikke brugt til hvidvask af penge, da forsikringsformen kræver en vis planlægning og ekspertise, hvilket gør den forholdsvis uattraktiv. Truslen om hvidvask af penge i relation til skadesforsikring anses derfor for mindre betydelig/uden betydning (niveau 1).

Sårbarhed

Finansiering af terrorisme

Vurderingen af truslen om hvidvask af penge i relation til skadesforsikring (f.eks. bil- eller arbejdspladsforsikring) viser, at der vil kunne forekomme to tilfælde:

(i) sort arbejde på motorkøretøj/bilforsikringssvig: midler fra svig sendes ved kontant overførsel; og

(ii) biler bliver stukket i brand for at opnå forsikringsudbetaling-.

a) risikoeksponering

Risikoeksponeringen er begrænset, da der er tale om enorme pengesummer, og da man ikke kan få fat på midlerne uden forudgående identifikation.

b) risikobevidsthed

Generelt er skadesforsikring mere sårbar end livsforsikring, da sektoren ikke nødvendigvis er klar over risiciene (kundekendskabskrav er ikke gennemført, og der er ingen journalisering-), eller særlige faresignaler vedrørende finansiering af terrorisme eller hvidvask af penge bliver ikke altid udløst. Forsikringsgiver har tendens til at være mere opmærksomme på tidspunktet for udbetaling, hvor risikoen opfattes som større.

c) retsgrundlag og kontroller

Skadesforsikring er omfattet af reglerne om bekæmpelse af hvidvask af penge og af finansiering af terrorisme på EU-niveau. Når medlemsstaterne har regler, synes kontrollerne (i nogle tilfælde med bl.a. egenerklæringer) at fungere tilfredsstillende.

Konklusion: I mange medlemsstater har lovgivning ført til, at der bliver udført kontroller, og at bevidstheden i sektoren er blevet øget. Der er dog stadig nogle svagheder mht. afsløring og indberetning af mistænkelige transaktioner. Niveauet af sårbarhed over for finansiering af terrorisme i relation til skadesforsikring anses derfor for i moderat grad betydeligt (niveau 2).

Hvidvask af penge

Vurderingen af sårbarheden over for hvidvask af penge i relation til skadesforsikring (f.eks. bil- eller arbejdspladsforsikring) viser:

a) risikoeksponering

For det meste misbruges skadesforsikring kan til hvidvask af penge i en bredere kontekst af svig (falske investeringer, tomme selskaber).

b) risikobevidsthed

Gennemførelsen af kundekendskabskrav er ikke udbredt i EU, men når medlemsstater har en ordning for bekæmpelse af hvidvask af penge i forhold til skadesforsikring, bemærker de, at forpligtede enheder er tilbøjelige til ikke at gennemføre nogen kundekendskabskrav overhovedet. Men i betragtning af det antal sager, er er tale om, er der intet, der tyder på, at det forøger risikoen for hvidvask af penge.

c) retsgrundlag og kontroller

Der gælder ingen EU-krav om at lade skadesforsikring blive omfattet af reglerne om bekæmpelse af hvidvask af penge finansiering af terrorisme De retlige rammer omkring skadesforsikring afhænger af national lovgivning.

Konklusion: Der er kun afsløret nogle få tilfælde af, at skadesforsikring er blevet misbrugt til hvidvask af penge. Generelt gøres dette som en del af et mere omfattende svindelarrangement. Niveauet af sårbarhed over for hvidvask af penge i relation til skadesforsikring anses derfor for mindre betydeligt(niveau 1)/uden betydning.

Risikobegrænsende foranstaltninger:

Der forslås ikke yderligere på nuværende tidspunkt.

18. Boksudlejning

Produkt
Bankboksudlejning

Sektor
Kredit- og finanssektoren og private sikkerhedsvirksomheder

Beskrivelse af risikoscenariet

Lovovertrædere lejer mange (kommercielle eller bank-) bokse til at opbevare store mængder valuta, monetære instrumenter eller værdifulde aktiver, indtil de kan veksles til penge med henblik på placering i banksystemet. Ligeledes kan de etablere mange bokskonti til at parkere store mængder sikkerheder, indtil de sælges og konverteres til valuta, pengeinstrumenter, udgående pengeoverførsler eller en kombination af disse, med henblik på placering i banksystemet. Frizoner kan bruges til afskærme ulovlige aktiviteter og udbytterne af dem.

Trussel

Finansiering af terrorisme

Truslen om terrorfinansiering i relation til boksudlejning anses ikke for relevant. Derfor er dette ikke en del af vurderingen.

Konklusion: Ikke relevant

Hvidvask af penge

Vurderingen af truslen om hvidvask af penge i relation til boksudlejning viser, at et karakteristisk træk ved dette scenarie er, at aktiverne bliver gemt og ikke nødvendigvis konverteret. Som følge heraf kan det være, at metoden ikke er økonomisk attraktiv. Men den gør det muligt at skjule udbytte af kriminalitet uden risiko for afsløring. Ifølge de retshåndhævende myndigheder bliver disse "sovende" depotsystemer i stadig højere grad brugt til at foretage sikre indbetalinger og bringe aktiver ud af det finansielle system.

Nøjagtige data er svære at tilvejebringe, fordi boksudlejning også bruges til pårørende. Det er et yderligere aspekt af hvidvasktruslen, idet den person, der har indbetalt penge, ikke nødvendigvis vil være den, der hæver dem.

Også andre aktører på markedet end banker stiller sådanne ydelser (opbevaringsfaciliteter) til rådighed, hvilket udvider det spektrum af værktøjer, der er til rådighed for kriminelle organisationer, og hæver trusselsniveauet.

Konklusion: Mange medlemsstater har bemærket en stigende tendens i kriminelle organisationers brug af denne metode til at skjule udbyttet af kriminalitet. Boksudlejning er ganske attraktiv, fordi den ikke kræver særlig ekspertise og er et rimelig sikkert værktøj til at undgå skattekontrol eller kontroller mht. bekæmpelse

af hvidvask af penge. Truslen om hvidvask af penge i relation til boksudlejning anses derfor for betydelig (niveau 3).

Sårbarhed

Finansiering af terrorisme

Sårbarheden over for terrorfinansiering i relation til boksudlejning anses ikke for specielt relevant. Derfor er sårbarheden over fra terrorfinansiering ikke en del af vurderingen.

Konklusion: Ikke relevant.

Hvidvask af penge

Ved vurderingen af sårbarheden over for hvidvask af penge i relation til boksudlejning bør der skelnes mellem ydelser, der stilles til rådighed af kreditinstitutter, og dem, der stilles til rådighed af enheder, der ikke er banker (opbevaringsfaciliteter).

a) risikoeksponering

I begge tilfælde er risikoeksponeringen høj, fordi der er tale om store summer. Niveauet af risikoeksponering vil kunne være større, når højrisikokunder er indblandet.

b) risikobevidsthed

Grundlæggende aspekter af kundekendskabskravet finder anvendelse på boksudlejning foretaget af kreditinstitutter. Nogle kompetente myndigheder tage en proaktiv tilgang i denne sektor, men bankerne er stadig sårbare med hensyn til indholdet af af boksene. Generelt har de ingen oplysninger om de midler, der er placeret i dem. De private virksomheder, der leverer de pågældende ydelser, efterlever ikke alle kravene til bekæmpelse af hvidvask af penge og af finansiering af terrorisme, og nogle tager imod kontant betaling for leje af bokse. Et andet spørgsmål er, om risikoen for terrorfinansiering opstår på tidspunktet for oplagringen eller først, når midlerne indføres i realøkonomien. Fra et retshåndhævelsesperspektiv er det desto lettere at bevare anonymiteten i forbindelse med en transaktion, flere midler der opbevares.

c) retsgrundlag og kontroller

Boksudlejning og frizonetilflugt er som sådan ikke omfattet af den retlige ramme for bekæmpelse af hvidvask af penge og af finansiering af terrorisme på EU-niveau. Men boksudlejning foretaget af kredit- og finansielle institutioner er omfattet af de rammer, som gælder for disse forpligtede enheder. Virksomheder, der foretager boksudlejning som anført i punkt 14 i bilag I til direktiv 2013/36/EU er udtrykkeligt omfattet af reglerne om bekæmpelse af hvidvask af penge og af finansiering af terrorisme. I praksis er finansielle institutioner imidlertid ikke altid i stand til at opfylde deres overvågningsforpligtelser og vurdere de finansielle kilder, da de ikke er bekendt med indholdet af boksene. Desuden

omfatte det ikke kommercielle oplagringsvirksomheder eller andre lagerfaciliteter, som kan benyttes til tilsvarende ydelser. I nogle lande er visse oplagrings-/boksleje-ydelser reguleret generelt og kontrolleres som sådan.

Konklusion: Når de foretages af kredit- og finansielle institutioner er boksudlejning omfattet af kundekendskabskrav og kontrol. Det er dog ikke altid muligt at fastslå den nøjagtige kilde til midlerne, og den løbende overvågning kan have en blind plet, idet finansieringsinstituttet sædvanligvis er uvidende om indholdet. Derudover kan bokse være tilgængelige for andre end den oprindelige kunde, hvilket øger sårbarheden. Markedet er fragmenteret af fremkomsten af private enheder og andre kommercielle boksudlejningstjenester. Niveauet af sårbarhed over for hvidvask af penge anses for i moderat grad betydeligt/betydeligt (niveau 2-3).

Risikobegrænsende foranstaltninger:

Medlemsstater / kompetente myndigheder:

- Tematiske inspektioner i sektoren med fokus på effektiviteten af de kundekendskabskrav, der gælder for finansielle og ikkefinansielle institutioner, som tilbyder boksudlejning.

1. Oprettelse af juridiske enheder og juridiske arrangementer

Produkt/tjenesteydelse
Oprettelse af juridiske enheder og juridiske arrangementer

Sektor
Udbydere af tjenester til truster eller selskaber, retlige aktører, skatterådgivere/regnskabssagkyndige/revisorer, udbydere af rådgivning om kapitalstruktur og branchestrategi, rådgivning og ydelser vedrørende fusioner og opkøb og rådgivning om forretningsstrategi ("professionelle formidlere")

Generel beskrivelse af den pågældende sektor og det/den relevante produkt/aktivitet

Udbydere af tjenester til truster eller selskaber, retlige aktører, skatterådgivere/regnskabssagkyndige/revisorer og udbydere af rådgivning om kapitalstruktur og branchestrategi, rådgivning og ydelser vedrørende fusioner og opkøb og rådgivning om forretningsstrategi leverer en lang række tjenesteydelser til privatpersoner og virksomheder om forretningsvirksomhed og formueforvaltning.

Det fjerde direktiv om bekæmpelse af hvidvask af penge kræver, at enheder identificerer den reelle ejer, når de indgår en forretningsforbindelse og tager risikobaserede og passende forholdsregler til at kontrollere identiteten af de reelle ejere som defineret i artikel 3, stk. 6.

I tillæg til lovgivning om hvidvask af penge er der i følgende selskabsretlige EU-direktiver fastsat generelle regler om etablering af selskaber med begrænset ansvar, navnlig med hensyn til kapital og oplysningskrav. Europæisk selskabsret er delvis kodificeret i direktiv 2017/1132/EF[49] om visse aspekter af selskabsretten, og medlemsstaterne har fortsat separate selskabslovgivninger, som ændres fra tid til anden for at være i overensstemmelse med EU's direktiver og forordninger.

Direktiv 2017/1132/EU dækker:

1. Offentlighed omkring selskabsdokumenter, gyldigheden af et selskabs forpligtelser samt ugyldighed. Det gælder for alle aktieselskaber og andre selskaber med begrænset ansvar.
2. **Stiftelse** af aktieselskaber og regler om **bevarelse af og ændring af deres kapital**. Det sætter et minimumskapitalkrav for EU-aktieselskaber på 25 000 EUR.

3. Oplysningskrav til **udenlandske filialer** af selskaber. Det dækker EU-selskaber, som etablerer sig i et andet EU-land eller virksomheder fra tredjelande, der opretter filialer i EU.

Derudover opstiller direktiv 2009/102/EF[50] på selskabsskattens område om enkeltmandsselskaber med begrænset ansvar regler for etablering af et **enkeltmandsselskab** (hvor alle anparter ejes af en enkelt anpartshaver). Det omfatter anpartsselskaber, men EU-landene kan beslutte at udvide de til at omfatte aktieselskaber. Det erstatter direktiv 89/667/EØF (Rådets 12. selskabsdirektiv).

- Direktivet opstiller også regler for etablering af et **enkeltmandsselskab** (hvor alle anparter ejes af en enkelt anpartshaver). Det omfatter anpartsselskaber, men EU-landene kan beslutte at udvide de til at omfatte aktieselskaber. Det erstatter direktiv 89/667/EØF.

Reglerne om stiftelse, kapital og oplysningskrav suppleres af **regler om bogføring og regnskabsrapportering.**[51]

Børsnoterede selskaber skal også opfylde visse **krav om gennemsigtighed.**[52]

Beskrivelse af risikoscenariet

Lovovertrædere opretter komplekse strukturer, der involverer mange forskellige jurisdiktioner, herunder navnlig offshore-jurisdiktioner med hemmelighedsfulde kæder af ejerskabsforhold, normalt via skuffeselskaber,[53] hvor ejeren af et selskab eller en anden juridisk struktur er registreret andetsteds. Der bliver udpeget strømænd, og de kan kun fremstå som ledere af selskabet ved at skjule forbindelsen med den virkelige reelle ejer. Ved at benytte offshoreselskaber kan lovovertræderne forblive anonyme, bringe midler, der stammer fra kriminel aktivitet, tilbage i det legale økonomiske kredsløb og begå skattesvig og skatteunddragelse og andre aktiviteter, der kan skade statshusholdningen, eller skjule kilderne til midlerne.

Det indbærer, at der skabes "uigennemsigtige strukturer", der defineres som strukturer, hvor den sande identitet af den eller de endelige reelle ejer(e) af selskaber og arrangementer i den pågældende struktur er tilsløret, f.eks. gennem brug af proformadirektører. I sådanne tilfælde er det kun proformadirektøren, der fremstår som den reelle ejer af selskabet. Disse ordninger gør brug af offshore-jurisdiktioner med svage regelsæt vedrørende bekæmpelse af hvidvask af penge og af finansiering af terrorisme, og det tiltrækker store investeringer. Den globale offshore-formue var i 2017 på ca. 8,2 billioner USD, 6 % højere end året før

[50] Europa-Parlamentets og Rådets Direktiv 2009/102/EF af 16. september 2009 på selskabsrettens område om enkeltmandsselskaber med begrænset ansvar (EØS-relevant tekst), EUT L 258 af 1.10.2009, s. 20.
[51] Selskabsrapportering: https://ec.europa.eu/info/business-economy-euro/company-reporting-and-auditing/company-reporting_en.
[52] Værdipapirmarkeder: https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-markets/securities-markets_en.
[53] En oversigt over skuffeselskaber i Den Europæiske Union: http://www.europarl.europa.eu/RegData/etudes/STUD/2018/627129/EPRS_STU(2018)627129_EN.pdf.

målt i amerikanske dollar.[54] Et foreløbigt skøn over offshore-formue tilhørende personer hjemmehørende i EU var 1,6 billioner USD i 2016.[55]

Generel bemærkning

For dette risikoscenarie omfatter vurderingen juridiske enheder som selskaber, selskabskonstruktioner, fonde, foreninger, nonprofitorganisationer, velgørenhedsorganisationer og lignende strukturer. Det dækker også truster og andre juridiske arrangementer med en lignende struktur eller funktion (f.eks. *fiducie*, *Treuhand*, *fideicomiso* …). Risikovurderingen angår aktivitetens art og ikke strukturen som sådan. Denne tilgang anfægter ikke de juridiske enheders særlige karakter i forhold til juridiske arrangementer (sidstnævnte har ikke status som juridiske personer og er grundlæggende et kontraktforhold). Hvad angår arten af den pågældende ydelse (her oprettelsen af strukturen) gør disse særlige forhold ikke nogen afgørende forskel, idet juridiske enheder og retlige arrangementer kan bruges på samme måde for til at skjule de sande reelle ejere. Hvilken type struktur, lovovertrædere foretrækker, afhænger af de juridiske regler i en given jurisdiktion, arten af lovovertrædernes ekspertise samt praktiske forhold. Organiserede kriminelle grupper kan let oprette alle disse strukturer, og de vil alle kunne være redskaber til at skabe uigennemskuelige og komplicerede ordninger, der gør det vanskeligere at identificere den reelle ejer og midlernes virkelige oprindelse.

Trussel

Finansiering af terrorisme

Lovovertrædere ønsker at oprette uigennemsigtige strukturer, hvorved man kan omgå eventuelle eksisterende restriktive forholdsregler. Vurderingen af truslen om terrorfinansiering i relation til oprettelsen af juridiske enheder og juridiske arrangementer viser, at terrororganisationer kan have svært ved at oprette de pågældende strukturer. Det er fordi disse terrororganisationer sædvanligvis optræder på sanktionslisterne. Jo mere terrororganisationen ønsker at skjule sin identitet som reel ejer, jo mere sofistikeret skal den proces være. Viden om både nationale og internationale love og skatteregler er nødvendig for at kunne oprette disse strukturer, som indebærer en høj grad af viden, der kun kan stilles til rådighed af professionelle formidlere. Retshåndhævende myndigheder og finansielle efterretningsenheder har imidlertid identificeret nogle enkle metoder, ved hjælp af hvilke lovovertrædere bruger bankkonti og professionelle formidlere til at hjælpe dem med let og hurtigt at etablere strukturer for at samle penge til finansiering af terrorvirksomhed. Derfor er evnen til at oprette juridiske enheder og juridiske arrangementer relevante for truslen om terrorfinansiering, selvom de retshåndhævende myndigheder kun har indberettet et begrænset antal af disse tilfælde.

Konklusion: Der er kun konstateret få tilfælde af anvendelse af disse metoder til finansiering af terror. Dette kan skyldes, at den nødvendige høje grad af teknisk

[54] Global Wealth 2018 report by The Boston Consulting Group: http://image-src.bcg.com/Images/BCG-Seizing-the-Analytics-Advantage-June-2018-R-3_tcm9-194512.pdf.

[55] Forestående undersøgelse udarbejdet af ECOPA og CASE: "*Estimating International Tax Evasion by Individuals*".

ekspertise og viden afskrækker terrororganisationer, som ville foretrække enklere og mere tilgængelige løsninger. Trusselsniveauet for finansiering af terrorisme i relation til oprettelsen af juridiske strukturer anses derfor for i moderat grad betydeligt (niveau 2).

Hvidvask af penge

Vurderingen af truslen om hvidvask af penge i relation til oprettelsen af juridiske enheder og juridiske arrangementer viser, at dette værktøj næsten udelukkende bruges til at skjule og sløre de reelle ejerforhold. Fra et omkostningsperspektiv oprettelsen af en retlig enhed eller et retligt arrangement forholdsvis ligetil og kan gøres online. Skuffeselskaber med en generelt formuleret formålsbestemmelse og ingen aktiviteter er meget almindelige. Skuffeselskaber, der allerede har været i drift i et par år, hvis aktier er overført til nye aktionærer er dyrere, men også mere eftertragtede af kriminelle. Stiftelser er også attraktive, idet der ikke gennemføres nogen kontrol af midlerne fra kompetente myndigheders side. Alle de pågældende enheder er uden reelle erhvervsmæssige aktiviteter. Visse omkostninger eller et højere niveau af ekspertise/planlægning kan være påkrævet, hvis kriminelle organisationer benytter mellemled for at skabe mere komplekse strukturer, f.eks. Arbejder med mere end ét land for bedre at skjule ejernes sande identitet. Viden om nationale og internationale love og regler er nødvendig for at kunne oprette disse strukturer, som indebærer en høj af grad viden, der kun kan stilles til rådighed af professionelle formidlere. Komplekse kæder af ejerskab i forskellige lande øger uigennemsigtigheden af pengehvidvasken. Så længe brugen af mellemled efter oprettelsen af selve strukturen er tilstrækkeligt til at skjule de reelle ejerforhold, er det en attraktiv og ret sikker metode til at hvidvaske udbyttet af kriminalitet.

Finansielle efterretningsenheder og retshåndhævende myndigheder mener, at kriminelle organisationer jævnligt bruger denne metode. En organiseret kriminel gruppering kan anvende flere slags professionelle hjælpere afhængigt af opgaven. Dette har været et centralt element i de fleste af de sager, der er indberettet til Europol, hvor systemer til hvidvask af penge hjælpes på vej af professionelle fra forskellige brancher, som regel en advokat og en revisor. For eksempel bruges økonomiske rådgivere til at designe en mekanisme til at integrere kriminelle kontanter i det legale økonomiske kredsløb, og advokater finder en juridisk legitimering af disse aktiviteter. Dette er forklaringen på kompleksiteten af de eksisterende hvidvaskmekanismer og behovet for ekspertviden til at opbygge dem og undgå at blive afsløret.

Konklusion: Selvom oprettelsen af juridiske enheder og juridiske arrangementer ikke kan isoleres fra selve de forretningsmæssige aktiviteter, vurderes dette risikobillede at være et lukrativt værktøj til hvidvaske udbyttet af kriminalitet. Trusselsniveauet for hvidvask af penge i relation til oprettelsen af juridiske strukturer anses derfor for i betydeligt/meget betydeligt (niveau 3/4).

Sårbarhed

Finansiering af terrorisme

Vurderingen af sårbarheden over for terrorfinansiering i relation til oprettelsen af juridiske enheder og juridiske arrangementer udviser følgende karakteristika:

a) risikoeksponering

Risikoeksponeringsaspektet er det forhold, at juridiske enheder og juridiske arrangementer under visse omstændigheder let kan oprettes på afstand og uden særlige identifikationskrav (gennem usikrede fordelingskanaler). Processen kan være fuldstændig anonym, og professionelle formidlere kan uforvarende blive misbrugt af terroristgrupper i højrisikoområder til at oprette en struktur uden noget legitimt formål. I andre situationer kan oprettelsen af strukturer, der ikke sker ansigt til ansigt, involvere professionelle formidlere, der er placeret uden for EU. I det tilfælde er adgangsporten til at konstatere, hvem der er den reelle ejer, det finansieringsinstitut, der har ansvaret for åbning af bankkontoen. Endelig vil nogle mellemled eller tredjeparter kunne sørge for dedikerede ydelser, der har til formål at skjule de reelle ejerforhold, og det kan gå ud over et helt erhverv, som vil kunne blive betragtet som medskyldig i at oprette disse finansieringssystemer for terrorister.

b) risikobevidsthed

Generelt synes professionelle formidlere at være klar over risikoen for at blive misbrugt gennem illegitime anmodninger om at oprette juridiske enheder og juridiske arrangementer. Risikoen for, at disse strukturer kan bruges til at skjule den reelle ejer er velkendt. Men da oprettelsen af juridiske enheder og juridiske arrangementer i henseende til terrorfinansiering også kan være baseret på lovlige penge, bliver faresignalerne er ikke altid udløst korrekt. Der kan være professionelle fra flere sektorer involveret i oprettelsen af disse strukturer, og de kompetente myndigheder er ikke altid i stand til at sørge for ordentlig vejledning til disse brancher.

c) retsgrundlag og kontroller

Regnskabssagkyndige og revisorer, skatterådgivere og retlige aktører (fra 2001), udbydere af tjenester til truster eller selskaber (fra 2005) og udbydere af rådgivning om kapitalstruktur og branchestrategi, rådgivning og ydelser vedrørende fusioner og opkøb og rådgivning om forretningsstrategi (fra 2005) er omfattet af EU's regler om bekæmpelse af hvidvask af penge.

På baggrund af niveauet for indberetning af mistænkelige transaktioner mener de kompetente myndigheder, at de eksisterende kontroller stadig er utilstrækkelige, og at de oplysninger, der modtages i begyndelsen af forretningsforbindelser, ikke er tilstrækkeligt udbyggede til, at man kan opdage og analysere de risici for terrorfinansiering, der forbundet med oprettelsen af juridiske enheder og juridiske arrangementer.

EU-medlemsstater har forskelligartede regler og beskatningssystemer, der kan udnyttes af terrororganisationer. At håndhæve kravene om identifikation af den reelle ejer i begyndelsen af et forretningsforhold er fortsat en vigtig udfordring for de berørte enheder. Selvom det er svært at kæde skuffeselskaber sammen med deres ejere, er sikkerhedseksperter og retshåndhævende embedsmænd enige om, at skuffeselskaber og andre juridiske enheder som truster udgør en trussel mod den nationale sikkerhed. De gør

det næsten umuligt at finde de folk, der faktisk finansierer terrorisme og andre kriminelle aktiviteter, og kan være ideelle redskaber for finansiering af terrorister.[56]

Mht. udbydere af rådgivning om kapitalstruktur og branchestrategi samt rådgivning og tjenesteydelser vedrørende fusioner og opkøb og rådgivning om forretningsstrategi foreligger der ingen information om, hvordan de overvåges af de kompetente myndigheder, og om de overholder reglerne om bekæmpelse af hvidvask af penge og terrorfinansiering.

Konklusion: Selvom det ikke nødvendigvis er den metode, der hyppigst bruges til terrorfinansiering, anses sårbarheden over for terrorfinansiering i relation til oprettelsen af juridiske strukturer som betydelig/meget betydelig (niveau 3/4).

Hvidvask af penge

Vurderingen af sårbarheden over for hvidvask af penge i relation til oprettelsen af juridiske enheder og juridiske arrangementer udviser følgende karakteristika:

a) risikoeksponering

Det vigtigste aspekt af risikoeksponeringen er det forhold, at juridiske enheder og juridiske arrangementer under visse omstændigheder let kan oprettes på afstand og uden særlige identifikationskrav (gennem usikrede fordelingskanaler). Processen kan være fuldstændig anonym, og professionelle formidlere kan uforvarende blive misbrugt af kriminelle organisationer i højrisikoområder til at oprette en struktur uden noget legitimt formål. I andre situationer kan oprettelsen af strukturer, der ikke sker ansigt til ansigt, involvere professionelle formidlere, der er placeret uden for EU. I det tilfælde er adgangsporten til at konstatere, hvem der er den reelle ejer, det finansieringsinstitut, der har ansvaret for åbning af bankkontoen. Endelig vil nogle mellemled eller tredjeparter kunne sørge for dedikerede ydelser, der har til formål at skjule de reelle ejerforhold, og det kan gå ud over et helt erhverv, som vil kunne blive betragtet som medskyldig i at oprette disse systemer til hvidvask af penge.

b) risikobevidsthed

Både udbydere af tjenester til truster eller selskaber og de juridiske erhverv/skatterådgivere synes at være klar over risikoen for illegitime anmodninger om at oprette juridiske enheder og juridiske arrangementer. Risikoen for, at disse strukturer kan bruges til at skjule den reelle ejer er velkendt. Der er dog stadig store mangler ved håndhævelsen. Dette er tilfældet, når flere forpligtede enheder er indblandet i oprettelse af strukturer, og hvor anvendelsen af kundekendskabskrav, herunder hvem der er den reelle ejer, hviler på den finansielle sektor, der ikke altid er godt rustet til situationer, hvor den reelle ejer med vilje skjuler sig.

Der er også betydelige mangler mht. enhedernes forståelse af deres forpligtelser vedrørende bekæmpelse af hvidvask af penge eller endda deres viden om disse

[56] "These U.S. companies hide drug dealers, mobsters and terrorists", Melanie Hicken and Blake Ellis, CNN Money, 9. december 2015.

forpligtelser. Dette gælder navnlig brugen af de juridiske arrangementer i *common law* som truster, der er mindre gennemsigtige juridiske strukturer, som er uvante for *civil law*-landene , og som ikke er kendt i deres nationale lovgivning eller brugt som investerings-/forretningsmodeller. Selv når man kan få vejledning om, hvordan kravane til bekæmpelse af hvidvask af penge skal anvendes på juridiske arrangementer i *civil law* lande — og at kundekendskabskravene skal anvendes — er det stadig vanskeligt at skaffe sig en ordentlig oversigt over disse juridiske strukturer. Dette er især tilfældet for juridiske arrangementer efter *common law*, der indgås i lande uden for EU.

Risikobevidstheden hos udbydere af rådgivning om kapitalstruktur og branchestrategi samt rådgivning og tjenesteydelser vedrørende fusioner og opkøb og rådgivning om forretningsstrategi er umulig at vurdere, da der ikke foreligger oplysninger om, hvorvidt de opfylder kravene om bekæmpelse af hvidvask af penge og af finansiering af terrorisme.

c) retsgrundlag og kontroller

Retsgrundlag: Regnskabssagkyndige og revisorer, skatterådgivere og retlige aktører (fra 2001), udbydere af tjenester til truster eller selskaber (fra 2005) og udbydere af rådgivning om kapitalstruktur og branchestrategi, rådgivning og ydelser vedrørende fusioner og opkøb og rådgivning om forretningsstrategi (fra 2005) er omfattet af EU's regler om bekæmpelse af hvidvask af penge.

EU's nuværende retsgrundlag kræver: i) identifikation af den reelle ejer før indgåelsen af et forretningsforhold, og ii) at medlemsstaterne indfører et centralt register over de reelle ejerforhold vedrørende selskaber og andre juridiske enheder, som er registreret på hver enkelt medlemsstats territorium.

Ikke desto mindre har EU's medlemsstater stadig forskelligartede regler og beskatningssystemer, der bliver udnyttet af kriminelle organisationer. Disse organisationer kan drage fordel af lempeligere regler for bekæmpelse af hvidvask af penge og af finansiering af terrorisme i henseende til at identificere de reelle ejere af juridiske enheder og arrangementer eller af nationale ordninger, ifølge hvilke der ikke skal betales skat af personlig indkomst eller af selskabsindkomst.

Kontroller: Kompetente myndigheder og finansielle efterretningsenheder har noteret sig, at der er involveret offshore-jurisdiktioner, hvor myndighedernes mulighed for at foretage efterforskning afhænger af, om der foreligger aftaler om gensidig retshjælp med disse lande. Konsekvensen er, at hvis der ikke er nogen aftale om gensidig retshjælp, vanskeliggøres processen med at fastslå de reelle ejerforhold.

Der findes IT-værktøjer, som muliggør, at selskabskonstruktioner kan skabes hurtigt og anonymt uden medvirken af en offentlig myndighed. Nogle juridiske arrangementer kan aftale på en meget uformel måde, hvilket skaber yderligere vanskeligheder for inspektionsarbejdet.

Mht. udbydere af rådgivning om kapitalstruktur, branchestrategi samt rådgivning og tjenesteydelser vedrørende fusioner og opkøb og rådgivning om forretningsstrategi foreligger der ingen information om, hvordan kompetente myndigheder kontrollerer dem,

og om de overholder reglerne om bekæmpelse af hvidvask af penge og af finansiering af terrorisme.

Konklusion: Risikoeksponeringen over for hvidvask af penge i relation til oprettelsen af juridiske enheder og juridiske arrangementer anses for at være betydelig på grund af den anonymitet, der fortsat findes, og karakteren af de indblandede kunder og områder, navnlig når basale eller forenklede IT-værktøjer anvendes uden medvirken af en offentlig myndighed. Risikobevidstheden hos professionelle formidlere forekommer ret tilfredsstillende, selvom antallet af indberetninger af mistænkelige transaktioner fortsat er meget lavt[57].

Selv efter medlemsstaternes gennemførelse af EU's direktiver om bekæmpelse af hvidvask af penge samt udpegning af ikkefinansielle virksomheder og erhverv fra 2001 mangler mange medlemsstater stadig en solid lovgivning om bekæmpelse af hvidvask af penge og af finansiering af terrorisme og reglerne synes ikke at være korrekt forstået. Retsreglerne er ikke tilpasset risikoen (de reelle ejerforhold identificeres efter oprettelsen af strukturen frem for før) og den nødvendige kontrol blev først indført for nylig med det 4. og det 5. hvidvaskdirektiv. Sårbarheden over for hvidvask af penge i relation til oprettelsen af juridiske enheder, juridiske arrangementer og nonprofitorganisationer/velgørenhedsorganisationer anses derfor for betydelig/meget betydelig (niveau 3/4).

Risikobegrænsende foranstaltninger:

Der er sket betydelige forbedringer med vedtagelsen og gennemførelsen af Den Finansielle Aktionsgruppes (FATF) standarder og medlemsstaternes opbakning til det arbejde, der i de senere år er gjort af Organisationen for Økonomisk Samarbejde og Udvikling vedrørende gennemsigtighed, men behovet for yderligere at øge gennemsigtigheden af EU's økonomiske og finansielle miljø er åbenbart. Vi kan ikke forhindre hvidvask og terrorfinansiering effektivt, medmindre miljøet er fjendtligt indstillet over for kriminelle, der søger ly for deres penge gennem uigennemsigtige strukturer. Integriteten i EU's finansielle system afhænger af gennemsigtigheden i selskaber og andre juridiske enheder, truster og tilsvarende juridiske arrangementer. De overordnede principper i EU's indsats er at opspore og efterforske hvidvask af penge og at forhindre det i at forekomme. Øget gennemsigtighed kunne virke stærkt præventivt.

[57] I FATF's 2013-rapport konstateres det, at "*indberetningsniveauet fra den juridiske sektor kan ikke forventes at ligge på samme niveau som de finansielle institutioners indberetninger. Der er en betydelig forskel i omfanget af transaktioner foretaget af retlige aktører i forhold til finansielle institutioner. Desuden er det niveau for involvering i hver transaktion, som påvirker det grundlag, hvorpå en mistanke kan opstå og blive vurderet, væsentligt anderledes."* I overensstemmelse hermed peger rapporten side 24 på *"en mere relevant sammenligning"* for den juridiske sektor end måske med andre udpegede ikkefinansielle virksomheder og erhverv *"navnlig dem, der yder professionel bistand",* hvorfra *"indberetninger fra retlige aktører lå på i gennemsnit 10 %, spændende fra under 1 % til 20 %.* Rapporten indeholder eksempler på indberetninger af mistænkelige transaktioner fra retlige aktører og udpegede ikkefinansielle virksomheder og erhverv i 2010 og 2011 for en række lande.

Siden udarbejdelsen af den første beretning om supranational risikovurdering har EU revideret sine regler om bekæmpelse af hvidvask af penge og af finansiering af terrorisme med henblik på at mindske risiciene i relation til hvidvask af penge og terrorfinansiering. I 2015 vedtog EU et moderniseret regelsæt, der omfatter:

- **Direktiv (EU) 2015/849** om forebyggende foranstaltninger mod anvendelse af det finansielle system til hvidvask af penge eller finansiering af terrorisme (fjerde hvidvaskdirektiv).[58]

- **Forordning (EU) 2015/847** om oplysninger, der skal medsendes ved pengeoverførsler[59] – gør overførsler mere transparente og hjælper derved de retshåndhævende myndigheder med at opspore terrorister og kriminelle.

Begge retsakter tager hensyn til FATF's 2012-henstillinger og går med hensyn til en række emner længere med henblik på at fremme de højest mulige standarder for bekæmpelse af hvidvask af penge og bekæmpelse af finansiering af terrorisme.

- **Direktiv (EU) 2018/843, det femte hvidvaskdirektiv**[60] **(ændringer til det fjerde hvidvaskdirektiv).**
- **Direktiv 2018/822/EU**[61], som bestemmer, at mellemmænd skal indgive oplysninger om indberetningspligtige grænseoverskridende skatteordninger til deres nationale myndigheder,[62] får virkning fra 2020.

Det femte hvidvaskdirektiv, der ændrer det fjerde hvidvaskdirektiv blev offentliggjort i Den Europæiske Unions Tidende den 19. juni 2018. Medlemsstaterne skal gennemføre dette direktiv senest den 10. januar 2020, men visse ændringer skal være gennemført senest den 10. marts 2020. Sammenkobling af registrene om reelle ejere kræves gennemført senest den 10. marts 2021.

Konkret med hensyn til oprettelsen af juridiske enheder og juridiske arrangementer, vil de ændringer, der bliver gennemført med dette nye retsgrundlag:

---

[58] Europa-Parlamentets og Rådets direktiv (EU) 2015/849 af 20. maj 2015 om forebyggende foranstaltninger mod anvendelse af det finansielle system til hvidvask af penge eller finansiering af terrorisme, om ændring af Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 og om ophævelse af Europa-Parlamentets og Rådets direktiv 2005/60/EF samt Kommissionens direktiv 2006/70/EF (EØS-relevant tekst), EUT L 141 af 5.6.2015, s. 73.

[59] Europa-Parlamentets og Rådets forordning (EU) 2015/847 af 20. maj 2015 om oplysninger, der skal medsendes ved pengeoverførsler, og om ophævelse af forordning (EF) nr. 1781/2006 (EØS-relevant tekst), EUT L 141, 5.6.2015, s. 1.

[60] Europa-Parlamentets og Rådets direktiv (EU) 2018/843 af 30. maj 2018 om forebyggende foranstaltninger mod anvendelse af det finansielle system til hvidvask af penge eller finansiering af terrorisme og om ændring af direktiv 2009/138/EF og 2013/36/EU (EØS-relevant tekst), EUT L 156 af 19.6.2018, s. 43.

[61] Rådets direktiv (EU) 2018/822 af 25. maj 2018 om ændring af direktiv 2011/16/EU for så vidt angår obligatorisk automatisk udveksling af oplysninger på beskatningsområdet i forbindelse med indberetningspligtige grænseoverskridende ordninger, EUT L 139 af 5.6.2018, s. 1.

[62] Administrativt samarbejde om (direkte) beskatning i EU: https://ec.europa.eu/taxation_customs/business/tax-cooperation-control/administrative-cooperation/enhanced-administrative-cooperation-field-direct-taxation_en.

- forbedre gennemsigtigheden mht. de reelle ejere af selskaber
- forbedre gennemsigtigheden mht. de reelle ejere af truster
- etablere sammenkobling af registre om reelle ejere på EU-plan, og
- forbedre samarbejdet og informationsudvekslingen mellem tilsynsmyndigheder for bekæmpelse af hvidvask af penge og mellem dem og banktilsynsmyndigheder og Den Europæiske Centralbank.

Inden for denne forbedrede lovgivningsramme er de vigtigste opgaver for de kompetente myndigheder/de selvregulerende organer fortsat:

- Medlemsstaterne bør sikre, at de kompetente myndigheder/selvregulerende organer sørger for undervisning og vejledning om risikofaktorer med fokus på de relationer, der ikke sker ansigt-til ansigt, offshore professionelle formidlere, kunder eller lande og komplekse strukturer/skuffe-konstruktioner.

- Medlemsstaterne bør sikre, at selvregulerende organer/kompetente myndigheder foretager tematiske inspektioner af, hvordan kravene til identifikation af den reelle ejer håndhæves.

- Kompetente myndigheder/selvregulerende organer bør til medlemsstaterne afgive årlige rapporter om de foranstaltninger, der er truffet for at kontrollere, at disse enheder opfylder deres forpligtelser mht. kundekendskabskrav, herunder kravene vedrørende de reelle ejerforhold, rapporter om mistænkelige transaktioner og interne kontroller.

- Medlemsstaterne bør sikre, at udbydere af rådgivning om kapitalstruktur og branchestrategi, rådgivning og tjenesteydelser vedrørende fusioner og opkøb og rådgivning om forretningsstrategi overholder deres forpligtelser mht. reelle ejerforhold.

2. Juridiske enheders og juridiske arrangementers forretningsaktiviteter

Produkt/tjenesteydelse
Juridiske enheders og juridiske arrangementers forretningsaktiviteter

Sektor
Udbydere af tjenester til truster eller selskaber, retlige aktører, skatterådgivere/regnskabssagkyndige/revisorer, udbydere af rådgivning om kapitalstruktur og branchestrategi og tilsvarende spørgsmål samt rådgivning og ydelser vedrørende fusioner og opkøb ("professionelle formidlere")

Generel beskrivelse af den pågældende sektor og det/den relevante produkt/aktivitet

Udbydere af tjenester til truster eller selskaber, retlige aktører, skatterådgivere/regnskabssagkyndige/revisorer og udbydere af rådgivning om kapitalstruktur og branchestrategi, rådgivning og ydelser vedrørende fusioner og opkøb og rådgivning om forretningsstrategi leverer en lang række tjenesteydelser til privatpersoner og virksomheder om forretningsvirksomhed og formueforvaltning.

Det fjerde direktiv om bekæmpelse af hvidvask af penge kræver, at enheder identificerer den reelle ejer, når de indgår en forretningsforbindelse og tager risikobaserede og passende forholdsregler til at kontrollere identiteten af de reelle ejere som defineret i artikel 3, stk. 6.

I tillæg til lovgivning om hvidvask af penge er der i følgende selskabsretlige EU-direktiver fastsat generelle regler om etablering af selskaber med begrænset ansvar, navnlig med hensyn til kapital og oplysningskrav. EU selskabsret er delvis kodificeret i direktiv 2017/1132/EF om visse aspekter af selskabsretten, og medlemsstaterne har fortsat separate selskabslovgivninger, som ændres fra tid til anden for at være i overensstemmelse med EU's direktiver og forordninger.

Direktiv 2017/1132/EU dækker:

1. Offentlighed omkring selskabsdokumenter, gyldigheden af et selskabs forpligtelser samt ugyldighed. Det gælder for alle aktieselskaber og andre selskaber med begrænset ansvar.
2. **Stiftelse** af aktieselskaber og regler om **bevarelse af og ændring af deres kapital**. Det sætter et minimumskapitalkrav for EU-aktieselskaber på 25 000 EUR.
3. Oplysningskrav til **udenlandske filialer** af selskaber. Det dækker EU-selskaber, som etablerer sig i et andet EU-land eller virksomheder fra tredjelande, der opretter filialer i EU.

I tillæg hertil opstiller **direktiv 2009/102/EF** (det 12. selskabsdirektiv) regler for etablering af et **enkeltmandsselskab** (hvor alle andele ejes af en enkelt anpartshaver). Det omfatter anpartsselskaber, men EU-landene kan beslutte at udvide de til at omfatte aktieselskaber. Det erstatter direktiv 89/667/EØF.

Reglerne om stiftelse, kapital og oplysningskrav suppleres af **regler om bogføring og regnskabsrapportering.**[63]

Børsnoterede selskaber skal også opfylde visse **krav om gennemsigtighed.**[64]

Beskrivelse af risikoscenariet

Stråmandsvirksomheder anvendt til svig via falsk fakturering: Lovovertrædere anvender stråmandsvirksomheder til at knytte fakturaer til importerede varer, og overbetalingen kanaliseres til terrorformål.

Handelsbaseret hvidvask af penge: Lovovertrædere bruger handelsbaseret hvidvask som legitimation af flytning af udbyttet af kriminalitet gennem bankkanaler (via veksler, fakturaer mv.) eller ved brug af globale transaktioner, ofte ved hjælp af falske dokumenter vedrørende handel med varer og tjenesteydelser[65]. Det kan potentielt åbne mulighed for hurtig overførsel af store beløb ved at angive et påstået økonomisk formål. Systemer med handelsbaseret hvidvask har også været brugt af internationale terrorgrupper sammen med komplekse finansieringsmetoder[66].

Falske lån: Virksomhederne opretter fiktive lån med hinanden for at skabe en informationssti, der skal legitimere overførsler af midler af illegal oprindelse. Lovovertrædere bruger fiktive lån til at legitimere flytning af midler gennem bankkanaler — uden nogen bagvedliggende økonomisk realitet.

Lovgivningsmæssigt har EU vedtaget flere regnskabsdirektiver[67] og har fastsat revisionskrav for at sikre, at virksomhedernes regnskaber er retvisende og troværdige.

Generel bemærkning

For dette risikoscenarie omfatter vurderingen juridiske enheder som selskaber, selskabskonstruktioner, fonde, foreninger, nonprofitorganisationer, velgørenhedsorganisationer og lignende strukturer. Det dækker også truster og andre juridiske arrangementer med en lignende struktur eller funktion (f.eks. *fiducie*, *Treuhand*, *fideicomiso* …).

Risikovurderingen angår aktivitetens art og ikke strukturen som sådan. Denne tilgang anfægter ikke de juridiske enheders særlige karakter i forhold til juridiske arrangementer (sidstnævnte har ikke status som juridiske personer og er grundlæggende et kontraktforhold). Hvad angår arten af den pågældende ydelse (her oprettelsen af

[63] Selskabsrapportering: https://ec.europa.eu/info/business-economy-euro/company-reporting-and-auditing/company-reporting_en.
[64] Værdipapirmarkeder: https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-markets/securities-markets_en.
[65] Handelsbaseret hvidvask — af FATF: http://www.fatf-gafi.org/publications/methodsandtrends/documents/trade-basedmoneylaundering.html.
[66] " DEA and European Authorities Uncover Massive Hezbollah Drug and Money Laundering Scheme", DEA — 1. februar 2016: et tilfælde, hvor den libanesiske gruppe Hizbollah hvidvaskede betydelige indtægter fra narkotikahandel i Europa som led i et handelsbaseret hvidvasksystem kaldet Black Market Peso Exchange (konvertering af peso på det sorte marked).
[67] Oversigt over selskabsrapportering: https://ec.europa.eu/info/business-economy-euro/company-reporting-and-auditing/company-reporting_en#overview.

strukturen) gør disse særlige karakteristika ikke nogen afgørende forskel, idet juridiske enheder og juridiske arrangementer kan bruges på samme måde for til at skjule de sande reelle ejere. Hvilken type struktur, lovovertrædere foretrækker, afhænger af de juridiske regler i en given jurisdiktion, arten af lovovertrædernes ekspertise samt praktiske forhold. Organiserede kriminelle grupper kan let oprette alle disse strukturer, og de vil alle kunne være redskaber til at skabe uigennemskuelige og komplicerede ordninger, der gør det vanskeligere at identificere den reelle ejer og midlernes virkelige oprindelse.

Trussel

Finansiering af terrorisme

Vurderingen af truslen om terrorfinansiering i relation til juridiske enheders og juridiske arrangementers forretningsaktiviteter viser, at terroristgrupperinger ikke nærer nogen særlig forkærlighed for denne type af metoder til finansiering af terroristvirksomhed. Ifølge retshåndhævende myndigheder er dette risikoscenarie ikke rigtig attraktivt for terrorister, idet det kræver, at der oprettes en uigennemsigtig struktur (ulovlig juridisk enhed eller juridisk arrangement) eller at man infiltrerer ejerkredsen i en lovlig juridisk enhed eller et juridisk arrangement. Det kræver ekspertise og evnen til at planlægge. Grundet de forskellige skridt, der skal tages, er det usandsynligt, at der hurtigt kan samles "rene" penge med denne metode. Men hvis lovovertræderne har ekspertisen, kan de anvende denne metode til pengeoverførsel i stedet for andre klassiske teknikker (penge- eller værdioverførselstjenester, hawala osv.). Metoden kan være attraktiv, hvis der er behov for at overføre store beløb til finansiering af terrorisme. Derfor kan terrorgrupper have til hensigt at bruge den.

Konklusion: Ud fra de oplysninger, som de retshåndhævende myndigheder og finansielle efterretningsenheder har tilvejebragt, anses trusselsniveauet for terrorfinansiering i relation til juridiske enheders og juridiske arrangementers forretningsaktiviteter for i moderat grad betydeligt (niveau 2).

Hvidvask af penge

Vurderingen af truslen om hvidvask i relation til juridiske enheders og juridiske arrangementers forretningsaktiviteter viser, at den mest udbredte metode, der bruges af organiserede kriminelle grupper til hvidvask af udbyttet af kriminalitet, er handelsbaseret hvidvask og falsk fakturering. Disse ulovlige aktiviteter kan gøre det muligt at bringe lovlige midler ud af virksomhedens cash flow: i) ved at bruge falske fakturaer, ii) ved at reducere grundlaget for skatteberegning, iii) ved at reducere indkomstskatten ved at tage lovlige midler fra selskabet og iv) ved at hvidvaske ulovligt udbytte ved at hæve kontanter fra en anden virksomheds konto via mellemled. Flere og flere handelstransaktioner er faktisk lovlige og omfatter eksport af varer og råvarer til markedsprisen, men oftest betalt kontant og eksporteret, før de bliver reeksporteret mellem forskellige lande. Det omfatter primært meget værdifulde varer (biler, elektronik, luksusvarer), men i stigende omfang også mindre værdifulde varer/varer med stort volumen som foderstoffer.

I næsten alle tilfælde bruger organiserede kriminelle grupperinger lovlige forretningsstrukturer til at hvidvaske deres kriminelle udbytte. Dette er almindelig kendt som *business recycling*. Kontantintensive virksomheder som catering og detailforretninger giver et godt dække for kilden til ellers uforklarlige kontantbeløb. Disse virksomheder kan udnyttes på flere forskellige måder af organiserede kriminelle grupperinger, men i de fleste

tilfælde bruges de som legitim indtægtskilde fra kunder til at sammenblande ulovlige midler med lovlige indtægter. I disse tilfælde bruges en medsammensvoren bogholders eller revisors tjenesteydelser til at legitimere kriminelle pengestrømme gennem falske fakturaer, kvitteringer og konti. I andre tilfælde har virksomheden ingen lovlig aktivitet og derfor ingen lovlig kilde til kontanter. Der bliver derfor oprettet fiktive konti og transaktioner med henblik på at forklæde kriminelle udbytter som lovlig indtjening på handel med varer og tjenesteydelser. Regnskaber kan også forfalskes med henblik på at gøre rede for likviditetsstrømmene.

Den nødvendige ekspertise og evne til planlægning er ganske vist ikke ubetydelig, men retshåndhævende myndigheder og finansielle efterretningsenheder mener, at organiserede kriminelle grupperinger jævnligt har anvendt denne metode, fordi den generelt er ganske tilgængelig, har lave omkostninger og er relativt let at udnytte. Imidlertid involverer denne metode også flere sektorer. F.eks. behandles overførsler af penge gennem virksomhedernes strukturer normalt gennem banksektoren.

Konklusion: Opbygningen af et handelsbaseret hvidvasksystem kan ganske vist kræve moderate niveauer af teknisk ekspertise og viden, men finansielle efterretningsenheder og retshåndhævende myndigheder har fundet mange sådanne sager, som viser, at metoden er rimelig let at få adgang til og at udnytte. På denne baggrund anses trusselsniveauet for hvidvask i relation til juridiske enheders og juridiske arrangementers forretningsaktiviteter og baseret på handelsbaseret hvidvask af penge som meget betydeligt (niveau 4).

Sårbarhed

Finansiering af terrorisme

Vurderingen af sårbarheden over for finansiering af terrorisme i relation til juridiske enheders og juridiske arrangementers forretningsaktiviteter viser:

a) risikoeksponering

Der kan samles betydelige beløb gennem forretningsaktiviteter til finansiering af terrororganisationer og -aktiviteter. Denne forretningsaktivitet er for det meste kontantbaseret og kan omfatte grænseoverskridende transaktioner med højrisikotredjelande.

b) risikobevidsthed

Både udbydere af tjenester til truster eller selskaber og de juridiske erhverv/skatterådgivere synes at være klar over risikoen for at blive misbrugt til at oprette juridiske enheder og juridiske arrangementer til illegale formål med forbindelse til hvidvask af penge og terrorfinansiering. Risikoen for, at disse strukturer kan bruges til at skjule den reelle ejer er velkendt. Der er imidlertid stadig betydelige mangler mht. deres forståelse af deres forpligtelser vedrørende bekæmpelse af hvidvask af penge og af finansiering af terrorisme eller endda mht. deres viden om dem. Men navnlig da forretningsaktiviteter i henseende til terrorfinansiering også kan være baseret på lovlige penge, udløser dette ikke altid faresignaler. De eksisterende kontroller er forholdsvis svage, så finansielle efterretningsenheder kan kun opspore og analysere risici for terrorfinansiering i relation til

forretningsaktiviteter i juridiske enheder og juridiske arrangementer under begrænsede omstændigheder. Der kan være professionelle fra mange sektorer involveret i oprettelsen af juridiske strukturer, og de kompetente myndigheder er ikke altid i stand til at sørge for ordentlig vejledning til disse brancher.

c) retsgrundlag og kontroller

Retsgrundlag: Regnskabssagkyndige og revisorer, skatterådgivere og retlige aktører (fra 2001), udbydere af tjenester til truster eller selskaber (fra 2005) og udbydere af rådgivning om kapitalstruktur og branchestrategi, rådgivning og ydelser vedrørende fusioner og opkøb og rådgivning om forretningsstrategi (fra 2005) er omfattet af EU's regler om bekæmpelse af hvidvask af penge. Disse EU-krav foreskriver, at den reelle ejer af en juridisk struktur eller et juridisk arrangement, herunder nonprofitorganisationer eller fonde, bliver identificeret, før en forretningsforbindelse indledes.

Kontrol:
De kompetente myndigheder mener, at de eksisterende kontroller stadig er utilstrækkelige, og at de oplysninger, der modtages i begyndelsen af forretningsforbindelser, ikke er tilstrækkelige til, at man kan opdage og analysere de risici for terrorfinansiering, der forbundet med oprettelsen af juridiske enheder og juridiske arrangementer.

Mht. udbydere af rådgivning om kapitalstruktur og branchestrategi samt rådgivning og tjenesteydelser vedrørende fusioner og opkøb og rådgivning om forretningsstrategi foreligger der ingen information om, hvordan de overvåges af de kompetente myndigheder, og om de overholder reglerne om AML/ CFT.

Konklusion: På baggrund af de indsamlede oplysninger, og selvom denne metode ikke nødvendigvis er det mest oplagte middel til terrorfinansiering, anses sårbarheden over for terrorfinansiering i relation til juridiske enheders og juridiske arrangementers forretningsaktiviteter for betydelig (niveau 3).

Hvidvask af penge

Vurderingen af sårbarheden over for hvidvask af penge i relation til juridiske enheders og juridiske arrangementers forretningsaktiviteter viser

a) risikoeksponering

Falske lån bruges i vidt omfang af organiserede kriminelle grupper. I visse tilfælde kan handelsbaseret hvidvask af penge indebære store internationale handelstransaktioner, der ikke er så lette for banker at at opdage. Vanskelighederne ved påvisning kan blive forøget ved den gennemgående brug af stråmænd, hvilket kan have betydning for sårbarhedsniveauet.

b) risikobevidsthed

Både udbydere af tjenester til truster eller selskaber og de juridiske erhverv/skatterådgivere synes at være klar over risikoen for at blive misbrugt til at oprette juridiske enheder og juridiske arrangementer til illegale formål med forbindelse til hvidvask af penge og

terrorfinansiering. Risikoen for, at disse strukturer kan bruges til at skjule den reelle ejer er velkendt. Udbydere af tjenester til truster eller selskaber er, generelt, klar over, at de ikke bør handle med tredjeparter, uden at overholde reglerne på korrekt måde. De transaktioner, der er tale om, er imidlertid temmelig komplekse (navnlig grænseoverskridende), hvilket gør de retshåndhævende myndigheders efterforskningsarbejde vanskeligere. Midlernes ulovlige oprindelse er det generelt svært at bevise på grund af antallet af involverede personer/grupper og geografiske områder samt de kanaler, der anvendes. Mistænkelige transaktioner er derfor ganske vanskelige at spore (handelsbaseret hvidvask og falsk fakturering).

c) retsgrundlag og kontroller

Retsgrundlag: Regnskabssagkyndige og revisorer, skatterådgivere og retlige aktører (fra 2001), udbydere af tjenester til truster eller selskaber (fra 2005) og udbydere af rådgivning om kapitalstruktur og branchestrategi, rådgivning og ydelser vedrørende fusioner og opkøb og rådgivning om forretningsstrategi (fra 2005) er omfattet af EU's regler om bekæmpelse af hvidvask af penge. Disse EU-krav foreskriver, at den reelle ejer af en juridisk struktur eller et juridisk arrangement, herunder almennyttige organisationer eller fonde, bliver identificeret, før en forretningsforbindelse indledes.

Kontroller: i adskillige tilfælde har kompetente myndigheder og finansielle efterretningsenheder noteret sig inddragelsen af offshore lande, hvor myndighedernes mulighed for at foretage efterforskning afhænger af eksistensen af aftaler om gensidig retshjælp med disse lande. Konsekvensen er, at så længe der ikke er nogen aftale om gensidig retshjælp, afsluttes processen med at fastslå de reelle ejerforhold.

Mht. udbydere af rådgivning om kapitalstruktur, branchestrategi samt rådgivning og tjenesteydelser vedrørende fusioner og opkøb og rådgivning om forretningsstrategi foreligger der ingen information om, hvordan kompetente myndigheder kontrollerer dem, og om de overholder reglerne om bekæmpelse af hvidvask af penge og af finansiering af terrorisme.

Konklusion: Sektorens risikoeksponering anses for at være meget betydelig på grund af manglen på en solid lovgivning om hvidvask i mange ikke-EU-lande og især mangelen på regler om identificering af de reelle ejere. Det betyder, at kontrollen er ikke-eksisterende i forhold til uigennemsigtige strukturer, der omfatter mange lande. Hertil kommer, at der ikke er nogen oplysninger om, hvorvidt sektoren opfylder kravene til bekæmpelse af hvidvask af penge og af finansiering af terrorisme. På denne baggrund anses sårbarhedsniveauet over for hvidvask af penge i relation til juridiske enheders og juridiske arrangementers forretningsaktiviteter og baseret på forretningsbaseret hvidvask af penge som betydeligt/meget betydeligt (niveau 3/4).

Risikobegrænsende foranstaltninger:

Efter den forbedrede lovgivning indført ved fjerde hvidvaskdirektiv og ændringerne i det femte hvidvaskdirektiv er gennemsigtighedskravene til oplysninger om de reelle ejerforhold i juridiske enheder og juridiske arrangementer blevet styrket:

- Den konkrete faktor ved afgørelsen af, hvilken medlemsstat der er ansvarlig for overvågning og registrering af oplysninger om de reelle ejerforhold i truster og lignende juridiske ordninger er klarlagt.

- Offentlig adgang til oplysningerne om reelle ejerforhold giver mulighed for, at civilsamfundet, herunder pressen og civilsamfundsorganisationerne, øger tilsynet med informationerne og derved bidrager til at bevare tilliden til virksomhedstransaktionernes og det finansielle systems integritet.

- Det styrkede offentlige tilsyn bidrager til at forebygge misbrug af juridiske enheder og juridiske arrangementer, herunder til skatteundgåelse.

- Medlemsstaternes centrale registre med information om de reelle ejerforhold bliver sammenkoblet via den europæiske centrale platform, som blev etableret ved direktiv (EU) 2017/1132.

- Direktiv 2018/822/EU får virkning fra 2020, fra hvilket tidspunkt formidlere får pligt til til deres nationale myndigheder at indberette automatisk udveksling af indberetningspligtige oplysninger om indberetningspligtige grænseoverskridende skattearrangementer.[68]

Inden for denne forbedrede lovgivningsramme er de vigtigste opgaver for de kompetente myndigheder/de selvregulerende organer fortsat:

- Kompetente myndigheder/de selvregulerende organer bør sørge for undervisning og vejledning om risikofaktorer med særligt fokus på relationer, der ikke er ansigt til ansigt, professionelle offshore formidlere, kunder eller lande og komplekse strukturer/skuffe-konstruktioner.

- Selvregulerende organer/kompetente myndigheder bør foretager tematiske inspektioner af, hvordan kravene til identifikation af den reelle ejer gennemføres.

- Kompetente myndigheder/selvregulerende organer bør til medlemsstaterne afgive årlige rapporter om de foranstaltninger, der er truffet for at kontrollere, at disse enheder opfylder deres forpligtelser mht. kundekendskabskrav, herunder kravene vedrørende de reelle ejerforhold, rapporter om mistænkelige transaktioner og interne kontroller.

[68] Administrativt samarbejde om (direkte) beskatning i EU: https://ec.europa.eu/taxation_customs/business/tax-cooperation-control/administrative-cooperation/enhanced-administrative-cooperation-field-direct-taxation_en.

3. Ophør af juridiske enheder og juridiske arrangementer

Produkt
Ophøret af juridiske enheders og juridiske arrangementers forretningsmæssige aktiviteter

Sektor
Udbydere af tjenester til truster eller selskaber, retlige aktører, skatterådgivere/regnskabssagkyndige/revisorer, udbydere af rådgivning om kapitalstruktur og branchestrategi, rådgivning og ydelser vedrørende fusioner og opkøb og rådgivning om forretningsstrategi ("professionelle formidlere")

Generel beskrivelse af den pågældende sektor og det/den relevante produkt/aktivitet

Udbydere af tjenester til truster eller selskaber, retlige aktører, skatterådgivere/regnskabssagkyndige/revisorer og udbydere af rådgivning om kapitalstruktur og branchestrategi, rådgivning og ydelser vedrørende fusioner og opkøb og rådgivning om forretningsstrategi leverer en lang række tjenesteydelser til privatpersoner og virksomheder om forretningsvirksomhed og formueforvaltning.

Det fjerde direktiv om bekæmpelse af hvidvask af penge kræver, at visse enheder identificerer den reelle ejer, når de indgår en forretningsforbindelse tager risikobaserede og passende forholdsregler til at kontrollere identiteten af de reelle ejere som defineret i artikel 3, stk. 6.

I tillæg til lovgivning om hvidvask af penge er der i følgende selskabsretlige EU-direktiver fastsat generelle regler om etablering af selskaber med begrænset ansvar, navnlig med hensyn til kapital og oplysningskrav. Europæisk selskabsret er delvis kodificeret i direktiv 2017/1132/EF[69] om visse aspekter af selskabsretten, og medlemsstaterne har fortsat separate selskabslovgivninger, som ændres fra tid til anden for at være i overensstemmelse med EU's direktiver og forordninger.

Direktiv 2017/1132/EU dækker:

1. Offentlighed omkring selskabsdokumenter, gyldigheden af et selskabs forpligtelser samt ugyldighed. Det gælder for alle aktieselskaber og andre selskaber med begrænset ansvar.
2. **Stiftelse** af aktieselskaber og regler om **bevarelse af og ændring af deres kapital**. Det sætter et minimumskapitalkrav for EU-aktieselskaber på 25 000 EUR.
3. Oplysningskrav til **udenlandske filialer** af selskaber. Det dækker EU-selskaber, som etablerer sig i et andet EU-land eller virksomheder fra tredjelande, der opretter filialer i EU.

[69] Europa-Parlamentets og Rådets direktiv (EU) 2017/1132 af 14. juni 2017 om visse aspekter af selskabsretten, EUT L 169 af 30.6.2017, s. 46.

I tillæg hertil opstiller **direktiv 2009/102/EF**[70] (det 12. delskabsdirektiv) regler for etablering af et **enkeltmandsselskab** (hvor alle andele ejes af en enkelt andelshaver). Det omfatter anpartsselskaber, men EU-landene kan beslutte at udvide de til at omfatte aktieselskaber. Det erstatter direktiv 89/667/EØF.

Reglerne om stiftelse, kapital og oplysningskrav suppleres af **regler om bogføring og regnskabsrapportering.**[71]

Børsnoterede selskaber skal også opfylde visse **krav om gennemsigtighed.**[72]

Beskrivelse af risikoscenariet

Bedrageri gennem en virksomhed konkurs/retslige likvidation: efter konkursen i en virksomhed bliver samme virksomhed købt af en tidligere aktionær, der skaber en ny struktur med henblik på at fortsætte samme forretningsaktivitet, men nu uden økonomiske problemer. Lovovertræderne fjerner pengene fra dækvirksomheden, før de illegale aktiviteter bliver opdaget, eller før aktiverne bliver beslaglagt af de kompetente myndigheder, og herved slører man revisionssporet vedrørende de penge, der er hvidvasket gennem det likviderede selskab.

Generel bemærkning

For dette risikoscenarie omfatter vurderingen juridiske enheder som selskaber, selskabskonstruktioner, fonde, foreninger, nonprofitorganisationer, velgørenhedsorganisationer og lignende strukturer. Det dækker også truster og andre juridiske arrangementer med en lignende struktur eller funktion (f.eks. *fiducie*, *Treuhand*, *fideicomiso* …).

Risikovurderingen angår aktivitetens art og ikke strukturen som sådan. Denne tilgang anfægter ikke de juridiske enheders særlige karakter i forhold til juridiske arrangementer (sidstnævnte har ikke status som juridiske personer og er grundlæggende et kontraktforhold). Hvad angår arten af den pågældende ydelse (her oprettelsen af strukturen) gør disse særlige forhold ikke nogen afgørende forskel, idet juridiske enheder og juridiske arrangementer kan bruges på samme måde for til at skjule de sande reelle ejere. Hvilken type struktur, lovovertrædere foretrækker, afhænger af de juridiske regler i en given jurisdiktion, arten af lovovertrædernes ekspertise samt praktiske forhold. Organiserede kriminelle grupper kan let oprette alle disse strukturer, og de vil alle kunne være redskaber til at skabe uigennemskuelige og komplicerede ordninger, der gør det vanskeligere at identificere den reelle ejer og midlernes virkelige oprindelse.

[70] Europa-Parlamentets og Rådets Direktiv 2009/102/EF af 16. september 2009 på selskabsrettens område om enkeltmandsselskaber med begrænset ansvar (EØS-relevant tekst), EUT L 258 af 1.10.2009, s. 20.
[71] Selskabsrapportering: https://ec.europa.eu/info/business-economy-euro/company-reporting-and-auditing/company-reporting_en.
[72] Værdipapirmarkeder: https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-markets/securities-markets_en.

Trussel

Finansiering af terrorisme

Vurderingen af truslen om terrorfinansiering hidrørende fra ophør af erhvervsaktivitet er blevet overvejet sammen med systemer til hvidvask af penge i relation til ophør af erhvervsaktivitet med det formål at skjule midlernes illegale oprindelse. I sådanne situationer bliver truslen om terrorfinansiering ikke mindre ved en særskilt vurdering.

Konklusion: Vurderingen af truslen om finansiering af terrorisme hidrørende fra ophør af erhvervsaktivitet anses for i let grad/moderat grad betydelig (niveau 1/2).

Hvidvask af penge

Vurderingen af truslen om hvidvask af penge hidrørende fra ophøret af juridiske strukturers erhvervsaktivitet viser, at konkurs er en del af en mere generel proces, og nogle judicielle tilsyn har rapporteret tilfælde, hvor falske konkurser er blevet brugt til at hvidvaske udbyttet fra kriminalitet. De retshåndhævende myndigheder har imidlertid kun fundet få tilfælde. Dette peger i retning af, at kriminelle organisationer opfatter metoden som uattraktiv eller svært tilgængelig, da den kræver en del logistiske og planlægningsmæssige færdigheder.

Konklusion: På baggrund af de oplysninger, der er indsamlet under vurderingsfasen, anses trusselsniveauet for hvidvask af penge hidrørende fra ophøret af erhvervsaktivitet for i let grad/moderat grad betydeligt (niveau 1/2).

Sårbarhed

Finansiering af terrorisme

Vurderingen af sårbarhed over for terrorfinansiering hidrørende fra ophør af erhvervsaktivitet er blevet overvejet sammen med systemer til hvidvask af penge i relation til ophør af erhvervsaktivitet med det formål at skjule midlernes illegale oprindelse. I sådanne situationer bliver truslen om terrorfinansiering ikke mindre ved en særskilt vurdering.

Konklusion: I sådanne tilfælde er sårbarhedsniveauet over for hvidvask af penge i moderat grad betydeligt (niveau 2).

Hvidvask af penge

Vurderingen af sårbarheden over for hvidvask af penge hidrørende fra ophøret af juridiske strukturers erhvervsaktivitet viser, at:

a) risikoeksponering

Situationer, hvor der er tale om ophøret af en erhvervsaktivitet, er generelt startet fra et tilfælde af bedrageri.

b) risikobevidsthed

Retshåndhævende myndigheders og finansielle efterretningsenheders afsløring af denne metode er let, da det meste starter med et tilfælde af bedrageri. Denne underliggende lovovertrædelses udløser faresignaler enten for sektoren eller for de kompetente myndigheder. Generelt er konkurs kompleks at gennemføre og forpligtede enheder (navnlig banker) er særligt opmærksomme på de pågældende scenarier, hvoraf de fleste anses for at være mistænkelige.

c) retsgrundlag og kontroller

Regnskabssagkyndige og revisorer, skatterådgivere og retlige aktører (fra 2001), udbydere af tjenester til truster eller selskaber (fra 2005) og udbydere af rådgivning om kapitalstruktur og branchestrategi, rådgivning og ydelser vedrørende fusioner og opkøb og rådgivning om forretningsstrategi (fra 2005) er omfattet af EU's regler om bekæmpelse af hvidvask af penge.

Der findes ingen særlige bestemmelser i EU's regler om bekæmpelse af hvidvask af penge, der dækker denne situation, bortset fra, at forpligtede enheder har pligt til at identificere og rapportere mistænkelige forpligtelser. Men antallet af modtagne indberetninger om mistænkelige transaktioner viser, at kontrollen er effektiv og giver mulighed for afsløring af mistanken situationer. De kuratorer, der styrer en insolvensbehandling, er også et ekstra kontrolelement.

Mht. udbydere af rådgivning om kapitalstruktur, branchestrategi samt rådgivning og tjenesteydelser vedrørende fusioner og opkøb og rådgivning om forretningsstrategi foreligger der ingen information om, hvordan kompetente myndigheder kontrollerer dem, og om de overholder reglerne om bekæmpelse af hvidvask af penge og af finansiering af terrorisme.

Konklusion: Konkurs er et problem for nogle medlemsstater, men afsløringen af sådanne tilfælde og branchens og andre forpligtede enheders opmærksomhedsniveau fører til den vurdering, at sårbarhedsniveauet er i moderat grad betydeligt (niveau 2).

Risikobegrænsende foranstaltninger:

EU's nugældende retsgrundlag har skærpet kravene til gennemsigtigheden af oplysningerne om de reelle ejerforhold for juridiske enheder og juridiske arrangementer. Det har også præciseret og tydeliggjort visse parters rolle som forpligtede enheder.

Inden for denne forbedrede lovgivningsramme er de vigtigste opgaver for de kompetente myndigheder/de selvregulerende organer fortsat:

A/ hvis ophøret har forbindelse til oprettelsen af en anden juridisk enhed eller juridisk arrangement

Kompetente myndigheder/selvregulerende organer:

- Medlemsstaterne bør sikre, at de kompetente myndigheder/de selvregulerende organer sørger for undervisning og vejledning om risikofaktorer med fokus på de relationer, der ikke sker ansigt-til ansigt, professionelle offshore formidlere eller kunder eller lande og komplekse strukturer/skuffe-konstruktioner.

- Medlemsstaterne bør sikre, at selvregulerende organer/kompetente myndigheder foretager tematiske inspektioner af, hvordan kravene til identifikation af den reelle ejer gennemføres.

- Kompetente myndigheder/selvregulerende organer bør til medlemsstaterne afgive årlige rapporter om de foranstaltninger, der er truffet for at kontrollere, at disse enheder opfylder deres forpligtelser mht. kundekendskabskrav, herunder kravene vedrørende de reelle ejerforhold, rapporter om mistænkelige transaktioner og interne kontroller.

- Medlemsstaterne bør indføre nogle mekanismer for at sikre, at oprettelsen af strukturer foregår under opsyn af en professionel (forpligtet enhed), der skal udvikle deres due diligence.

- Medlemsstaterne bør indføre mekanismer til sikring af, at oplysninger i det centrale register om de reelle ejerforhold kontrolleres regelmæssigt.

- Medlemsstaterne bør sikre, at udbydere af rådgivning om kapitalstruktur og branchestrategi, rådgivning og tjenesteydelser vedrørende fusioner og opkøb og rådgivning om forretningsstrategi overholder deres forpligtelser mht. reelle ejerforhold.

B/ hvis ophøret har forbindelse til købet af en anden juridisk enhed eller juridisk arrangement

Kompetente myndigheder/selvregulerende organer:

- Kompetente myndigheder/de selvregulerende organer bør sørge for undervisning og vejledning om risikofaktorer med særligt fokus på relationer, der ikke er ansigt til ansigt, professionelle offshore formidlere, kunder eller lande og komplekse strukturer/skuffe-konstruktioner.

- Selvregulerende organer/kompetente myndigheder bør foretager tematiske inspektioner af, hvordan kravene til identifikation af den reelle ejer gennemføres.

- Kompetente myndigheder/selvregulerende til medlemsstaterne afgive årlige rapporter om de foranstaltninger, der er truffet for at kontrollere, at disse enheder opfylder deres forpligtelser mht. kundekendskabskrav, herunder kravene vedrørende de reelle ejerforhold, rapporter om mistænkelige transaktioner og interne kontroller.

- Medlemsstaterne bør indføre mekanismer til sikring af, at oplysninger i det centrale register om de reelle ejerforhold kontrolleres regelmæssigt.

Medlemsstaterne bør sikre, at udbydere af rådgivning om kapitalstruktur og branchestrategi, rådgivning og tjenesteydelser vedrørende fusioner og opkøb og rådgivning om forretningsstrategi overholder deres forpligtelser mht. reelle ejerforhold.

4. Meget værdifulde varer – kulturgenstande og antikviteter

Produkt
Meget værdifulde varer – kulturgenstande og antikviteter

Sektor
Forhandlere af meget værdifulde aktiver

Beskrivelse af risikoscenariet

Finansiering af terrorisme – Lovovertrædere opnår indtægter fra salg af røvede kulturgenstande og antikviteter. Den ulovlige handel med kulturgenstande er blandt de største kriminelle handelskategorier, anslås til muligvis at udgøre den tredje- eller fjerdestørste kategori. Men der findes næppe nogen instrumenter til måling af den lovlige handel eller data om omfanget af de illegale forretninger (det særlige ved denne ulovlige handel er, at den lovlige og den ulovlige handel undertiden er forbundet med hinanden).

Der findes næppe nogen data eller instrumenter til måling af ulovlig handel. Men ifølge Interpol er det sorte marked i kunstværker ved at blive lige så indbringende som markederne for narkotika, våben og forfalskede produkter.

I den informationsmappe, UNESCO udarbejdede i anledning af 40-års jubilæet for 1970-konventionen, anføres det, at sammen med handelen med narkotika og våben udgør det sorte marked for antikviteter og kulturgenstande en af de mest solidt forankrede ulovlige handelstyper i verden[73].

Værdien af den ulovlige handel med antikviteter trafik er det også vanskeligt at vurdere[74] pga. dens usynlige og skjulte karakter.[75] Det skønnes, at kun 30-40 % af salg af antikviteter finder sted gennem auktionshuse, hvor genstandene bliver vist i kataloger.[76] Resten sker gennem private (således ofte ikke overvågede og ikke registrerede) transaktioner.[77]

---

[73] UNESCO. The Fight against the Illicit Trafficking of Cultural Objects: the 1970 Convention: Past and Future. 15. og 16. marts 2011. http://unesdoc.unesco.org/images/0019/001916/191606E.pdf.
[74] Alesia Koush 'Fight against the Illegal Antiquities' Traffic in the EU: Bridging the Legislative Gaps' Bruges, College of Europe 2011; Hardy 'Illicit trafficking, provenance research and due diligence: the state of the art'. Forskningsrapport, 30. marts 2016.
[75] Duncan Chappell & Kenneth Polk, Unravelling the Cordata‖: Just How Organised Is the International Traffic in Cultural Objects?', i Stefano Manacorda & Duncan Chappell (eds.), *Crime in the Art and Antiquities' World. Illegal Trafficking in Cultural Property.*
[76] Peter Watson, Sotheby's: The Inside Story, Random House, 1997, citeret i Chauncey D. Steele.
[77] Alesia Koush, op. cit., p. 4.

Undersøgelser viser, at den samlede økonomiske værdi af den ulovlige handel med antikviteter og kunst er større end noget andet område af international kriminalitet med undtagelse af våbenhandel og narkotika[78] og er anslået til omkring 3-6 mia. USD om året.[79]

Det har været mange rapporter om forbindelserne mellem ulovlig handel med antikviteter og ulovlig handel med narkotika, dyr samt våben, hvidvask af penge og skatteunddragelse samt finansieringen af krigsmaskiner og terrororganisationer, hvilket bringer ulovlig handel med antikviteter på niveau med de alvorlige former for grænseoverskridende organiseret kriminalitet.

Hvidvask af penge – Lovovertrædere konverterer indtægterne fra kriminelle aktiviteter til antikviteter og kunstgenstand for lettere at kunne opbevare eller flytte disse aktiver.

Trussel

Finansiering af terrorisme

Vurderingen af truslen om terrorfinansiering som følge af ulovlig handel med røvede kulturgenstande og antikviteter viser, at de retshåndhævende myndigheder har fundet tilfælde af ulovlig handel med røvede kulturgenstande i EU. Medlemsstaternes retshåndhævende myndigheder har foretaget flere undersøgelser, ifølge hvilke den underliggende ulovlige handel med varer, der er bragt ud af konfliktområder[80] via fjernøstlige lande blev brugt til lettere at skjule varernes oprindelse. Hvor stor en andel det ulovlige marked udgør, bør naturligvis overvejes, men det er per definition svært at finde ud af. Af de nationale undersøgelser, der er foretaget indtil nu, fremgår det, at den største trussel kommer fra, at der sker plyndring af disse varer i tredjelande, navnlig i konfliktområder som Syrien, og at de terrororganisationer, der kontrollerer territoriet, derpå lægger afgifter på disse aktiviteter. For eksempel hedder det: "i stedet for at handle med kulturgenstande tjener Islamisk Stat penge på at sælge gravetilladelser og opkræve transitafgifter".[81] Men terrorister kan også sælge produkterne for at opnå indtægter, som det ses af førstehåndsbeviser indsamlet af USA[82] og anerkendt af De Forenede Nationers Sikkerhedsråd.[83]

De fleste genstande stjålet af terrorister i en række konfliktområder er små/mellemstore genstande, som stammer fra ulovlige udgravninger, hvilket gør det endnu sværere for de retshåndhævende myndigheder at fastslå tingenes herkomst og bevise, at et certifikat er falsk, især for mindre genstandes vedkommende.

---

[78] Lisa J. Borodkin, The Economics of Antiquities looting and a Proposed Legal Alternative', *Columbia Law Review*, No 2, 1995, p. 377-418.
[79] *Samme., s*. 377. Forfatterens skøn.

[80] https://blogs.state.gov/stories/2018/06/20/en/tackling-illicit-trafficking-antiquities-and-its-ties-terrorist-financing
[81] Kalifat i tilbagegang: An Estimate of Islamic State's Financial Fortunes, ICSR, 2017.
[82] https://www.justice.gov/usao-dc/pr/united-states-files-complaint-seeking-forfeiture-antiquities-associated-islamic-state
[83] FN's Sikkerhedsråds resolution 2347(2017) konstaterer (som R 2199, vedtaget i henhold til det bindende kapitel VII), at Islamisk Stat og grupper knyttet til al-Qaeda "genererer indtægter fra direkte eller indirekte deltagelse i plyndring og smugling af kulturarv" og bruger dem til at finansiere *"rekrutteringsindsatsen og at styrke deres kapacitet til at organisere og gennemføre terrorangreb"*.

Da tingene kan blive solgt i EU af formidlere, er der en indirekte, men reel risiko for finansiering af terrorisme.

Fra hensigts- og kapacitetsynspunktet udgør dette risikoscenarie en økonomisk set realistisk mulighed, når det tages i betragtning, at plyndring af kulturgenstande kan generere betydelige indtægter. Det er dog ikke en let metode. Den kræver (i kildelandene) adgang til den ulovlige/sorte økonomi (idet genstandene derefter ofte bliver hvidvasket og blandet med legale kredsløb i modtagerlandene), teknisk ekspertise og kendskab til kunstmarkedet, hvilket ikke alle terrorgrupper har kapacitet til. Desuden er det ikke tilstrækkelig sikkert eller diskret at transportere disse genstande, og at omsætte dem til kontanter kræver tid til planlægning, hvilket ikke harmonerer med terrorgruppers behov for at få adgang til kontanter hurtigt.

Man kan i forbindelse med trusselsanalysen ikke se bort fra truslens internationale dimension. Retshåndhævende myndigheder og FN beretter om dokumentation for, at der foregår plyndringer af og ulovlig handel med kulturgenstande i konfliktområderne. Disse aktiviteter giver økonomisk afkast, der kan anvendes af udenlandske terrorkrigere til at begå terrorhandlinger på EU's territorium. Der er også dokumentation for, at nogle radikaliserede i EU er fundet i besiddelse af kulturgenstande af uvis oprindelse.

Konklusion: På nuværende tidspunkt er der begrænset dokumentation for, at ulovlig handel med røvede kulturgenstande og antikviteter konkret vil blive brugt til at finansiere terroraktiviteter i EU. Det er imidlertid en attraktiv indtægtskilde for organisationer, der kontrollerer territorium i konfliktområder, som har til hensigt at finansiere terroraktiviteter i EU. Det påkrævede niveau af viden, ekspertise og planlægningskapacitet reducerer imidlertid trusselsniveauet. Trusselsniveauet mht. terrorfinansiering i relation til ulovlig handel med kulturgenstande og antikviteter anses derfor for i moderat grad betydeligt (dog forøget på grund af situationen i Mellemøsten og Nordafrika, og det forhold, at det territoriale "kalifat" – som havde institutionaliseret plyndringerne – er forsvundet, stopper ikke fortsættelsen af en vis udplyndring af mindre omfang) (niveau 2).

Hvidvask af penge

Vurderingen af truslen om hvidvask af penge, der hidrører fra ulovlig handel med røvede kulturgenstande og antikviteter, viser, at dette risikoscenarie kan være af interesse for organiserede kriminelle grupper, eftersom disse "produkter" kan konverteres til kontanter med henblik på at hvidvaske udbyttet fra kriminalitet eller at undgå skat. Retshåndhævende myndigheder mener, at denne form for ulovlig handel overvejende forekommer i frihavnszoner, og at dette gør det vanskeligere at måle omfanget af fænomenet. Der er dokumentation for, at organiserede kriminelle grupper bruger denne metode (mht. hvilken der er behov for ekspertise og viden for at sælge varerne til den bedste pris). Den illegale økonomi spiller også en rolle i dette scenarie, men er pr. definition vanskelig at vurdere. Nogle kriminelle net har forsøgt at afsætte forfalskede varer som stjålne, røvede antikviteter og har tilvejebragt svigagtige oplysninger om genstandenes herkomst.

Konklusion: Dette risikoscenarie kan være et attraktivt redskab for organiserede kriminelle grupper med henblik på at konvertere udbyttet af kriminalitet til rene kontanter. Det kræver imidlertid et højt fagligt niveau og er ikke en sikker aktivitet for dem. Trusselsniveauet mht. hvidvask af penge i relation til ulovlig handel med kulturgenstande anses derfor for i moderat grad betydeligt (niveau 2).

Sårbarhed

Finansiering af terrorisme

Vurderingen af sårbarheden over for terrorfinansiering hidrørende fra ulovlig handel med røvede kulturgenstande og antikviteter viser, at denne risiko for øjeblikket kun er i sin vorden, men at den kan vokse på kort sigt. Røvet gods kan tilbagesendes til EU i det nuværende klima. For eksempel kan der være, at nogle små stjålne kulturgenstande/mønter kan sælges af mennesker, der er radikaliseret i hjemlandet og som vender hjem til Europa, i mængder, der muligvis er for små til at kunne blive opdaget eller retsforfulgt.

a) risikoeksponering

Undersøgelser viser, at antikviteter udbydes til EU-samlere fra forskellige lande uden for EU, som regel via internetauktioner eller specialiserede onlinebutikker. Terrororganisationer kan bruge hemmeligholdelsesforanstaltninger som f.eks. spoofing af IP-adresse, hvilket gør det vanskeligt at identificere og fastslå sælgerens faktiske placering. Udnyttelse af sociale medier er også konstateret at være et hyppigere og hyppigere benyttet værktøj til at skære mellemleddet væk og sælge kulturgenstande direkte til købere.

Kontanttransaktioner foretrækkes (nogle gange for store beløb), men onlinetransaktioner er også udbredte uden mulighed for, at den finansielle institution kan identificere reelle ejer/sælger af antikviteterne. Der er ingen særlig overvågning af transaktionerne.

b) risikobevidsthed

Ifølge de retshåndhævende myndigheder enten ankommer kulturgenstandene ikke til EU's territorium eller forbliver uopdaget. Dette synes at vise, at de kompetente myndigheder og finansielle efterretningsenheders synlighed mht. dette forhold er meget lav. Forpligtede enheder foretager ikke nogen registrering (f.eks. om oprindelsen af kulturgenstande eller til hvem de sælges), og der er ingen rapportering. Toldmyndighederne har vanskeligt ved at opdage kulturgenstandenes illegale oprindelse.

c) retsgrundlag og kontroller

Regler om bekæmpelse af hvidvask af penge: ifølge EU's gældende regler om bekæmpelse af hvidvask af penge er personer, der handler med varer, underlagt EU's krav, når de modtager betaling i kontanter af et beløb på 10 000 EUR eller mere. Dette krav fokuserer på betalinger med kontanter og tager ikke hensyn til risiciene vedrørende andre typer betalingstransaktioner.

EU's nuværende regler om bekæmpelse af hvidvask af penge (fjerde hvidvaskdirektiv som ændret ved femte hvidvaskdirektiv) er nu rettet mod personer, der driver handel med kunstværker, og betragter dem som forpligtede enheder, når de handler med eller optræder som mellemled i forbindelse med handelen med kunstværker. Dette omfatter personer, der

opmagasinerer, handler med eller formidler handel kunstværker, når dette gennemføres af frihavne.

EU's ad hoc handelsforbud: EU har vedtaget ad hoc-foranstaltninger for import af kulturgenstande til Unionens toldområde fra Syrien og Irak. Rådets forordning (EF) nr. 1210/2003 af 7. juli 2003 om visse specifikke restriktioner i de økonomiske og finansielle forbindelser med Irak og Rådets forordning (EU) nr. 36/2012 om restriktive foranstaltninger på baggrund af situationen i Syrien forbyder handel med kulturgenstande med disse lande, hvor der er begrundet mistanke om, at varerne er bragt ud uden den retmæssige ejers tilladelse eller er bragt ud i strid med national ret eller folkeretten. De kompetente myndigheder har imidlertid stadig problemer med at spore et kulturgode med oprindelse i disse lande, og at anvende disse regler kan til tider være udfordrende på grund af de pågældende genstandes karakter (f.eks. en genstand, der ikke er ulovlig som sådan, men hvis virkelige herkomst det er vanskeligt at fastslå). Det er interessant at bemærke, at i de medlemsstater, som har formået at standse kulturskatte fra Irak eller Syrien, er dette tiltag en del af det daglige arbejde i de selvsamme institutioner, der kontrollerer den generelle import af kulturgenstande, og at anvende de relevante regler medfører ikke yderligere byrder på dem.

Under alle omstændigheder er de eksisterende EU-regler begrænset til bestemte regioner og dækker ikke alle tilfælde af import af kulturgenstande. Dette resulterer i, at kontrollen er utilstrækkelig i forhold til at tage vare på risiciene.

Konklusion: Selvom der ikke er meget, der tyder på, at de pågældende metoder anvendes i EU, ser det ud til, at risikoeksponeringen i øjeblikket kun er i sin vorden, men kan forøges som følge af den geopolitiske kontekst. Lovreglerne tillader ikke en effektiv overvågning af de pågældende transaktioner på grund af, at de forpligtede enheder ikke synes at være klar over denne sårbarhed over for terrorfinansiering (ingen rapportering, ingen registrering). Sårbarhedsniveauet over for finansiering af terrorisme i relation til køb af kulturgenstande og antikviteter anses derfor for betydeligt/meget betydeligt (niveau 3/4).

Hvidvask af penge

Vurderingen af sårbarheden over for hvidvask af penge hidrørende fra ulovlig handel med røvede kulturgenstande og antikviteter viser, at:

a) risikoeksponering

Da det af karakter er sensitivt, foretrækker man på markedet for kulturgenstande og antikviteter at anvende uformelle kanaler, hvor der ikke er nogen særlig sikkerhed eller overvågning af transaktioner. Der anvendes kontant betaling (til tider med store beløb), hvor identifikationen af køberen er næsten umulig.

b) risikobevidsthed

Sektoren virker mere bevidst omkring hvidvask af penge end om risiciene for terrorfinansiering. I flere medlemsstater modtager forhandlere af genstande af høj værdi

relevant undervisning og vejledning. Der er imidlertid et meget lavt niveau af indberetning af mistænkelige transaktioner, hvilket rejser spørgsmål om forståelsen af listen.

c) retsgrundlag og kontroller

Personer, der handler med varer, er omfattet af EU's regler om bekæmpelse af hvidvask af penge, når de modtager betaling i kontanter af et beløb på 10 000 EUR eller mere. EU's nuværende regler om bekæmpelse af hvidvask af penge anser nu også personer, der handler med kunstværker, som forpligtede enheder. Desuden er der i mange medlemsstater indført bestemmelser, som har til formål at begrænse kontante betalinger. Men ligesom med hensyn til terrorfinansiering er de nuværende kontroller utilstrækkelige til at håndtere de risici, som røvede kulturgode kan udgøre.

Desuden mener G7-medlemmerne, at ulovlig handel med kulturgenstande udgør en høj risiko, og at der skal arbejdes videre på dette område.

Konklusion: Selvom risikobevidstheden er højere end for terrorfinansiering, har vurderingens andre elementer fælles træk. Disse omfatter et lavt niveau af rapportering, og at der ingen beviser er for, at begrænsninger af kontantbetalinger har begrænset risiciene. Sårbarhedsniveauet over for hvidvask af penge i relation til køb af kulturgenstande og antikviteter anses derfor for betydeligt/meget betydeligt (niveau 3/4).

Risikobegrænsende foranstaltninger:

1) Kommissionen:

- Den 13. juli 2017 fremsatte Europa-Kommissionen et forslag til forordning om import af kulturgenstande[84], der skulle fastsætte betingelserne og procedurerne for indførsel af kulturgenstande i EU's toldområde. Kommissionen er også i færd med at gennemføre en undersøgelse om "Bedre viden om ulovlig handel med kulturgenstande inden for EU og de nye teknologier til at bekæmpe den".[85]
- Kommissionen har desuden vedtaget et forslag[86] til en hurtig styrkelse af EU's bestemmelser om forebyggelse af finansiering af terrorisme ved at øge gennemsigtigheden af kontantbetalinger. Dette skal ske ved at indføre en begrænsning i adgangen til at gennemføre kontante betalinger eller med alle andre hensigtsmæssige midler. Ved at begrænse mulighederne for at bruge kontanter ville forslaget hjælpe med til at afbryde finansieringen af terrorisme, da behovet for at bruge ikke anonyme betalingsmidler enten ville afskrække fra aktiviteten eller hjælpe til med, at den lettere kunne afsløres og efterforskes. Et sådant forslag vil også have som mål at harmonisere restriktionerne i EU med henblik på at skabe lige vilkår for virksomheder og fjerne konkurrenceforvridninger på det indre

[84] Europa-Parlamentets og Rådets forordning (EU) 2019/880 af 17. april 2019 om indførsel og import af kulturgenstande, PE/82/2018/REV/1, EUT L 151 af 7.6.2018, s. 1.
[85] Offentliggørelsen af denne undersøgelse var oprindelig planlagt til 2018/2019.
[86] Europa-Parlamentets og Rådets forordning (EU) 2018/1672 af 23. oktober 2018 om kontrol med likvide midler, der føres ind i eller ud af Unionen, og om ophævelse af forordning (EF) nr. 1889/2005, EUT L 284 af 12.11.2018, s. 6.

marked. Det ville også hjælpe på bekæmpelsen af hvidvask af penge, skattesvig og organiseret kriminalitet.

- Medlemsstaterne bør underrette om de foranstaltninger, som forhandlere af varer har truffet for at efterkomme deres forpligtelser mht. bekæmpelse af hvidvask af penge og af finansiering af terrorisme. Dette ville gøre det muligt for Kommissionen at foretage en yderligere vurdering af de risici, der udgøres af, at tjenesteudbydere accepterer kontante betalinger. Kommissionen vil også vurdere fordelene ved at lade yderligere sektorer blive omfattet af reglerne om bekæmpelse af hvidvask af penge og af finansiering af terrorisme.
- Det bør tages stilling til spørgsmålet om bevisbyrden og private salg.

2) Medlemsstaterne:

- Medlemsstaterne bør på passende måde tage hensyn til de risici, som kontantbetalinger udgør, i deres nationale risikovurderinger og træffe passende risikobegrænsende foranstaltninger. Medlemsstaterne bør overveje at lade de sektorer, der i særlig grad er udsat for risici for hvidvask af penge og terrorfinansiering, blive omfattet af de forebyggende ordninger vedrørende bekæmpelse af hvidvask af penge og af finansiering af terrorisme på grundlag af deres nationale risikovurdering.
- Medlemsstaterne bør tilskynde til øget samarbejde mellem retshåndhævende myndigheder og arkæologer, der er deres "øjne og ører" på dette felt.
- Medlemsstaterne bør uddanne de retshåndhævende myndigheders personale (told og politi) og sikre samarbejde og informationsudveksling mellem toldmyndigheder, grænsevagter og andre myndigheder.
- Fremme godkendelseskrav enten i eksportlandet og/eller i EU eller krav om egenerklæring, dvs. erklæring fra EU-importøren om, at varerne er bragt ud af eksportlandet i overensstemmelse med dettes love og forskrifter.
- Oplysningskampagner og fremme af foranstaltninger over for kunstmarkeder og museer, f.eks. grundig due diligence, forpligtelser til at føre computerstyrede lagerlister samt krav om formel EU-anerkendelse af eksisterende etiske kodeks eller adfærdskodeks for museer og kunstmarkeder.
- Overveje at tiltræde UNIDROIT-konventionen og Europarådets NICOSIA-konvention - eller gennemføre nogle af de foranstaltninger, der er tale om i disse konventioner.
- Forpligte virksomheder, der handler med kunst og opmagasinerer antikviteter (kaldet "frihavne"), til at oplyse om alle mistænkelige transaktioner, og at pålægge ejere af virksomheder, der handler med og opmagasinerer kunst og antikviteter, som bliver indblandet i handel med sådanne varer, virkningsfulde, forholdsmæssige og afskrækkende sanktioner, herunder strafferetlige sanktioner, når dette er nødvendigt.

3) Forpligtede enheder

- Øget anvendelse af skriftlige kontrakter med henblik på at få en meget detaljeret faktura med en klar beskrivelse af varerne (f.eks. værdi, produktbeskrivelse og et billede i høj kvalitet), hvilke også ville give mulighed fo, at den reelle ejer af transaktionen kan identificeres.

- Tilskynde til, at praksis med private transaktioner i kontanter til anonyme købere bringes til ophør.
- Fremme idéen om et solidt system til sporing af både online og fysisk handel i overensstemmelse med hele filosofien om bekæmpelse af hvidvask af penge.

5. Meget værdifulde aktiver – Ædelmetaller og ædelsten

Produkt
Meget værdifulde aktiver – guld og diamanter

Sektor
Forhandlere af meget værdifulde aktiver

Generel beskrivelse af den pågældende sektor og det/den relevante produkt/aktivitet

I EU er diamantmarkedet hovedsagelig begrænset til ét land — Belgien, og belgiske diamanthandlere sidder på den overvejende del af EU's diamantmarked. 1.700 virksomheder er officielt registreret som diamanthandlere hos Federal Public Service of Economy. Belgiens samlede import og eksport udgjorde 48 mia. USD alene i 2015. Verdens største mineselskaber har et kontor i Antwerpen og sælger en stor del af deres varer direkte til belgiske virksomheder. Belgien har fire diamantbørser, der er medlemmer af World Federation of Diamond Bourses. Ifølge 2015-oplysninger offentliggjort af Antwerpens diamantcenter[87] kommer 84% af alle uslebne diamanter og 50% af alle slebne diamanter på jorden fra Antwerpen.

Specialiserede finansielle institutioner stiller likviditet til rådighed for diamanthandelen. Virksomheder, der handler med diamanter, har brug for denne form for finansiering til køb store mængder uslebne diamanter og til at finansiere oparbejdningen af disse varer til slebne diamanter.

Beskrivelse af risikoscenariet

udbyttet af kriminalitet (f.eks. narkotikahandel) bliver enten flyttet til et andet land for at købe guld og smykker, som så sælges i et andet land ved brug af falske fakturaer og certifikater eller bliver brugt direkte til at købe guld i landet og solgt til en ædelmetalmægler, som derefter sælger det til andre virksomheder. Indtægterne fra salget kan derefter overføres til en tredjepart til at finansiere nye kriminelle aktiviteter. Lovovertrædere foretrækker ædelmetaller som guld og ædelsten som diamanter, da de er billige at opbevare og lette at forvandle til kontanter.

Trussel

Finansiering af terrorisme

Vurderingen af truslen om finansiering af terrorisme i relation til køb af guld og diamanter viser, at terroristerne benytter denne metode, da den er let tilgængelig og en realistisk økonomisk mulighed. Det kræver et moderat niveau af planlægning og ekspertise. Guld er almindeligt benyttet i krigszoner og er meget attraktivt for terrorister.

Konklusion: Niveauet af truslen om terrorfinansiering i relation til køb af guld og diamanter anses for i moderat grad betydeligt/betydeligt (niveau 2-3).

[87] Antwerp World Diamond Centre, https://www.awdc.be/.

Hvidvask af penge

Vurderingen af truslen om hvidvask af penge i forbindelse med køb af guld og diamanter viser, at lovovertræderne har udviklet store systemer til hvidvask af penge ved at bruge denne metode. Ifølge FATF's analyse er dette et højrisikoscenarie, idet guld og diamanter er let at flytte over grænserne (skjult i en bil for eksempel). Den internationale handel med guld har også været set som en teknik til at hvidvaske kriminelle indtægter. Den pågældende sag vedrørte anmeldt import af guld fra de Forenede Arabiske Emirater (UAE) til et EU-medlemsland, videresalget af guldet til en anden EU-medlemsstat og udførsel derfra tilbage til UAE. Aktivitetens karrusel-karakter og den lave kvalitet af det transporterede falske guld i denne sag giver anledning til at formode, at varehandelen kun blev foretaget for godtgøre berettigelsen af kriminelle pengeoverførsler. Denne metode er tæt forbundet med vurderingen af kurerer med guld og diamanter (se særskilt afsnit).

Konklusion: Trusselsniveauet mht. hvidvask af penge i relation til køb af guld og diamanter anses for meget betydeligt (niveau 4).

Sårbarhed

Finansiering af terrorisme

Niveauet af sårbarhed over for terrorfinansiering i relation til køb af guld og diamanter viser følgende:

a) risikoeksponering

Nogle repræsentanter for den private sektor nævner, at brugen af kontanter i diamanthandelen er faldet takket være de begrænsninger, der er pålagt i visse nationale love om bekæmpelse af hvidvask (i nogle lande er kontante betalinger begrænset til 10% af det samlede beløb for transaktionen, med et maksimum på 3 000 EUR). Der foreligger imidlertid ingen konkrete oplysninger om guldhandelen, hvor betaling med kontanter stadig anvendes gennemgående uden mulighed for at identificere de parter, der er involveret i transaktionen.

b) risikobevidsthed

Den er meget lav for så vidt angår risiciene for finansiering af terrorisme. Der gælder ingen særlig lovgivning, der begrænser transport og køb af guld og diamanter. På grund af den grænseoverskridende karakter af sådanne bevægelser er det svært eller ligefrem umuligt at føre kontrol.

For så vidt angår handel med diamanter har nogle nationale organisationer af diamanthandlere udviklet en organisatorisk ramme for vejledning, kurser og hjælp til indberetninger om mistænkelige transaktioner samt bistand til risikoanalyse. Disse organisationer kan også sørge for "kend dine kunder"-databaser, hvilket omfatter sanktionslister, oplysninger om politisk eksponerede personer og/eller lister over tredjelande med høj risiko. Nogle diamanthandlere sikrer, at identifikations- og verifikationsprocedurer bliver gennemført før en transaktion, der omfatter betaling via bankoverførsel.

Imidlertid er denne praksis temmelig begrænset og ikke tilstrækkeligt udbredt til, at man kan anse sektoren for velkendt med risiciene.

Med hensyn til handelen med guld blev der ikke modtaget nogen særlig feedback fra den private sektor, idet det var umuligt at identificere et kontaktpunkt med henblik på at drøfte bekæmpelse af hvidvask af penge.

c) retsgrundlag og kontroller

Personer, der handler med varer, er omfattet af EU's regler om bekæmpelse af hvidvask af penge, når de modtager betaling i kontanter af et beløb på 10 000 EUR eller mere. Disse krav mht. bekæmpelse af hvidvask af penge er begrænset til betalinger med kontanter og tager ikke hensyn til de risici, der kommer af brugen af andre betalingsmidler.

For så vidt angår handel med diamanter er en af de største grupper af diamanter i Europa omfattet af reglerne om bekæmpelse af hvidvask af penge og af finansiering af terrorisme. Derfor er de fleste europæiske diamanthandlere underkastet registreringskrav (efter kontrol af egnethed og hæderlighed — især fra et reel ejer-synspunkt) og inspektioner fra deres ansvarlige myndigheder, der har kompetence til at kontrollere både overholdelse af forpligtelserne vedrørende bekæmpelse af hvidvask af penge og vedrørende kontante betalinger.

EU har "Kimberley"-myndigheder[88] i seks lande, der kontroller importerede og eksporterede forsendelser af uslebne diamanter, især for tilstedeværelsen af et Kimberley-certifikat (Belgien, Det Forenede Kongerige, Tyskland, Tjekkiet, Rumænien og Portugal). Det betyder, at uslebne diamanter ikke kan importeres til eller eksporteres fra EU uden et Kimberley-certifikat og uden at passere en af de seks specialmyndigheder i Kimberly-processen (KP). Disse seks KP-myndigheder er udpeget af EU-Kommissionen og virker under dennes tilsyn. Derfor er transport af uslebne diamanter altid undergivet kontrol, når de bringes ind i eller ud af EU. Da handel med uslebne diamanter uden et KP-certifikat er ensbetydende med "ulovlig handel", er KP en stærk præventiv foranstaltning mod hvidvask af penge.

EU's regler er noget anderledes for polerede diamanter, idet de kan indføres overalt i EU. For så vidt angår medlemsstater, der har et meget strengt import- og eksportkontrolsystem for diamanter, som er importeret fra lande uden for EU eller eksporteres ud af EU, er det muligt at omgå denne kontrolmekanisme ved at importere/eksportere via et andet EU-land.

National lovgivning er imidlertid ikke harmoniseret hverken for diamanter eller guld, og dette skaber en risiko for, at der er forskelle i de opstillede krave (f.eks. mht. registrering) og de kontroller, der gennemføres.

For så vidt angår guld er den manglende harmonisering af lovgivningen også problematisk mht. kontrol og håndhævelse.

[88] Kimberley-processen (KP) er en påtagen forpligtelse til at fjerne konfliktdiamanter fra den globale forsyningskæde. I dag forhindrer deltagerne aktivt 99,8 % af den globale handel. Siden KP blev indført i 2003 er den identificerbare handel med konfliktdiamanter faldet fra 15 % til under 1 %. https://www.kimberleyprocess.com/en/european-union-0.

Antallet af rapporter om mistænkelige transaktioner er temmelig lavt for denne kategori af forpligtede enheder. Transaktioner sker ofte ansigt til ansigt, hvilket udgør en særlig udfordring mht. beskyttelse af medarbejdere.

Konklusion: Efter det ovenfor anførte anses sårbarheden over for finansiering af terrorisme i relation til køb af guld og diamanter for betydeligt (niveau 3).

Hvidvask af penge

Niveauet af sårbarhed over for hvidvask af penge i relation til køb af guld og diamanter viser, at

a) risikoeksponering

Nogle repræsentanter for den private sektor nævner, at brugen af kontanter i diamanthandelen er faldet takket være de begrænsninger, der er pålagt i visse nationale love om bekæmpelse af hvidvask (i nogle lande er kontante betalinger begrænset til 10 % af det samlede beløb for transaktionen, med et maksimum på 3 000 EUR). Der foreligger imidlertid ingen konkrete oplysninger om guldhandelen, hvor betaling med kontanter stadig anvendes gennemgående uden mulighed for at identificere de parter, der er involveret i transaktionen.

b) risikobevidsthed

Den er meget lav for så vidt angår risiciene for hvidvask af penge. Der gælder ingen særlig lovgivning, der begrænser transport og køb af guld og diamanter. På grund af den grænseoverskridende karakter af sådanne bevægelser er kontroller vanskelige eller ligefrem umulige gennemføre.

For så vidt angår handel med diamanter har nogle nationale organisationer af diamanthandlere udviklet en organisatorisk ramme for vejledning, kurser og hjælp til indberetninger om mistænkelige transaktioner samt bistand til risikoanalyse. Disse organisationer kan også sørge for "kend dine kunder"-databaser, hvilket omfatter sanktionslister, oplysninger om politisk eksponerede personer og/eller lister over tredjelande med høj risiko. Nogle diamanthandlere sikrer, at identifikations- og verifikationsprocedurer bliver gennemført før en transaktion, der omfatter betaling via bankoverførsel.

Imidlertid er denne praksis temmelig begrænset og ikke tilstrækkeligt udbredt til, at man kan anse sektoren for velkendt med risiciene. Diamant- og guldsektorerne består for det meste består af små virksomheder (ofte enkeltmandsvirksomheder), hvor den ansvarlige ikke har nogen juridisk baggrund og kan have svært ved at omsætte lovgivningen om bekæmpelse af hvidvask af penge til praksis og bringe procedurerne vedrørende kundekendskabskrav i anvendelse.

Med hensyn til handelen med guld blev der ikke modtaget nogen særlig feedback fra den private sektor, idet det var umuligt at identificere et kontaktpunkt med henblik på at drøfte bekæmpelse af hvidvask af penge.

c) retsgrundlag og kontroller

Personer, der handler med varer, er omfattet af EU's regler om bekæmpelse af hvidvask af penge, når de modtager betaling i kontanter af et beløb på 10 000 EUR eller mere. Disse krav mht. bekæmpelse af hvidvask af penge er begrænset til betalinger med kontanter og tager ikke hensyn til de risici, der kommer af brugen af andre betalingsmidler.

For så vidt angår handel med diamanter er en af de største grupper af diamanter i Europa omfattet af reglerne om bekæmpelse af hvidvask af penge og af finansiering af terrorisme. Derfor er nogle af de europæiske diamanthandlere underkastet registreringskrav (efter kontrol af egnethed og hæderlighed — især fra et reel ejer-synspunkt) og inspektioner fra deres ansvarlige myndigheder, der har kompetence til at kontrollere både overholdelsen af forpligtelserne vedrørende bekæmpelse af hvidvask af penge og vedrørende kontante betalinger.

EU har Kimberley"myndigheder i seks lande, der kontroller importerede og eksporterede forsendelser af uslebne diamanter, især for tilstedeværelsen af et Kimberley-certifikat (Belgien, Det Forenede Kongerige, Tyskland, Tjekkiet, Rumænien og Portugal). Det betyder, at uslebne diamanter ikke kan importeres til eller eksporteres fra EU uden et Kimberley-certifikat og uden at passere en af de seks specialmyndigheder i KP. Disse seks KP-myndigheder er udpeget af Kommissionen og virker under dennes tilsyn. Derfor er transport af uslebne diamanter altid undergivet kontrol, når de bringes ind i eller ud af EU. Da handel med uslebne diamanter uden et KP-certifikat er ensbetydende med "ulovlig handel", er KP en stærk præventiv foranstaltning mod hvidvask af penge.

EU's regler er noget anderledes for polerede diamanter, idet de kan indføres overalt i EU. For så vidt angår medlemsstater, der har et meget strengt import- og eksportkontrolsystem for diamanter, som er importeret fra lande uden for EU eller eksporteres ud af EU, er det muligt at omgå denne kontrolmekanisme ved at importere/eksportere via et andet EU-land.

National lovgivning er imidlertid ikke harmoniseret hverken for diamanter eller guld, og dette skaber en risiko for, at der er forskelle i de opstillede krave (f.eks. mht. registrering) og de kontroller, der gennemføres.

For så vidt angår guld er den manglende harmonisering af lovgivningen også problematisk mht. kontrol og håndhævelse.

Antallet af rapporter om mistænkelige transaktioner er temmelig lavt for denne kategori af forpligtede enheder. Transaktioner sker ofte ansigt til ansigt, hvilket udgør en særlig udfordring mht. beskyttelse af medarbejdere.

Konklusion: Selvom regler indført i nogle medlemsstater har skærpet risikobevidstheden, er sektoren endnu ikke organiseret godt nok til, at det er muligt at gennemføre en effektiv overvågning og vejledning. Sårbarhedsniveauet over for hvidvask af penge i relation til køb af guld og diamanter anses derfor for betydeligt (niveau 3).

Risikobegrænsende foranstaltninger:

1) Medlemsstaterne:

- Medlemsstaterne bør på passende måde tage hensyn til de risici, som kontantbetalinger udgør, i deres nationale risikovurderinger og træffe passende risikobegrænsende foranstaltninger. Medlemsstaterne bør overveje at lade de sektorer, der i særlig grad er udsat for risici for hvidvask af penge og terrorfinansiering, blive omfattet af de forebyggende ordninger vedrørende bekæmpelse af hvidvask af penge og af finansiering af terrorisme på grundlag af deres nationale risikovurdering.

- Medlemsstaterne bør sikre, at de kompetente myndigheder foretager tilstrækkelige uanmeldte stikprøvekontroller i diamantvirksomheders og guldhandleres forretningslokaler for at afdække eventuelle smuthuller i overholdelsen af kundekendskabskravene og inddrage diamanteksperter til at kontrollere flowet af varer.

2) Forpligtede enheder:

- Uddannelse i kundekendskabskrav, navnlig for mindre virksomheder.
  Denne opgave kan varetages af en sektorsammenslutning eller af en diamantbørs for diamanthandlernes vedkommende. Uddannelsen vil kunne dreje sig om grundlæggende krav vedrørende bekæmpelse af hvidvask af penge og af finansiering af terrorisme, f.eks. hvordan man identitetskontrollerer kunder, hvordan man udfører en risikoanalyse, hvad reelle ejere er, hvad en finansiel efterretningsenhed er, og hvordan man underretter en sådan mv.
- Øget anvendelse af skriftlige kontrakter med henblik på at få en meget detaljeret faktura med en klar beskrivelse af varerne (f.eks. værdi, vægt, kvalitet).

3) Kommissionen:

- Efter den nye forordning om kontrol med likvide midler er definitionen af kontanter blevet udvidet til at omfatte ikke kun pengesedler, men også andre instrumenter eller højlikvide aktiver som f.eks. checks, rejsechecks, forudbetalte kort og guld.

- Der kunne gennemføres yderligere undersøgelser med henblik på at uddybe analysen af de økonomiske sektorer/ situationer som er mest udsat for risici i forhold til bekæmpelse af hvidvask af penge og af finansiering af terrorisme.

Der kunne foretages yderligere typologiarbejde med henblik på at identificere de økonomiske sektorer, der er særligt udsatte for risici for hvidvask af penge og terrorfinansiering, før skræddersyede risikobegrænsende foranstaltninger udformes. Analysen kunne også kortlægge medlemsstaters praksis, da mange af dem har besluttet at at lade visse yderligere erhverv være omfattet af ordningen mht. bekæmpelse af hvidvask af penge og af finansiering af terrorisme pga. deres egen risikoanalyse.

6. Meget værdifulde aktiver – bortset fra ædelmetaller og ædelsten

Produkt
Meget værdifulde aktiver – bortset fra ædelmetaller og ædelsten

Sektor
Forhandlere af meget værdifulde aktiver

Beskrivelse af risikoscenariet

Lovovertrædere bruger meget værdifulde varer som en let måde til at integrere midlerne ind i det legale økonomiske kredsløb, idet de konverterer kriminelle kontanter til en anden aktivklasse, som bevarer sin værdi og også kan rumme muligheder for kapitalvækst. Visse produkter som personbiler - men også smykker, ure og luksusskibe er særligt attraktive som både livsstilsgoder og økonomiske aktiver.

Trussel

Finansiering af terrorisme

Vurderingen af truslen om terrorfinansiering i relation til køb af andre former for meget værdifulde varer (andre varer end guld, diamanter, kulturgenstande og antikviteter) er ikke blevet anset for relevant fra et terrorfinansieringsperspektiv. Derfor er truslen om terrorfinansiering ikke en del af vurderingen.

Konklusion: ikke relevant

Hvidvask af penge

Vurderingen af truslen om hvidvask af penge i relation til køb af andre former for meget værdifulde varer (andre varer end guld, diamanter, kulturgenstande og antikviteter) viser, at kriminelle organisationer gennemgående har brugt denne metode, som er let at bruge og ikke kræver nogen særlig ekspertise (den omfatter handel med smykker, biler, både og ure).

Kriminelle kontanter bliver ofte omvekslet til varer, som er meget efterspurgte på udenlandske markeder. Biler og andre køretøjer er en af de hyppigst købte og eksporterede varer. Hovedmarkederne er i Nordafrika og i Mellemøsten. Maskiner eksporteres til Irak og Kuwait, luksusure, guld og smykker eksporteres til Mellemøsten og Nordafrika, og mad eksporteres til Afrika.

Manglende restriktioner på kontantbetalinger i nogle EU-lande gør dem mere attraktive for kontantbaseret handelsbaseret hvidvask af penge. I andre lande – selv i lande med restriktioner og rapporteringsforpligtelser – er blandt dem med de mindste rapporteringsforpligtelser. I nogle tilfælde medbringer kriminelle kunder forretninger for millioner til den handlende, hvilket er en yderligere initiativhæmmende faktor i forhold til rapportering.

Kinesiske organiserede kriminelle grupperinger ses at have udnyttet luksusvarer (haute couture) og populære europæiske højstatusbrands på det kinesiske marked. Illegale

kontanter gives til kinesiske borgere, der bruger dem til at købe luksusvarer. Disse luksusvarer bliver fortrinsvis solgt online i Kina og provenuet bruges til at foretage betalinger i Kina. Kinesiske organiserede kriminelle gruppers illegale aktiviteter i Europa er den vigtigste kilde til kriminelt udbytte, der bruges til at købe disse varer. Disse ulovlige aktiviteter omfatter skatte- og afgiftssvig vedrørende kinesiske varer, vareforfalskning, handel med narkotika, udnyttelse af arbejdskraft og seksuel udnyttelse.

Ifølge de retshåndhævende myndigheders oplysninger blev kinesiske statsborgere med bopæl i EU brugt som pengesmuglere indtil 2015-2016. De åbnede bankkonti, foretog kontante indskud og overførte pengene til Kina. En anden metode var at bruge de tilrejsende kinesiske turister til at overføre kontanter ved deres tilbagekomst til Kina. Med tiden og takket være de retshåndhævende myndigheders indskriden gik de kinesiske kriminelle grupperinger over til andre teknikker som f.eks. at benytte indkøbere til at købe luksusvarer. Efter at være blevet købt i Europa bliver varerne bragt til Kina, hvor de sælges med en avance, og det opnåede overskud overføres internt i Kina mellem køberne af varerne og de kriminelle strukturer. Denne metode er en måde, hvorpå de kriminelle kan gennemføre en fuld hvidvask-cyklus, så de frit kan anvende provenuet i Kina til for eksempel at betale for nye partier kinesiske varer. Når de bliver indført i Europa, bliver disse varepartier prissat under værdien og solgt uden papirer. De indvundne kontanter bliver på ny hvidvasket og bragt fra Europa til Kina, hvilket skaber en kriminel cyklus, som omgår både de retshåndhævende myndigheder og skattemyndigheders indskriden.

Konklusion: Trusselsniveauet mht. hvidvask af penge i relation til køb af andre former for meget værdifulde varer anses for meget betydeligt (niveau 4).

Sårbarhed

Finansiering af terrorisme

Vurderingen af truslen om terrorfinansiering i relation til køb af andre former for meget værdifulde varer (andre varer end guld, diamanter, kulturgenstande og antikviteter) er ikke blevet anset for relevant fra et terrorfinansieringsperspektiv. Sårbarhed over for terrorfinansiering er derfor ikke en del af vurderingen.

Konklusion: Ikke relevant.

Hvidvask af penge

Vurderingen af sårbarheden over for hvidvask af penge i relation til køb af andre former for meget værdifulde varer (andre varer end guld, diamanter, kulturgenstande og antikviteter) viser, at dette risikoscenarie har de samme sårbarheder som dem, der gælder for køb af guld og diamanter.

a) risikoeksponering:

Det er vanskeligt at angive de forskellige typer varer, der vil kunne anvendes til at hvidvaske penge. Men handelen med andre meget værdifulde varer end guld og diamanter kan være stærkt afhængig af kontanttransaktioner med lavt niveau af sikkerhed og

overvågning i fordelingskanalerne. Den kan involvere grænseoverskridende transaktioner, der er vanskelige at kontrollere.

b) risikobevidsthed:

Den er meget lav for så vidt angår risiciene for hvidvask af penge. Sektoren er fuldstændig åben, og der er ingen konkrete organisatoriske rammer, som kan sørge for vejledning og uddannelse. Foranstaltninger til opfyldelse af kundekendskabskrav bliver ikke anvendt, og niveauet for indberetning af mistænkelige transaktioner viser, at forståelsen af risikoen er meget lav.

c) retsgrundlag og kontroller:

Personer, der handler med varer, er omfattet af EU's regler om bekæmpelse af hvidvask af penge, når de modtager kontant betaling af et beløb på 10 000 EUR eller mere. Denne definition er imidlertid temmelig generel og specificerer ikke, hvilke kategorier af handelsvarer, der falder ind under hvidvaskdirektivet. Hertil kommer, at disse krav mht. bekæmpelse af hvidvask af penge er begrænset til betalinger med kontanter og ikke tager hensyn til de risici, der kommer af brugen af andre betalingsmidler. Ikke desto mindre har nogle medlemsstater har indført restriktioner mht. kontantbetaling.

Der er imidlertid ingen harmoniserede nationale lovgivninger til at imødegå risiciene i forbindelse med handel med meget værdifulde varer. Det lader til, at niveauet for registerføring er meget lavt, og at kontroller ikke findes.

Konklusion: Selvom regler indført i nogle medlemsstater har skærpet risikobevidstheden, er sektoren endnu ikke organiseret godt nok til at gennemføre en effektiv overvågning og give vejledning. Trusselsniveauet mht. hvidvask af penge i relation til køb af andre former for meget værdifulde varer anses for betydeligt (niveau 3).

Risikobegrænsende foranstaltninger:

1) Kommissionen:

Kommissionen har undersøgt de potentielle virkninger af restriktioner af kontantbetalinger og har udgivet en rapport om emnet.[89] Rapporten konkluderer, at Kommissionen ikke bør overveje lovgivningsinitiativer på dette område på nuværende tidspunkt. Begrænsninger af kontantbetalinger er et følsomt emne for mennesker i EU, hvoraf mange ser på

[89] Rapport fra Kommissionen til Europa-Parlamentet og Rådet om restriktioner for kontantbetalinger — COM (2018) 483 final: https://ec.europa.eu/info/sites/info/files/economyfinance/com_2018_483_f1_report_from_commission_en_v4_p1_981536.pdf.

muligheden for at betale kontant som en grundlæggende frihedsrettighed, som ikke bør begrænses uforholdsmæssigt.

- Medlemsstaterne bør underrette om de foranstaltninger, som vareforhandlere, der er omfattet af hvidvaskdirektivet, har truffet for at efterkomme deres forpligtelser mht. bekæmpelse af hvidvask af penge og af finansiering af terrorisme. På dette grundlag kunne Kommissionen foretage en yderligere vurdering af de risici, der udgøres af, at tjenesteudbydere accepterer kontantbetalinger. Kommissionen vil også vurdere fordelene ved at lade yderligere sektorer blive omfattet af reglerne om bekæmpelse af hvidvask af penge og af finansiering af terrorisme.

2) Medlemsstaterne:

Medlemsstaterne bør på passende måde tage hensyn til de risici, som kontantbetalinger udgør, i deres nationale risikovurderinger og træffe passende risikobegrænsende foranstaltninger. Medlemsstaterne bør overveje at lade sektorer, der i særlig grad er udsat for risici for hvidvask af penge og terrorfinansiering, blive omfattet af de forebyggende ordninger vedrørende bekæmpelse af hvidvask af penge og af finansiering af terrorisme på grundlag af deres nationale risikovurdering.

7. Kurerer af ædelmetaller og ædelsten

Produkt
Guld og andre ædelmetaller

Sektor
/

Beskrivelse af risikoscenariet

Det vedrører den grænseoverskridende transport af guld og andre ædelmetaller samt ædelsten. Lovovertrædere, der har tjent kontanter på deres illegale aktiviteter, søger at konvertere dem til guld og andre ædelmetaller eller sten, så de enten kan tilbageføre midler eller flytte disse varer til steder, hvor de lettere kan indplaceres i den legale økonomi.

Kurerer kan anvende luft-, sø- og jernbanetransport for at krydse en international grænse, via for eksempel:
- containertransport eller andre former for fragt, skjult i breve eller postpakker — hvis lovovertrædere ønsker at flytte meget store mængder guld og andre ædelmetaller, er deres eneste mulighed ofte at skjule det blandt fragt, der kan transporteres i containere eller på anden måde transporteres over grænserne, eller
- snedigt skjul af guld blandt varer sendt med almindelige brev- eller pakkeforsendelser.

Trussel

Finansiering af terrorisme

Vurderingen af truslen om terrorfinansiering i relation til guld og andre ædelmetaller viser kun få indikatorer af, at terrorgrupper bruger eller har til hensigt at benytte denne kanal til at finansiere terroraktiviteter.

Guld- og diamantkurerer er ikke den mest attraktive og sikre mulighed for terrorgrupper — selvom disse aktiver ofte benyttes i krigszoner, idet de er lette at handle. Der er opdaget/indberettet nogle tilfælde af udenlandske terrorkrigere, der har byttet deres ejendele til guld, men situationen er ikke tilbagevendende og kræver under alle omstændigheder planlægning og viden.

Konklusion: Guld- og ædelmetalkurerer er ikke en foretrukken metode for terrorgrupper, der er tilbøjelige til at gøre brug af kontanter. Trusselsniveauet for finansiering af terrorisme anses derfor for i et vist omfang betydeligt til betydeligt (2).

Hvidvask af penge

Vurderingen af truslen om hvidvask af penge i i relation til kurerer af guld og andre ædelmetaller viser, at organiserede kriminelle grupper har anvendt denne metode til at hvidvaske udbyttet af kriminalitet. I modsætning til terrororganisationer anser organiserede kriminelle grupper det for at være en attraktiv måde, hvorpå man kan hvidvaske udbytte af kriminalitet. Det kræver mere planlægning end at flytte kontanter,

men kræver ikke den store ekspertise, så længe det drejer sig om let omsættelige aktiver (dvs. præference for guld sammenlignet med andre ædelmetaller — diamanter sammenlignet med andre sten). Aktiviteterne er ikke kostbare. Lovovertrædere har derfor den nødvendige kapacitet til og hensigt om at bruge denne metode. Retshåndhævende myndigheder rapporterer, at der har været anvendt andre typer ædelmetaller (sølv, platin), men disse er ikke hyppigt anvendt, fordi de er mindre let omsættelige og kræver højere vekselgebyrer end guld og diamanter.

Undersøgelser foretaget i EU viser, at en af de mest relevante kontantrelaterede teknikker er at transformere kontanter til guld eller smykker. Nogle EU-lande som Italien og Belgien har aktive guldmarkeder. Side om side med det legale marked viser oplysninger, at guldet bliver stjålet og smeltet om. Efter at kriminelle kontanter er blevet vekslet til guld, eksporteres det til Mellemøsten og Nordafrika, hvor der er stor efterspørgsel i markedet.

Konklusion: Trusselsniveauet mht. hvidvask af penge i relation til guld og andre ædelmetaller anses for betydeligt (niveau 3).

Sårbarhed

Finansiering af terrorisme

Vurderingen af sårbarheden over for finansiering af terrorisme i relation til kurerer for guld og andre ædelmetaller viser, at

a) risikoeksponering

Vurderingen af sårbarheden over for terrorfinansiering viser, at risikoeksponeringen er uløseligt forbundet med den kontantbaserede aktivitet (anonymitet, hastighed). Risikoeksponeringen er derfor særdeles betydelig for denne metode.

b) risikobevidsthed

Sektoren viser en begrænset risikobevidsthed, og de eksisterende kontroller er særdeles svage.

c) retsgrundlag og kontroller

Indtil den nye kontantforordning træder i kraft, er der ingen kontrol af rigtigheden af de obligatoriske angivelser af transport af ædelmetaller/sten ved EU's ydre grænser. Disse aktiver er ikke lette at opdage. Kontrol i bestemmelseslande uden for EU bidrager ikke til at nedbringe risikoen (konvertering af guld/diamanter til kontanter i bestemmelseslande uden kundekendskabskrav).

Konklusion: Kurerer af guld og andre ædelmetaller er ikke genstand for ordentlig overvågning på grund af sektorens begrænsede risikobevidsthed. Kontrollerne er svage og anvendelsen af kontanter øger sårbarheden. Der eksisterer ingen kontrol med angivelser af flytning af ædelmetaller/sten ved EU's ydre grænser. Trusselsniveauet mht. finansiering af terrorisme i relation til kurerer af guld og andre ædelmetaller anses derfor for meget betydeligt (niveau 4).

Hvidvask af penge

Vurderingen af truslen om hvidvask af penge i relation til kurerer af guld og andre ædelmetaller viser følgende:

a) risikoeksponering

Risikoeksponeringen er snævert forbundet med den kontantbaserede aktivitet (anonymitet, hurtighed). Risikoeksponeringen er derfor særdeles betydelig for denne metode.

b) risikobevidsthed

Sektoren udviser begrænset risikobevidsthed, og de eksisterende kontroller er særdeles svage. Retshåndhævende myndigheder har også bemærket, at kriminelle organisationer udnytter vagheden i EU's regelsæt, navnlig for så vidt angår videregivelse af oplysninger om kontantbetalinger.

c) Retsgrundlag og kontroller

Der findes ingen kontroller i forbindelse med den obligatoriske angivelse af transport af ædelmetaller/sten ved EU's ydre grænser (dvs. dette er ikke omfattet af forordningen om kontrol med likvide midler). De pågældende aktiver er ikke lette at opdage. Kontrol i bestemmelseslande uden for EU bidrager ikke til at nedbringe risikoen (konvertering af guld/diamanter til kontanter i bestemmelseslande uden kundekendskabskrav).

Konklusion: Kurerer af guld og andre ædelmetaller er ikke genstand for et ordentlig overvågning på grund af sektorens begrænsede risikobevidsthed. De eksisterende kontroller er svage, og anvendelsen af kontanter øger sårbarheden. Der eksisterer ingen kontrol med angivelse af flytning af ædelmetaller/sten ved EU's ydre grænser. Sårbarhedsniveauet over for hvidvask af penge i relation til guld og andre ædelmetaller anses derfor for meget betydeligt (niveau 4).

Risikobegrænsende foranstaltninger:

Som anbefalet i den supranationale risikovurdering 2017 har Kommissionen vedtaget en ny kontantforordning med henblik på at reducere de beskrevne risici.

8. Investering i fast ejendom

Produkt
Køb og salg af fast ejendom

Sektor
Sektoren for fast ejendom, uafhængige retlige aktører, notarer, kreditinstitutter

Beskrivelse af risikoscenariet

Hvidvask af penge gennem fast ejendom er et voksende globalt problem, der skønnes at have nået 1,6 billioner USD om året. Selvom den præcise størrelsesorden af den ulovlige aktivitet i sektoren er vanskelig at vurdere, menes personer eller selskaber med en høj risiko for hvidvask af penge i 2017 at have ejet ejendom for mere end 4,2 mia. GBP i London alene[90]. I Frankrig har den finansielle efterretningsenhed, TRACFIN, identificeret ejendomssektoren som en primær kanal til hvidvask af penge i landet. Ud af i alt 62.000 mistankeberetninger, der indgik til TRACFIN i 2016, kom kun 84 fra ejendomsmæglere, på trods af at der fandt næsten en million transaktioner sted det år[91].

Lovovertræderne kan (via visum-ordninger) som ikke hjemmehørende investere i et land og udvikle net til hvidvask af penge/ terrorfinansiering.

Trussel

Finansiering af terrorisme

Vurderingen af risikoen for terrorfinansiering i relation til investering i fast ejendom er blevet vurderet sammen med de systemer til hvidvask af penge, der vedrører investering i fast ejendom med henblik på at skjule midlernes illegale oprindelse. Det er derfor ikke nødvendigt at vurdere truslen om terrorfinansiering separat.

Konklusion: Truslen om finansiering af terrorisme i relation til investering i fast ejendom anses for meget betydelig (niveau 4).

Hvidvask af penge

Vurderingen af truslen om hvidvask af penge i relation til investering i fast ejendom har sat fokus på organiserede kriminelles gennemgående brug af ejendomssektoren til hvidvask af udbyttet af kriminalitet. Sektoren for fast ejendom anvendes oftest i kombination med andre sektorer som f.eks. udbydere af tjenester til truster og selskaber eller juridisk rådgivning, men udgør en vis trussel i sig selv. At operere på grundlag af fast

[90] Faulty towers: Understanding the impact of overseas corruption on the London property market, Transparency International UK, marts 2017:
https://www.transparency.org.uk/publications/faulty-towers-understanding-the-impact-of-overseas-corruption-on-the-london-property-market/#.W9LY-LpuaUk.

[91] Le Monde, "Blanchiment d'Argent: les agenter immobiliers font-ils preuve de profiterer?", 29. December 2017:
http://www.lemonde.fr/societe/article/2017/12/29/blanchiment-d-argent-les-agents-immobiliers-en-premiereligne_5235527_3224.html

ejendom kræver ikke særlig ekspertise eller viden og kan være økonomisk ganske attraktivt afhængigt af den leverede ydelse.

Konklusion: På baggrund af stærke beviser indsamlet af retshåndhævende myndigheder for, at fast ejendom ofte anvendes i systemer til hvidvask af penge, og fordi disse tjenester kan kombineres med andre ikkefinansielle faggruppers ydelser, anses trusselsniveauet for hvidvask af penge i relation til fast ejendom for meget betydeligt (niveau 4).

Sårbarhed

Finansiering af terrorisme

Vurderingen af sårbarheden over for terrorfinansiering i relation til investering i fast ejendom er blevet vurderet sammen med de systemer til hvidvask af penge, der vedrører investering i fast ejendom med henblik på at skjule midlernes illegale oprindelse. Det er derfor ikke nødvendigt at vurdere truslen om terrorfinansiering separat.

Konklusion: Sårbarheden over for finansiering af terrorisme i relation til investering i fast ejendom anses for meget betydelig (niveau 4).

Hvidvask af penge

Vurderingen af sårbarhed over for hvidvask af penge i relation til investering i fast ejendom viser følgende:

a) risikoeksponering

Selvom metoden er i aftagende i praksis, kan kontanter stadig bruges til at finansiere ejendomstransaktioner i nogle medlemsstater. Dette øger risikoen for anonyme transaktioner. Ejendomsmæglere deltager normalt i et samarbejde med andre faggrupper, hvilket gør det vanskeligt at overvåge forretningsforbindelsen effektivt (sektorer sætter deres lid til hinanden mht. at gennemføre kontrol)[92], og derfor øges risikoeksponeringen. Ejendomstransaktioner kan være baseret på pengestrømme, der kommer fra lande uden for EU og fra højrisikokunder som f.eks. politisk eksponerede personer.

b) risikobevidsthed

Bevidsthedsniveauet er ujævnt i sektoren, og afhænger især af størrelsen af organisationen/virksomheden. Større strukturer kan være mere bevidste om risikoen for at blive misbrugt og mene, at de har en rolle at spille med hensyn til at overvåge deres kunder. Nogle af dem er at ved at udvikle informations- og undervisningsværktøjer samt risikovurderinger. Sektorens medlemmer er bevidste om deres retlige forpligtelser, f.eks. tilfælde, hvor der gælder skærpede kundekendskabskrav.

[92] Ikke desto mindre ligger det endelige ansvar hos den pågældende, dvs. de erhvervsdrivende må ikke stole på hinanden (jf. betragtning 35 til og artikel 25 i det fjerde hvidvaskdirektiv). Tværtimod kan det, at flere opfylder deres forpligtelser mht. kundekendskabskrav, øge chancen for at afsløre hvidvaskaktiviteter.

For små enheders vedkommende, bortset fra retlige aktører, som er en del af en paraplyorganisation, er bevidsthedsniveauet drastisk lavere, fordi: i) de ikke nødvendigvis er integreret i en samlet organisatorisk ramme, der sørger for vejledning og undervisning, ii) de har en mindre omsætning og kan derfor have vanskeligheder med at forstå og anvende en kompleks hvidvasklovgivning (dette er især tilfældet for enkeltmandsvirksomheder), og/eller iii) de har tendens til at sætte deres lid til andre sektorer med hensyn til gennemførelsen af kundekendskabskrav.

De samme oplysninger er muligvis ikke tilgængelige i alle faser af transaktionen, f.eks. hvis køberens identitet ændres af praktiske eller forretningsmæssige grunde, og denne ændring ikke er kendt ved indledningen af forretningsforbindelsen. Bevidsthedsniveauet i små enheder afhænger af, hvor megen undervisning, der er til rådighed.

Under alle omstændigheder gør de forpligtede enheders "spredthed" det ikke lettere at gennemføre kontrollen og forstå de kundekendskabskrav, der skal bringes i anvendelse. Tilsynet med sektoren er også ufuldstændigt og baseret på svage informationsstier (ingen skriftlige kontrakter, "solicitors", som kun er vant til at stemple et dokument osv.).

c) retsgrundlag og eksisterende kontroller

Ejendomsmæglere er omfattet af EU-reglerne om bekæmpelse af hvidvask af penge. Efter de ændringer, der blev indført ved det femte hvidvaskdirektiv, vil oplysninger om enhver fysisk eller juridisk persons ejendomsret til fast ejendom blive gjort centralt tilgængelige for offentlige myndigheder. Dette kræver ikke oprettelse af et centralt register over fast ejendom. Alternativt kan man bruge elektroniske informationssøgningssystemer.

Men når flere forpligtede enheder er involveret i ejendomstransaktioner, er det vanskeligt for de kompetente myndighederne at identificere den ejendomsmæglerens rolle og at konstatere faresignaler. Den juridiske praksis og procedurer for ejendomstransaktioner varierer fra land til land. I nogle lande kan ejendomsmægleren udarbejde den indledende juridiske dokumentation (selvom det kan være påkrævet, at en advokat færdiggør transaktionen), mens det i andre lande er en advokat, der udarbejder den juridiske dokumentation, herunder kontrakten.

Indberetning af mistænkelige transaktioner er ujævn og er kun tilfredsstillende, når de foretages af andre forpligtede enheder end ejendomsmæglere (nogle ejendomsmæglere synes at antage, at da de ikke er involveret i overførslen af midler, er det ikke dem, der står for rapportering om mistænkelige transaktioner). Som en konsekvens heraf kan undersøgende myndigheder foretage deres egen analyse, men ikke på grundlag af ejendomsoplysninger. Den private sektors repræsentanter mener, at det er en stor udfordring at identificere de reelle ejerforhold, da det ikke er obligatorisk at registrere sådanne oplysninger. Dette er især tilfældet, når køber og sælger handler i "trust".

Praksis på området varierer, og repræsentative brancheforeninger gør en indsats for at fremme kendskabet til og give deres medlemmer eksempler på god praksis.[93]

[93] Som et eksempel på god selvregulerende adfærd har de repræsentative organisationer i Belgien udviklet et onlineværktøj til at indsamle oplysninger og videregive dem til de nationale myndigheder. Dette værktøj er under udrulning i alle andre lande i EU, og nationale myndigheder kan yde støtte til at fremme overholdelse.

Konklusion: Sektoren for fast ejendom er ikke organiseret godt nok til i tilstrækkelig grad at øge risikobevidstheden. Inddragelse af forskellige former for forpligtede enheder i et ejendomstransaktions-/forretningsforhold trækker i retning af at afholde sektoren fra at gennemføre sit eget kundekendskabskrav. Rapporteringen af mistænkelige transaktioner er ikke tilfredsstillende. Kontrollerne er vanskelige at gennemføre, og der er ikke altid en god informationssti. Sårbarhedsniveauet over for hvidvask af penge i relation til sektoren for fast ejendom anses derfor for betydeligt/meget betydeligt (niveau 3/4).

Risikobegrænsende foranstaltninger:

1) kompetente myndigheder:

- Medlemsstaterne bør sikre, at de kompetente myndigheder/selvregulerende organer, der fører tilsyn med sektoren for fast ejendom, udarbejder en årsrapport om de tilsynsforanstaltninger, der er indført for at sikre, at sektoren præcist gennemfører sine forpligtelser med hensyn til bekæmpelse af hvidvask af penge og af finansiering af terrorisme. Selvregulerende organer bør aflægge årlig rapport om antallet af rapporter om mistænkelige transaktioner, der er indgivet til de finansielle efterretningsenheder.
- Inspektioner på stedet svarende til populationen af fastejendomsrepræsentanter på medlemsstatens territorium.

2) medlemsstaterne:

- Medlemsstaterne bør sørge for vejledning om risikofaktorer i forbindelse med ejendomshandler og særlig uddannelse i situationer, hvor flere faggrupper deltager i ejendomstransaktioner (f.eks. ejendomsmægler, advokat, finansieringsinstitut).

3) styring på flere niveauer og lokal forvaltning: forbedret videnudveksling og samarbejde:

Europæiske byer er særligt udsatte for de negative samfundsmæssige konsekvenser af, at penge hvidvaskes i fast ejendom. Dette blev fremhævet under den offentlige høring i "Tax3-Udvalget" i Europa-Parlamentet den 5. februar 2019. I 2018 var Amsterdam vært for en tre-dages konference med titlen "Flyvende penge" om virkningen af ulovlige pengestrømme, hvor 14 europæiske byer fortalte om deres erfaringer. En konklusion var, at det ville være nyttigt at se, hvordan de forskellige styringsniveauer, der deltager i bekæmpelsen af hvidvask af penge i fast ejendom (lokalt, nationalt og europæisk), kan samarbejde yderligere, dele viden og erfaringer og skabe løsninger, f.eks. mht. yderligere at forbedre udvekslingen af oplysninger inden for EU og gennemføre undervisning/vejledning for sektoren (og forpligtede parter).

9. Tjenester leveret af regnskabssagkyndige og revisorer, rådgivere og skatterådgivere

Produkt
Tjenester leveret af regnskabssagkyndige, revisorer og skatterådgivere

Sektor
Eksterne regnskabssagkyndige, revisorer og skatterådgivere

Generel beskrivelse af den pågældende sektor og det/den relevante produkt/aktivitet

Regnskabssagkyndige, revisorer og rådgivere arbejder i forskellige stillinger og sektorer, i små og store revisionsfirmaer, små og mellemstore virksomheder, store virksomheder, det offentlige og nonprofitorganisationer, uddannelse osv.

Med hensyn særligt til hvidvask af penge er erhvervet omfattet af national lovgivning om bekæmpelse af hvidvask af penge og af finansiering af terrorisme og af FATF's henstillinger. Erhvervets øvrige kontroller og risikobegrænsende tiltag omfatter:

- screening af reelle ejere som del af kend din kunde-/kundekendskabskravsprocessen.
- anvendelse af nye teknologier som dataanalyse, data og process-mining, kunstig intelligens, screening af transaktioner i realtid, block chain og intelligente kontrakter, hvilket kan bidrage til at bekæmpe risikoen or svig og hvidvask af penge.

Deres meget forskellige faglige aktiviteter kan grupperes således:

- **Regnskabssagkyndige** bistår organisationer med at udarbejde deres økonomiske og ikke-økonomiske data for at måle resultater, herunder de sociale konsekvenser af deres økonomiske aktiviteter. Herved bistår de organisationen med at styre og kontrollere risici og sørge for god ledelse, etik og bæredygtighed. De beretter også om disse målinger til omverdenen, så interessenter kan basere deres beslutninger på organisationens resultater. I nogle tilfælde kan de tilbyde yderligere tjenesteydelser (se rådgivere nedenfor).
- **Revisorer**[94] attesterer oplysninger ved at give en uvildig sagkyndig udtalelse med henblik på at forbedre en organisations information eller dens kontekst. Mht. lovpligtig revision foretager de en lovbestemt kontrol af store og mellemstore virksomheders regnskaber og danner sig en mening om dem. I nogle tilfælde kan de tilbyde yderligere tjenesteydelser (se rådgivere nedenfor).

[94] Yderligere oplysninger om EU's revisionslovgivning: https://ec.europa.eu/info/eu-law-topic/eu-auditing-law_en
Om revision af selskabers regnskaber: https://ec.europa.eu/info/business-economy-euro/company-reporting-and-auditing/auditing-companies-financial-statements_da

- **Rådgivere:** Mange organisationer er afhængige af revisorerhvervets rådgivning, f.eks. om økonomi, skat, virksomheders sociale ansvar, HR, databeskyttelse og cybersikkerhed.

Skatterådgivere udfører en række aktiviteter. Hovedaktiviteterne inden for rådgivning kan grupperes således:

- Overholdelse af skatteregler: udarbejdelse af selvangivelser, socialsikrings- og lønopgørelser, overholdelse af forskellige krav om lovpligtig indberetning, registrering eller offentliggørelse
- Rådgivning: rådgivning om konkrete skatterelaterede spørgsmål, der ikke forekommer rutinemæssigt (f.eks. arv, fusioner eller spin-off, insolvenser, oprettelse af selskab, køb af fast ejendom), skatteundersøgelse, skatteplanlægning/skatteoptimering
- Skattetvister og -klager, rådgivning om disse sager, repræsentation i skattestraffesager.

Skatterådgiveres hovedaktiviteter varierer fra land til land, afhængigt af om erhvervet som skatterådgiver er organiseret på tilsvarende måde som revisor- eller advokatbranchen.

- I syv ud af 22 lande (BE, ES, GR, IE, PT, RO og SK) kan skatterådgivere ikke repræsentere deres klienter for skattedomstole (eller i givet forvaltningsdomstole), da kun advokater kan dette. I Irland og Spanien kan skatterådgivere dog repræsentere klienter for domstolene under en appelsag.
- I 8 lande (FI, IT, LV, LU, NL, PL, CH og UK) kan skatterådgivere repræsentere deres klienter for domstolene for så vidt angår skatteretlige spørgsmål, men ikke i skattestraffesager (i Luxembourg drejer det sig om repræsentation ved revisorer for retten i første instans).
- I seks lande (AT, CZ, DE, HR, RU og UA) kan skatterådgivere også repræsentere deres klienter i skattestraffesager (selvom dette ikke sker i praksis i CZ og HR).
- I otte lande (AT, DE, FI, LV, NL, PL, RU og UA) kan skatterådgivere repræsentere deres klienter for den højeste domstol i skattesager, skønt dette i Østrig og Finland kun gælder den øverste forvaltningsdomstol. I Frankrig er skatterådgivere advokater.

Uanset, om hvervet som skatterådgiver er et selvstændigt erhverv i et land, er der få skatterådgivere, der udelukkende arbejder med skat. Da skat ofte er relateret til andre områder, er det almindeligt, at skatterådgivere også tilbyder tjenesteydelser på disse områder (bogføring, pension, rådgivning, juridisk rådgivning, rådgivning om selskabsret, revision og voldgift).

På EU-niveau har, foruden traktaten om EU's funktionsmåde, en række EU-direktiver betydning for erhvervet som skatterådgiver:
- direktiv 2005/36/EF om anerkendelse af erhvervsmæssige kvalifikationer
- tjenesteydelsesdirektivet (2006/123/EF)
- direktiver om advokaters udveksling af tjenesteydelser (1977/249/EØF) og deres etableringsret (1998/5/EF)
- direktiv 2005/60/EF;
- direktiv 2011/83/EU kommer til at spille en rolle, hvor skatterådgivere har forbrugere som kunder, og
- direktiv 2000/31/EF finder anvendelse på grænseoverskridende skatterådgivning.

Det ændrede revisordirektiv (2014/56/EU) og revisorforordningen (537/2014/EU), som har skullet anvendes fra den 17. juni 2016, og hvorved der indføres skærpede krav til lovpligtig revision af virksomheder af interesse for offentligheden, f.eks. børsnoterede selskaber, kreditinstitutter og forsikringsselskaber. Dette er for at mindske risikoen for overdreven familiær tilknytning mellem revisorer og deres klienter, fremme professionel skepsis og begrænse interessekonflikter. Forordningen fastsætter krav vedrørende udførelsen af ikkerevisionsydelser. Desuden pålægger forordningen de eksterne revisorer en pligt til at indberette en væsentlig overtrædelse af regler eller en væsentlig trussel mod eller væsentlig tvivl om den fortsatte drift af den reviderede virksomhed til tilsynsmyndighederne.

Beskrivelse af risikoscenariet

Lovovertrædere kan bruge eller anmode om tjenester ydet af regnskabssagkyndige, revisorer og skatterådgivere, dog med et moderat niveau af deltagelse fra de professionelle aktørers side, i den hensigt at:

- misbruge klientkonti

- købe fast ejendom

- oprette truster og selskaber/administrere truster og selskaber

- gennemføre visse retssager, oprette og administrere velgørenhedsorganisationer

- sørge for over- eller underfakturering eller afgivelse af urigtige oplysninger om import/eksport af varer

- stille forsikring til rådighed, og/eller

- yde bistand med overholdelse af skatteregler

Eksperter på disse felter kan deltage i systemer til hvidvask af penge ved at bistå med at oprette "uigennemsigtige strukturer", dvs. virksomhedsstrukturer, hvor identiteten af den reelle ejer/de reelle ejere af enheder og arrangementer i den pågældende struktur er skjult ved hjælp af f.eks. stråmænd som direktører. Oprettelsen af de pågældende strukturer, der ofte er oprettet i flere lande, herunder offshore centre, er kompliceret og kræver professionel bistand mht. lovgivning og skat.

Trussel

Finansiering af terrorisme

Vurderingen af truslen om finansiering af terrorisme i relation til ydelser leveret af regnskabssagkyndige og revisorer, rådgivere og skatterådgivere er blevet overvejet sammen med systemer til hvidvask af penge i relation til ydelser fra disse faggrupper med henblik på at skjule midlernes illegale oprindelse (se nedenfor). Det er derfor ikke nødvendigt at vurdere truslen om terrorfinansiering separat.

Konklusion: Vurderingen af truslen om finansiering af terrorisme i relation til ydelser leveret af rådgivere og skatterådgivere anses for meget betydelig (niveau 4). Vurderingen af truslen om finansiering af terrorisme i relation til visse yderligere tjenester leveret af regnskabssagkyndige og revisorer anses for betydelig (niveau 3).

Hvidvask af penge

Vurderingen af truslen om hvidvask af penge i relation til ydelser leveret af regnskabssagkyndige og revisorer, rådgivere og skatterådgivere har visse fællestræk med juridisk rådgivning fra advokater.

Som for alle andre aktiviteter af juridisk karakter er **risikoen for organiserede kriminelle grupperingers infiltration eller ejerskab** en trussel mht. hvidvask af penge for regnskabssagkyndige og revisorer, rådgivere og skatterådgivere. Disse faggrupper kan uforvarende komme til at deltage i hvidvask af penge, men kan også være medskyldige eller forsætligt forsømmelige i forbindelse med udførelsen af deres forpligtelser mht. kundekendskabskrav.

Retshåndhævende myndigheder har bevis for, at organiserede kriminelle grupperinger ofte bruger skatterådgiveres rådgivning og inddrager denne sektor i deres hvidvasksystemer. Skatterådgiveres ydelser anses for at være nyttige ved udformningen af systemer til hvidvask af penge, fordi de er nødvendige til visse typer aktiviteter og/eller fordi specialiseret skatteekspertise og -færdigheder kan være til hjælp ved hvidvask af udbyttet af kriminalitet. Adgang til skatterådgiveres juridiske ydelser er ganske let og kræver ingen særlige kompetencer eller særlig viden. Kriminelle organisationer anvender disse fagfolks færdigheder at til at oprette systemer til hvidvask af penge, så de ikke selv behøver at tilegne sig disse kompetencer. Der er også tegn på, at nogle kriminelle forsøger at samvirke med og bevidst inddrage skatterådgivere i deres systemer til hvidvask af penge.

Fagfolk kan være involveret i hvidvaskprocessen i forskellig grad. De kan konsulteres med hensyn til råd om, hvordan man kan omgå bestemte juridiske regler, og hvordan man kan undgå at udløse faresignaler, som pengeinstitutterne har indført. Eller de kan have en mere proaktiv tilgang ved direkte at støtte eller iscenesætte hvidvaskprocessen. Ofte søger lovovertræderne imidlertid at inddrage skatterådgivere, fordi de tjenester, de tilbyder, er afgørende for en bestemt transaktion, og de tilføjer respektabilitet til transaktionen.

Eksperter på disse områder er blandt de fagfolk, som anvendes mest af organiserede kriminelle grupperinger til at hvidvaske udbytte af kriminalitet pga. de typer af ydelser, de kan tilbyde deres kunder. De kan oprette selskabsstrukturer, konstruere regnskabssystemer, levere bogføringsydelser, udarbejde dokumentation (regnskaber eller referencer, svigagtige indkomster og udgifter), fungere som insolvensbehandlere samt yde almindelig regnskabsrådgivning. Gennem disse ydelser kan nogle regnskabssagkyndige bistå organiserede kriminelle grupperinger med at sløre deres identitet og oprindelsen af de penge, de har med at gøre.

De fleste af disse ydelser bruges til lovlige formål. De kan imidlertid også understøtte en lang række systemer til hvidvask af penge. Disse omfatter svigagtig handel, falske fakturaer, udarbejdelse af urigtige angivelser om indtjening, svigagtig konkurs, skatteunddragelse og andre typer misbrug af regnskaber.

Konklusion: Ydelser leveret af rådgivere og skatterådgivere, revisorer og regnskabssagkyndige anvendes hyppigt i forbindelse med systemer til hvidvask af penge, og de opfattes af organiserede kriminelle grupperinger som en måde, hvorpå de kan kompensere for deres manglende viden. Trusselsniveauet mht. hvidvask af penge i relation til ydelser leveret af rådgivere og skatterådgivere anses for meget betydeligt (niveau 4). Trusselsniveauet mht. hvidvask af penge i relation til visse tjenester leveret af regnskabssagkyndige og revisorer anses for betydeligt (niveau 3).

Sårbarhed

Finansiering af terrorisme

Vurderingen af truslen om finansiering af terrorisme i relation til ydelser leveret af regnskabssagkyndige, revisorer og skatterådgivere er blevet overvejet sammen med systemer til hvidvask af penge i relation til ydelser fra disse faggrupper med henblik på at skjule midlernes illegale oprindelse. Det er derfor ikke nødvendigt at vurdere truslen om terrorfinansiering separat.

Konklusion: På tilsvarende måde som mht. hvidvask af penge anses vurderingen af sårbarheden over for finansiering af terrorisme i relation til ydelser leveret af regnskabssagkyndige, revisorer, rådgivere og skatterådgivere for betydelig (niveau 3).

Hvidvask af penge

Vurderingen af sårbarheden over for hvidvask af penge i relation til ydelser leveret af regnskabssagkyndige og revisorer, rådgivere og skatterådgivere viser følgende:

a) risikoeksponering

Skatterådgivere kan ofte blive indraget i styringen af komplekse transaktioner, der omfatter skatterelateret rådgivning. Disse transaktioner kan eksponere sektoren for højrisikokunder (f.eks. politisk eksponerede personer) eller komplekse juridiske enheder og juridiske arrangementer, hvor identifikationen af den reelle ejer er særligt problematisk. Denne sektor er også i høj grad i stand til at håndtere de skattemæssige aspekter i forbindelse med disse komplicerede juridiske enheder og juridiske arrangementer, da det er deres kerneforretning.

b) risikobevidsthed

Regnskabssagkyndige, revisorer og skatterådgivere skal overholde strenge etiske og faglige regler, og de anser dette for at være en tilstrækkelig beskyttelse mod hvidvask af penge og terrorfinansiering, der forekommer i eller gennem deres sektor. Denne sektor kan imidlertid også blive infiltreret af organiserede kriminelle grupperinger, og nogle sektorielle tilsynsorganer er stadig ikke tilstrækkeligt rustet til at opdage den slags misbrug (dvs. ordentlige testkrav mangler i nogle lande).

Sektoren nyder godt af en stærkt organisatorisk ramme på EU-plan. For eksempel har European Federation for Accountants and Auditors for SMEs (EFAA), der er en paraplyorganisation for nationale organisationer for regnskabssagkyndige og revisorer, 17 medlemmer over hele Europa og repræsenterer over 320.000 regnskabssagkyndige og revisorer samt skatterådgivere. Confédération Fiscale Européenne omfatter 26 nationale organisationer fra 21 europæiske lande og repræsenterer mere end 200.000 skatterådgivere. Accountancy Europe er et andet eksempel. Den er en sammenslutning af 51 faglige organisationer fra 36 lande, som repræsenterer næsten 1 millioner professionelle regnskabssagkyndige, revisorer og rådgivere.

Disse organisationers rolle er at sikre udveksling af oplysninger om nationale love, der er relevante for deres sektor, og at koordinere overholdelse af EU-lovgivningen. De sikrer også, at medlemmerne er opmærksomme på ændringer i EU-lovgivningen, som har indflydelse på for eksempel deres forpligtelser mht. bekæmpelse af hvidvask af penge.

For revisorer har revisorforordningen også oprettet CEAOB [Committee of European Audit Oversight bodies]: Udvalget af europæiske revisionstilsynsmyndigheder. CEAOB er en ramme for samarbejde mellem de nationale tilsynsmyndigheder for revisorer i EU. Dets rolle er at styrke den EU-dækkende revisionskontrol.[95]

En stærk organisation garanterer ikke nødvendigvis en høj kvalitet af samarbejde med de kompetente myndigheder på alle felter.[96] Desuden mener nogle kompetente myndigheder og finansielle efterretningsenheder, at regnskabssagkyndige, revisorer og skatterådgivere stadig ikke i tilstrækkelig grad er klar over de risici, der er forbundet med uigennemsigtige strukturer og de metoder, der anvendes til at tilsløre de reelle ejerforhold. En tovejs informationsstrøm er imidlertid nødvendig for at forbedre situationen, og deling af typetilfælde og oplysninger mellem retshåndhævende myndigheder ville muliggøre en bedre risikovurdering.

c) retsgrundlag og kontroller

Regnskabssagkyndige og revisorer,[97] rådgivere og skatterådgivere har været underlagt EU's krav om bekæmpelse af hvidvask af penge siden 2001. De skal anvende kundekendskabskrav, hvor de deltager, uanset om de handler på deres klients vegne og for dennes regning i forbindelse med en finansiel transaktion eller en transaktion vedrørende fast ejendom, eller ved at yde bistand i forbindelse med planlægningen eller udførelsen af transaktioner for deres klienter vedrørende i) køb og salg af fast ejendom eller virksomheder, ii) forvaltning af klienters penge, værdipapirer eller andre aktiver, iii) åbning eller forvaltning af bank-, opsparings- eller værdipapirkonti, iv) tilvejebringelse af nødvendige bidrag til oprettelse, drift eller ledelse af selskaber og v) oprettelse, drift eller ledelse af truster, selskaber, fonde eller lignende strukturer.

---

[95] https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-reforms-and-their-progress/regulatory-process-financial-services/expert-groups-comitology-and-other-committees/committee-european-auditing-oversight-bodies_en

[96] Art. 12, stk. 2, i revisorforordningen pålægger de eksterne revisorer en pligt til at indberette en væsentlig overtrædelse af regler eller en væsentlig trussel mod eller væsentlig tvivl om den fortsatte drift af den reviderede virksomhed til tilsynsmyndighederne.

[97] Tilsynet med revisorer af virksomheder af interesse for offentligheden ligger ikke i hænderne på professionelle/selvregulerende organer.

Skatterådgivere, rådgivere, regnskabssagkyndige og revisorer er en ganske kompleks og forskelligartet branche. Generelt kan man sige, at sektoren er kendetegnet ved langvarige forretningsforbindelser, der øger de professionelles mulighed for at opdage usædvanlige transaktioner eller adfærd. Men når der søges konkrete råd vedrørende irregulære eller enkeltstående transaktioner, kan de professionelle udføre deres opgaver uden at have fuld forståelse af deres klienters økonomiske situation. Dette har indflydelse på niveauet for deres indberetning af mistænkelige transaktioner, som stadig er temmelig lavt, men bedre end advokaternes. Sektoren forklarer undertiden dette lave indberetningsniveau for mistænkelige transaktioner med, at på dette felt er det ikke den professionelle, der har ansvaret, som behandler eller igangsætter en finansiel transaktion på sin klients vegne. Advarselssignaler er ikke baseret på transaktionen, men på usædvanlige adfærdsmønstre. Noget af regnskabskyndiges og skatterådgiveres arbejde kan omfatte et element af undersøgelse og revision, som kan udgøre nyttige oplysninger til brug for mulige indberetninger om mistænkelige transaktioner.[98]

Da uigennemsigtige strukturer kan oprettes i mange jurisdiktioner, herunder i offshore-centre, kan professionelle udnytte skattemæssige og lovgivningsmæssige forskelle til at sælge deres tjenesteydelser.

Konklusion: Regnskabssagkyndige og revisorer, rådgivere og skatterådgivere er velorganiserede. Der er imidlertid svagheder i den måde de gennemfører kontrollet og styrer risici. Niveauet af sårbarhed over for hvidvask af penge i relation til ydelser leveret af regnskabssagkyndige, revisorer rådgivere og skatterådgivere anses derfor for betydeligt (niveau 3).

Risikobegrænsende foranstaltninger:

1) Kommissionen:

Direktiv (EU) 2015/849 som ændret ved direktiv (EU) 2018/843 har præciseret sit anvendelsesområde for dækningen af revisorer, eksterne revisorer og skatterådgivere, idet det udvides til at omfatte enhver anden person, der yder materiel hjælp, bistand eller rådgivning om skatteanliggender som vigtigste forretnings- eller erhvervsmæssige virksomhed.

For så vidt angår reelle ejerforhold skal selskaber og truster være i besiddelse af oplysninger om, hvem deres reelle ejer er. Desuden er reelle ejere nu forpligtet til at forsyne selskaberne med de oplysninger, de har brug for. Selskaber og truster skal give disse oplysninger til deres revisorer.

Effektive, forholdsmæssige og afskrækkende foranstaltninger eller sanktioner finder anvendelse i tilfælde af manglende overholdelse af disse regler.

[98] Se forrige note.

Direktiv 2018/822/EU får virkning fra 2020, og i medfør af direktivet skal mellemled indgive oplysninger om indberetningspligtige grænseoverskridende skatteordninger[99] til deres nationale myndigheder.

Inden for disse rammer bør Kommissionen fortsætte med at foretage:

- gennemførelseskontrol vedrørende overholdelsen af gennemsigtighedskravene til oplysninger om reelle ejerforhold (registrering) — medlemsstaterne skal underrette om tekniske elementer i deres nationale ordning til bekæmpelse af hvidvask af penge og af finansiering af terrorisme og herved sikre gennemsigtighed mht. oplysninger om reelle ejerforhold, og
- gennemførelseskontrol med overholdelsen af identifikationskrav for information om reelle ejerforhold (definition af den reelle ejer) — medlemsstaterne skal underrette om tekniske elementer i deres nationale ordning til bekæmpelse af hvidvask af penge og af finansiering af terrorisme vedrørende definitionen af reel ejer.

2) kompetente myndigheder:

- Medlemsstaterne bør sikre, at de kompetente myndigheder/selvregulerende organer (når de er tilsynsansvarlige), der kontrollerer eksterne revisorer, eksterne regnskabssagkyndige og skatterådgivere, oplyser om de kontrolforanstaltninger, de har indført for at sikre, at sektoren præcist gennemfører sine forpligtelser vedrørende bekæmpelse af hvidvask af penge og af finansiering af terrorisme. Når de modtager rapporter om mistænkelige transaktioner, skal tilsynsmyndighederne årligt afgive rapport om antallet af rapporter indsendt til de finansielle efterretningsenheder.
- Inspektioner på stedet svarende til populationen af eksterne revisorer, eksterne regnskabssagkyndige og skatterådgivere på medlemsstatens territorium.

3) medlemsstaterne:

- Medlemsstaterne bør sørge for vejledning om risikofaktorer i forbindelse med transaktioner, der involverer eksterne revisorer og skatterådgivere.

Fremme en bedre forståelse blandt eksterne revisorer, eksterne regnskabssagkyndige og skatterådgivere for, hvordan fortrolighedsforholdet mellem advokat og klient skal fortolkes og anvendes. Medlemsstaterne bør udstede retningslinjer for gennemførelsen af fortrolighedsforholdet mellem advokat og klient — hvordan man skal opdele juridiske tjenesteydelser, der er omfattet af selve kernen af fortrolighedsforholdet mellem advokat og klient og andre juridiske tjenesteydelser, der ikke er omfattet af fortrolighedsforholdet mellem advokat og klient, når de leveres til den samme klient.

[99] https://ec.europa.eu/taxation_customs/business/tax-cooperation-control/administrative-cooperation/enhanced-administrative-cooperation-field-direct-taxation_en

10. Juridiske tjenester leveret af notarer og andre uafhængige retlige aktører

Produkt
Juridiske tjenester leveret af retlige aktører

Sektor
Uafhængige retlige aktører, advokater, notarer

Beskrivelse af risikoscenariet

Lovovertrædere kan bruge eller bestille ydelser hos en retlig aktør (f.eks. en advokat, notar eller anden uafhængig retlige aktør) mht.:

- misbrug af klientkonti

- køb af fast ejendom

- oprettelse af truster og selskaber/administration af truster og selskaber, eller

- gennemførelse af visse retstvister.

De kan deltage i systemer til hvidvask af penge ved at bistå med at oprette "uigennemsigtige strukturer", dvs. virksomhedsstrukturer, hvor identiteten af den reelle ejer/de reelle ejere af enheder og arrangementer i den pågældende struktur er skjult ved hjælp af f.eks. stråmænd som direktører. Oprettelsen af de pågældende strukturer, der ofte er oprettet i flere lande, herunder offshore centre, er kompliceret og kræver fagfolks bistand mht. lovgivning og skat.

Trussel

Finansiering af terrorisme

Vurderingen af truslen om finansiering af terrorisme i relation til juridiske ydelser leveret af retlige aktører er blevet overvejet sammen med systemer til hvidvask af penge i relation til ydelser leveret af disse faggrupper med henblik på at skjule midlernes illegale oprindelse. Det er derfor ikke nødvendigt at vurdere truslen om terrorfinansiering separat.

Konklusion: Vurderingen af truslen om finansiering af terrorisme i relation til ydelser leveret af retlige aktører anses derfor for meget betydelig (niveau 4).

Hvidvask af penge

Vurderingen af truslen om hvidvask af penge i relation til juridiske tjenesteydelser leveret af retlige aktører har visse fællestræk med juridiske tjenesteydelser leveret af regnskabssagkyndige, revisorer og skatterådgivere.

- som for alle andre aktiviteter af juridisk karakter udgør risikoen for organiserede kriminelle grupperingers infiltration eller ejerskab en trussel mht. hvidvask af penge for retlige aktører. Disse faggrupper kan uforvarende komme til at deltage i hvidvask af penge,

men kan også være medskyldige eller forsætligt forsømmelige i forbindelse med udførelsen af deres forpligtelser mht. kundekendskabskrav.

- Retshåndhævende myndigheder rapporterer, at organiserede kriminelle grupperinger ofte bruger retlige aktører og inddrager denne sektor i deres hvidvasksystemer. Retlige aktørers ydelser anses for at være nyttige ved udformningen af systemer til hvidvask af penge, da de er nødvendige til visse typer aktiviteter og/eller fordi specialiseret juridiske og notarielle færdigheder kan være til hjælp ved hvidvask af udbyttet af kriminalitet. Advokater er særligt udsatte for at blive misbrugt af kriminelle, fordi at antage en advokat tilfører respektabilitet og et skær af legitimitet til en aktivitet, også selvom den tjenesteydelse, der leveres, kan hjælpe kriminelle med at hvidvaske penge.

Retlige aktører kan understøtte hvidvask af penge ved at anvende de værktøjer, de allerede har til rådighed (f.eks. klientkonti) eller ved at hjælpe deres kunder med at oprette og administrere konti, truster og selskaber til at skjule og/eller legitimere deres midlers oprindelse.

Der er mange måder, hvorpå klientkonti kan bruges til hvidvask af penge, hvoraf de mest almindelige er:

- ved at udføre finansielle transaktioner på vegne af en klient, herunder offshore banking
- ved at acceptere store kontante indskud på klientens konto efterfulgt af kontanthævninger eller udstedelse af checks
- ved at købe fast ejendom, selskaber eller ejendomme på vegne af en klient, og
- i nogle tilfælde ved at bruge af den retlige aktørs egen personlige konto til at modtage og overføre penge.

Advokater kan hjælpe ved at oprette og administrere skuffeselskaber og lovlige selskaber ved at udarbejde kontrakter og oprette virksomhedskonti. Offshore-selskaber og truster er særligt attraktive for organiserede kriminelle grupperinger pga. deres strenge regler og praksis for bankhemmelighed og juridisk og administrativ hemmeligholdelse, og den anonymitet, som de giver. Foruden juridisk rådgivning og papirarbejde, som de tilbyder, kan retlige aktører også deltage aktivt i administrationen af et selskab og dets aktiver. De kan f.eks. repræsentere deres klienter i forbindelse med køb og salg af et selskab og er ansvarlige for at afhænde finansielle aktiver ved beordre pengeoverførsler, købe andre selskaber eller investere i fast ejendom. Tilsvarende kan advokater indtage en stilling i selskabet (f.eks. ejer, leder og administrator) og på den måde yderligere distancere deres klient fra kriminelle aktiver.

I de fleste EU-lande sørger advokater for den komplette dokumentation ved stiftelse og registrering af selskaber, overførsel af adkomster, åbning af konti i pengeinstitutter, fakturaer og internationale handelsdokumenter. Karakteren af denne dokumentation er en udfordring for undersøgelser på grund af den tekniske karakter og den fortrolighed, det medfører.

Kriminelle organisationer anser ikke adgang til retlige aktører for at være særlig kompliceret. For dem betyder det at bruge juridiske aktørers færdigheder, at de ikke var behov for selv at udvikle disse kompetencer. For at hvidvaske penge har nogle organiserede kriminelle grupperinger infiltreret advokatvirksomheder, urigtigt udgivet sig for at være advokater eller stjålet advokaters identitet.

Konklusion: Ifølge oplysninger fra retshåndhævende myndigheder benyttes retlige aktører hyppigt i forbindelse med hvidvask af penge. At bruge retlige aktørers tjenester gøre, at kriminelle organisationer ikke behøver at udvikle deres egen viden og ekspertise og "blåstempler" deres aktiviteter Trusselsniveauet for hvidvask af penge i relation til retlige aktører (advokater, notarer og uafhængige retlige aktører) anses derfor for meget betydeligt (niveau 4).

Sårbarhed

Finansiering af terrorisme

Vurderingen af sårbarhed over for terrorfinansiering i relation til juridiske tjenesteydelser leveret af retlige aktører er blevet overvejet sammen med systemer til hvidvask af penge i relation til tjenesteydelser fra disse professionelle med det formål at skjule midlernes illegale oprindelse. Det er derfor ikke nødvendigt at vurdere truslen om terrorfinansiering separat.

Konklusion: Vurderingen af truslen om finansiering af terrorisme i relation til ydelser leveret af retlige aktører anses for betydelig (niveau 3).

Hvidvask af penge

Vurderingen af sårbarhed over for hvidvask af penge i relation til juridisk rådgivning ydet af retlige aktører viser følgende:

a) risikoeksponering

Risikoeksponeringen kommer af karakteren af visse ydelser/aktiviteter, der leveres af retlige aktører (som kræver overholdelse af regler om bekæmpelse af hvidvask af penge).

Risikoeksponeringen for denne sektor er præget af, at den ganske ofte kan være involveret i styringen af komplekse juridiske situationer. Især det forhold, at juridiske tjenesteydelser ikke nødvendigvis indebærer håndtering af egentlige finansielle transaktioner, betyder, at retlige aktører skal udløse andre typer faresignaler, som er vanskeligere at definere (f.eks. en kundes adfærd).

b) risikobevidsthed

Sektoren er ikke homogent organiseret (området for retlige aktører varierer fra den ene medlemsstat til den anden - det burde ikke være en risiko i sig selv), selvom nogle EU-organisationer spiller en vigtig rolle i forbindelse med orientering om, hvordan man anvender kravene om bekæmpelse af hvidvask af penge og finansiering af terrorisme, ved at sørge for vejledning og at lette udvekslingen af oplysninger. De bidrager især med at opstille en liste over advarselssignaler, som folk, der arbejder inden for sektoren, kan bruge, f.eks. klientens adfærd eller identitet, sløringsteknikker (brug af mellemled, undgåelse af personlig kontakt), beløbsstørrelse (uforholdsmæssigt mange private midler) m.m. Branchen synes allerede synes at være opmærksom på nogle risici, f.eks. at en klient giver instrukser om transaktioner på afstand eller uden legitim grund, eller hvis der er

mange skift af juridisk rådgiver inden for en kort tidsramme eller brug af adskillige juridiske rådgivere uden god grund.

Generelt er niveauet for indberetning af mistænkelige transaktioner er meget lavt for så vidt angår retlige aktører (selvom rapporter om mistænkelige transaktioner fra retlige aktører ikke kan sammenlignes med juridiske rapporter fra for eksempel finansieringsinstitutter).

I nogle lande er selvregulerende organer reguleret af staten og er uafhængige, og de fungerer effektivt som mellemled mellem de finansielle myndigheder og de pågældende faggrupper. De organiserer, undersøger og vurderer de faktiske forhold, hvilket gør det lettere for de finansielle myndigheder at sondre mellem hvidvask af penge og normaltilfælde.

c) retsgrundlag og kontroller

Notarer, advokater og andre uafhængige retlige aktører har været omfattet af EU's krav om bekæmpelse af hvidvask af penge siden 2001. De skal anvende kundekendskabskrav, hvor de deltager, uanset om de handler på deres klients vegne og for dennes regning i forbindelse med en finansiel transaktion eller en transaktion vedrørende fast ejendom, eller ved at yde bistand i forbindelse med planlægningen eller udførelsen af transaktioner for deres klienter vedrørende: i) køb og salg af fast ejendom eller virksomheder, ii) forvaltning af klienters penge, værdipapirer eller andre aktiver, iii) åbning eller forvaltning af bank-, opsparings- eller værdipapirkonti, iv) tilvejebringelse af nødvendige bidrag til oprettelse, drift eller ledelse af selskaber og v) oprettelse, drift eller ledelse af truster, selskaber, fonde eller lignende strukturer.

Retlige aktører er organiseret og reguleret på forskellig måde afhængig af de pågældende medlemsstater. Juridiske tjenesteydelser bliver ligeledes ofte udført ansigt til ansigt, hvilket udgør en særlig udfordring mht. beskyttelse af medarbejdere Der er også forskelle mellem de forskellige faggrupper, da notarerne som faggruppe også virker i offentlig tjeneste og i nogle medlemsstater har status af indehavere af offentlige embeder.

Under alle omstændigheder bør anonymiteten af den retlige aktør, der rapporterer mistanken, beskyttes i fuldt omfang. I nogle medlemsstater er der en risiko for, at navnet på den notar, der er ophav til erklæringen, ville kunne komme til at figurere i rapporten om den mistænkelige transaktion, især hvis den følges op af en retssag. For at undgå dette bør der udvikles regler med henblik på at hindre enhver videregivelse af oplysninger om oprindelsen til rapporten om den mistænkelige transaktion.

Fortrolighedsforholdet mellem advokat og klient (professionel tavshedspligt) er et anerkendt princip på EU-niveau, som er udtryk for en hårfin balance i lyset af Den Europæiske Unions Domstols retspraksis om retten til en retfærdig rettergang (C-305/05), der på sin side afspejler principperne i Den Europæiske Menneskerettighedsdomstol samt i chartret (f.eks. artikel 47). Der er tilfælde, hvor disse faggrupper udøve aktiviteter, der er omfattet af reglerne om fortrolighedsforholdet mellem advokat og klient (dvs. at de vurderer den pågældende klients retsstilling eller forsvarer eller repræsenterer deres klienter i retssager) og samtidig udøver aktiviteter, der ikke er omfattet af fortrolighedsforholdet mellem advokat og klient, f.eks. at yde juridisk rådgivning i

forbindelse med oprettelse, drift eller ledelse af selskaber. Området for fortrolighed, fortrolighedsforholdet mellem advokat og klient og professionel tavshedspligt varierer fra land til land og det praktiske grundlag for at tilsidesætte denne beskyttelse bør afklares.

Konklusion: Sektorens risikobevidsthed synes stadig at være begrænset. På trods af den eksisterende lovgivning sikrer tilsynet med sektoren ikke altid en ordentlig overvågning af mulige hvidvaskmisbrug. Sårbarhedsniveauet over for hvidvask af penge i relation til juridisk rådgivning leveret af retlige aktører anses derfor for betydeligt (niveau 3).

Risikobegrænsende foranstaltninger:

1) Kommissionen:

- I forbindelse med direktiv 2015/849 (EU) som ændret ved direktiv 2018/843 (EU):
  - Gennemførelseskontrol vedrørende overholdelsen af gennemsigtighedskravene til oplysninger om reelle ejerforhold (registrering): Medlemsstaterne skal underrette om tekniske elementer i deres nationale ordning til bekæmpelse af hvidvask af penge og af finansiering af terrorisme og herved sikre gennemsigtighed mht. oplysninger om reelle ejerforhold.
  - Gennemførelseskontrol med overholdelsen af identifikationskrav for information om reelle ejerforhold (definition af den reelle ejer): Medlemsstaterne skal underrette om tekniske elementer i deres nationale ordning til bekæmpelse af hvidvask af penge og af finansiering af terrorisme vedrørende definitionen af den reelle ejer.
  - For bedre at formidle EU's lovgivning om bekæmpelse af hvidvask af penge og medvirke til at sikre en effektiv og ensartet anvendelse af EU-retten, bør Kommissionen støtte uddannelsesaktiviteter for den juridiske profession (advokater og notarer).
  - At afholde høringsrunder/diskussioner med interessenter for at bidrage til at holde Kommissionen underrettet om gennemførelsen af direktiverne om hvidvask af penge og finansiering af terrorisme i EU og at øge kendskabet til og at udveksle bedste praksis vedrørende forskellige aspekter af de retlige aktørerers overholdelse af reglerne om bekæmpelse af hvidvask af penge.
- Direktiv 2018/822/EU får virkning fra 2020, og i medfør af direktivet skal mellemled indgive oplysninger om indberetningspligtige grænseoverskridende skatteordninger[100] til deres nationale myndigheder.

[100] https://ec.europa.eu/taxation_customs/business/tax-cooperation-control/administrative-cooperation/enhanced-administrative-cooperation-field-direct-taxation_en

2) kompetente myndigheder:

- Medlemsstaterne bør sikre, at de kompetente myndigheder/selvregulerende organer, der fører tilsyn med uafhængige retlige aktører, advokater og notarer udarbejder en årsrapport om tilsynsforanstaltninger til sikring af, at sektoren præcist gennemfører sine forpligtelser mht. bekæmpelse af hvidvask af penge og af finansiering af terrorisme. Når selvregulerende organer de modtager rapporter om mistænkelige transaktioner, skal de årligt afgive rapport om antallet af rapporter indsendt til de finansielle efterretningsenheder.

- Inspektioner på stedet svarende til populationen af uafhængige retlige aktører, advokater og notarer på medlemsstatens territorium.

3) medlemsstaterne:

- Medlemsstaterne bør sørge for vejledning om risikofaktorer i forbindelse med transaktioner, der involverer uafhængige retlige aktører, advokater og notarer.

Selvregulerende organer bør gøre en indsats for at øge antallet af tematiske inspektioner og rapportering. De bør også arrangere undervisning for at skabe en bedre forståelse af risiciene og forpligtelserne til at overholde reglerne om bekæmpelse af hvidvask af penge og af finansiering af terrorisme.

1. Generel beskrivelse af spilsektoren

Generel beskrivelse af den pågældende sektor og det/den relevante produkt/aktivitet

Ifølge EU's nuværende regler om bekæmpelse af hvidvask af penge (4. hvidvaskdirektiv) er spiltjenester defineret som tjenester, som indebærer, at der gøres en indsats med penge i hasardspil, herunder spil med et element af færdigheder, f.eks. lotteri, kasinospil, pokerspil og væddemål, som udbydes på en fysisk lokalitet eller ved hjælp af forskellige midler på afstand, ved hjælp af elektroniske midler eller anden kommunikationsfremmende teknologi og efter individuel anmodning fra en tjenestemodtager

Udtrykket "spil" refererer således til en række forskellige tjenester og distributionskanaler. I forbindelse med denne risikovurdering er spilsektoren opdelt i landbaserede (offline) og onlinespil og den landbaserede sektor er yderligere opdelt i afsnit om væddemål, bingo, kasinoer, spilleautomater, lotterier og poker. En yderligere opdeling i forskellige onlinespilprodukter blev ikke anset for nødvendig, da de relevante risici, trusler og sårbarheder primært synes at være nyttet til karakteren af online transaktioner snarere end til konkrete former for onlinespil.

Alle udbydere af spiltjenester er forpligtede enheder efter fjerde hvidvaskdirektiv. Medlemsstaterne har pligt til at regulere og overvåge dem i forhold til finansiering af terrorisme og hvidvask af penge og give deres kompetente myndigheder udvidede tilsynsbeføjelser til at overvåge dem og sikre, at de personer, som i praksis leder sådanne enheders drift, samt sådanne enheders reelle ejere besidder den fornødne egnethed og hæderlighed.

Udbydere af spiltjenester skal gennemføre kundekendskabsprocedurer i forbindelse med indkasseringen af gevinster, ved indsatsen eller begge dele, når de udfører transaktioner på mindst 2 000 EUR, hvad enten transaktionen gennemføres på én gang eller som flere operationer, der ser ud til at være indbyrdes forbundne. Mens medlemsstaterne har mulighed for at undtage visse spiltjenester fra nogle af eller alle kravene ifølge det fjerde hvidvaskdirektiv efter en passende risikovurdering, er dette ikke tilfældet for kasinoer. En medlemsstats brug af en undtagelse bør kun overvejes under meget begrænsede og behørigt begrundede omstændigheder, og når risiciene for hvidvask af penge eller finansiering af terrorisme er lave, og disse undtagelser bør indberettes til Kommissionen. Det fjerde hvidvaskdirektiv skulle være gennemført i national ret senest den 26. juni 2017, hvorfor virkningerne af de ændringer, der ved direktivet blev indført mht. spilsektoren, er vanskelige at vurdere på dette tidlige tidspunkt.

Der findes ingen sektorspecifik EU-lovgivning om spil. Det står medlemsstaterne frit for at fastsætte målene for deres politik og fastsætte beskyttelsesniveauet for forbrugerne og forebygge kriminalitet, herunder hvidvask af penge. Dog finder bestemmelserne i EU-traktaterne anvendelse. Den Europæiske Unions Domstol har givet generel vejledning for fortolkningen af de grundlæggende friheder i det indre marked på spilområdet og herved

taget hensyn til områdets særlige karakter. Medlemsstaterne kan indskrænke eller begrænse grænseoverskridende levering af spiltjenester for at beskytte befolkningen, men de er forpligtet til at godtgøre , at de pågældende foranstaltninger er egnede og nødvendige, og at de gennemføres på en konsekvent og systematisk måde.

Spilsektoren i EU er derfor meget forskelligartet, lige fra monopolordninger (der drives af en statskontrolleret offentlig operatør eller af en privat virksomhed på grundlag af en eneret) til licenssystemer eller en blanding af begge dele. Som reaktion på samfundsmæssige, teknologiske og lovgivningsmæssige udfordringer og udviklingstendenser har et betydeligt antal medlemsstater revideret eller er i færd med at revidere deres spillovgivning. Disse revisioner sker under hensyn til nye former for spiltjenester, som har medført en stigning i spiltjenester, der udbydes af operatører, som godkendt i en EU-medlemsstat, samt grænseoverskridende tilbud, der ikke er tilladt ifølge nationale regler i den modtagende medlemsstat.

Spilsektoren er præget af hurtig økonomisk vækst og teknologisk udvikling. For eksempel blev indtægterne fra onlinespil i EU anslået til omkring 16,5 mia. EUR i 2015, og de forventes at stige til ca. 25 mia. EUR i 2020. Indtægterne fra det offline/landbaserede spilmarked forventes ligeledes at vokse fra omkring.77,5 mia. EUR i 2015 til omkring 82-84 mia. EUR i 2020.

Gennem ikke-lovgivningsmæssige foranstaltninger som beskrevet i meddelelsen fra 2012 "Mod et samlet europæisk regelsæt for onlinespil" (COM(2012) 596 final) har Kommissionen tilskyndet medlemsstaterne til at fastsætte et højt niveau for beskyttelse af forbrugerne, navnlig i lyset af de risici, der er forbundet med spil, og som omfatter udvikling af ludomani og andre negative personlige og sociale konsekvenser. Især i en henstilling om principper for beskyttelse af forbrugere og spillere i forbindelse med onlinespiltjenester og for at forhindre mindreåriges spil online (2014/478/EU) har Kommissionen præsenteret forskellige former for praksis med henblik på at begrænse social skade, hvoraf nogle kan være relevante for bekæmpelse af hvidvask af penge, f.eks. registrerings- og kontrolprocesser.

Desuden er effektivt tilsyn nødvendigt for på hensigtsmæssig måde at opfylde målsætninger af almen interesse. Medlemsstaterne bør udpege kompetente myndigheder og fastlægge klare retningslinjer for operatørerne, herunder om hvidvask af penge. Kommissionen støtter også samarbejdet mellem de nationale tilsynsmyndigheder inden for rammerne af den administrative samarbejdsaftale vedrørende onlinespiltjenester (underskrevet af de fleste medlemsstater i Det Europæiske Økonomiske Samarbejdsområde i 2015).

At kontrollere det stigende antal såkaldte uautoriserede spiltilbud og kanalisere dem ind i den godkendte, regulerede spilsektor indbefatter nogle af de største og mest krævende opgaver for myndighederne. Det anslås, at millioner af forbrugere i EU spiller på uautoriserede onlinespil-websteder. Derfor er det nødvendigt at skabe øget bevidsthed om de risici, der er forbundet med uregulerede spil-websteder, f.eks. svig, som er uden nogen form for kontrol på EU-niveau. Omfanget af dette uautoriserede spil, der normalt foregår online, varierer meget fra medlemsstat til medlemsstat afhængigt af, hvor godt det autoriserede marked fungerer.

Kontrol af det uautoriserede marked og de dermed forbundne risici ligger uden for denne rapports område ud for den antagelse, at det ikke er muligt direkte at hvidvaske penge

gennem en ulovlig aktivitet (gevinsterne ville stadig være ulovlige). Men kontrolorganer og forpligtede enheder bør være opmærksomme på onlineteknikker, som kan gøre det muligt at skjule brugeres og pengekilders sande identitet og lader transaktionerne fremtræde som lovlige og på den måde muliggør, at pengene kan bruges i fremtidige transaktioner på lovlige markeder.

2. Væddemål

Produkt
Spil (landbaseret/offline)

Sektor
Spilsektoren

Generel beskrivelse af den pågældende sektor og det/den relevante produkt/aktivitet

Offline eller landbaserede væddemål (herunder heste- og hundevæddeløb, event-væddemål) udbudt på særlige, godkendte salgssteder af autoriserede forhandlere (der modtager en provision af hver indsats, men også tilbyder andre tjenester) eller på steder, hvor sportsbegivenheder finder sted (ofte heste- eller hundevæddeløbsbaner). Størrelsen af præmien kan enten afhænge af de samlede forudbetalte indsatser (dvs. de såkaldte "totalisatorspil", *pari mutuel* eller "poolspil") eller de odds, som er aftalt mellem bookmakeren og spilleren (dvs. *pari à la cote* eller "fixed-odds betting"). En medlemsstat kan have et fast antal aktører (herunder én enkelt monopoludbyder) eller et ubegrænset antal operatører, så længe de opfylder visse kriterier. Der kan også fastsættes et minimum/maksimum for antallet af spilbutikker pr. licenseret udbyder.

Beskrivelse af risikoscenariet

Der er identificeret tre grundscenarier:

1) en lovovertræder gør en indsats og indkasserer gevinsterne (konvertering).

2) en lovovertræder deponere kontanter på sin spilkonto og hæver dem efter et stykke tid uden at spille for dem (skjul).

3) en lovovertræder placerer penge på en spilkonto ét sted og en medgerningsmand hæver midlerne et andet sted (skjul, sløring og overførsel).

En lovovertræder kan øge sine chancer for at vinde ved at placere indsatser på en serie af events, som vil give gunstigere akkumulerede odds eller reducere risikoen for tab ved at gardere væddemålene (væddemål på begge mulige udfald af samme begivenhed).

En lovovertræder kan også fjerne enhver usikkerhed helt igennem ved at henvende sig en vinder og købe gevinstkuponen.

Trussel

Finansiering af terrorisme

Vurderingen af truslen om terrorfinansiering i relation til væddemålsaktiviteter er ikke blevet anset for at være relevant. I denne henseende er truslen om terrorfinansiering ikke en del af vurderingen.

Konklusion: ikke relevant

Hvidvask af penge

Vurderingen af truslen om hvidvask af penge i relation til væddemålsaktiviteter viser følgende:

- som det er tilfældet for alle andre spilaktiviteter, er en af de trusler, som hvidvask af penge udgør for væddemålsaktiviteter, **risikoen for organiserede kriminelle grupperingers infiltration eller ejerskab**.

Denne trussel kan variere afhængigt af, hvilken type organisation, der er står for væddemålene. For så vidt angår nationale monopoler på sportsvæddemål er risikoen infiltration af væddemålsoperatørens ejerkreds så godt som ikke eksisterende. Det er dog muligt, at individuelle detailforhandlere, som væddemålsoperatørerne bruger til at sælge deres spiltjenester til kunderne kunne blive infiltreret.

Organiserede kriminelle organisationers infiltration i væddemålsaktiviteter kræver moderate niveauer af planlægning eller teknisk ekspertise og beror primært på mekanismer, der muliggør, at den reelle ejers identitet forbliver skjult, f.eks. registrering af aktiver i tredjeparters navne (stråmænd).

- en anden gennemgående trussel er **matchfixing**. Undersøgelser har vist, at kriminelle grupperinger bruger væddemål til at profitere af matchfixing af sportskonkurrencer i EU. Sportsagenter og mellemmænd korrumperer eller intimiderer spillere og/eller dommere til at garantere det resultat, de ønsker i en kamp, mens andre agenter placerer store pengesummer som online og offline indsatser uden for EU. I sådanne tilfælde kræver matchfixing kontakter (og pengeoverførsler) mellem deltagere i væddemålet, spillere, hold-officials og/eller dommere. En beslægtet trussel er væddemål på fiktive kampe eller arrangementer, selvom dette dog mest er forbundet med onlinespil.

- køb af **vinderkuponer** for at sikre gevinster kan udgøre en anden af kriminelle grupperingers intention om at hvidvaske penge.

<u>Konklusion</u>: Retshåndhævende myndigheder har konstateret flere metoder eller kanaler, der kan bruges af organiserede kriminelle grupperinger, når de giver sig i lag med væddemålsaktiviteter. Ud over den horisontale trussel, som risikoen for infiltration og ejerskab udgør, er matchfixing det andet vigtige aspekt. For organiserede kriminelle grupperinger er det kun nødvendigt med moderate niveauer af planlægning, viden og ekspertise som grundlag for at bruge disse metoder, og det opfattes som en attraktiv, sikker og økonomisk realistisk mulighed.

I denne henseende anses truslen fra hvidvask af penge i relation til væddemålsaktiviteter som <u>betydelig</u> (niveau 3).

Sårbarhed

Finansiering af terrorisme

Vurderingen af sårbarheden over for terrorfinansiering i relation til væddemålsaktiviteter er ikke blevet anset for at være relevant. I denne henseende er truslen om terrorfinansiering ikke en del af vurderingen.

<u>Konklusion</u>: ikke relevant

Vurderingen af sårbarheden over for hvidvask af penge i relation til væddemål viser følgende:

a) risikoeksponering:

Væddemålsaktiviteter er præget af betydelige mængder hurtige og anonyme transaktioner, ofte kontantbaseret. Bugen af kontanter har været faldende pga. alternative væddemålsmetoder, men udgør fortsat mere end 50% af omsætningen i nogle lande. Mange deltagere i væddemål bruger i det væsentlige kontanter af hensyn til fortrolighed eller af hensyn til omdømme.

Ifølge brancheeksperter omfatter de mulige faresignaler:

- væddemål med store indsatser til ekstremt korte odds, der sandsynligvis vil sikre en gevinst.
- kunder, der regelmæssigt anmoder om kopier af vindende væddemål eller kvitteringer for vinderkuponer.
- kunder, der betaler kontant og regelmæssigt anmoder om, at gevinster bliver udbetalt via check eller med betalingskort.
- kunder, der regelmæssigt anmoder om kvitteringer, når de indkasserer totalisatorgevinster.

b) risikobevidsthed:

- ifølge de finansielle efterretningsenheder er væddemålssektoren ikke tilstrækkeligt bevidst om risiciene, som det fremgår af det lave antal indberetninger om mistænkelige transaktioner samt deres ringe kvalitet.

- sårbarheden over for hvidvask er markant forøget på grund af anvendelsen af distributionsnet (kiosker, detailhandlere, salgssteder), som ikke nødvendigvis er omfattet af krav om bekæmpelse af hvidvask af penge og af finansiering af terrorisme. Identifikation af kunden påhviler de enkelte detailforhandlere, der arbejder for en vædddemålsoperatør, og de er måske ikke altid i stand til at opdage mistænkelige transaktioner (f.eks. kumulative indsatser, opdeling af høje indsatser eller usædvanlige indsatser), afhængigt af den type forhold, der er mellem operatører og forhandlere. Antallet af rapporter om mistænkelige transaktioner er ujævn, og en del af sektoren er stadig ikke bevidst om risiciene og/eller hvilke typer transaktioner, der skal indberettes (ingen konsistent indberetningspligt).

- ifølge repræsentanter for væddemålssektoren har de finansielle efterretningsenheder og andre kompetente myndigheder den forkerte opfattelse af og manglende forståelse for de risikofaktorer, der er forbundet med væddemål. Det lader til, at finansielle efterretningsenheder allerede har forventninger til den type mistanker, en spiloperator bør rapportere (finansielle efterretningsenheder forventer mistænkelige tilfælde af matchfixing, mens operatøren er tilbøjelig til at rapportere irregulære beløb i transaktionen). Væddemålsoperatører lider under manglende tilbagemeldinger fra de finansielle efterretningsenheder vedrørende rapporterne om mistænkelige transaktioner.

Derudover har væddemålsoperatører udarbejdet kundekendskabskrav, der kan mindske risikoen for hvidvask af penge. Nogle operatører kræver systematisk identifikation af vindere (over et vist beløb), f.eks. med fokus på den reelle ejer. De kunne også tilbyde forskellige metoder til udbetaling af gevinster for at begrænse brugen af kontanter og indføre "spillerkort"[101] for at øge operatørens viden om sine kunder.

c) retsgrundlag og kontroller:

Væddemålsaktiviteter har været omfattet af EU's regler om bekæmpelse af hvidvask af penge siden gennemførelsen af fjerde hvidvaskdirektiv. Men på grund af direktivets principper om mindsteharmonisering kan der stadig være forskelle fra medlemsstat til medlemsstat med hensyn til regulering, tilsyn med sektoren og håndhævelse af reglerne om bekæmpelse af hvidvask af penge og af finansiering af terrorisme.

Nogle medlemsstater har indført lovgivning om hvidvaskaspekterne af væddemål og/eller specifikke krav i licensaftaler. I disse tilfælde er de pågældende regler ofte strenge med hensyn til at udstede en tilladelse (fornøden egnethed og hæderlighed med hensyn til kontrol for bekæmpelse af hvidvask af penge hos nøglepersoner) og at opfylde løbende indberetningsforpligtelser. Disse forpligtelser skal opfyldes, når som helst der er betænkeligheder i forhold til kunden, f.eks. at vide, om satsnings- og tabsniveauer giver grund til bekymring vedrørende bekæmpelse af hvidvask af penge og af finansiering af terrorisme, eller om kundens spillevaner er overensstemmende med dennes levefod. Det indebærer, at en effektiv intern rapporteringsprocedure er påkrævet, og både ledelse og medarbejdere skal have en god viden om bekæmpelse af hvidvask af penge. I denne henseende kræver nogle nationale lovgivninger, at væddemålssektoren foretager en risikovurdering, der viser, at passende kontrolforanstaltninger og procedurer er til stede.

Men de kompetente myndigheder er stadig usikre på, hvordan man kan gennemføre kontroller, navnlig overvågning af indsatser i realtid for at afsløre hvidvask og eventuelt suspendere indsatser i tilfælde af mistanke. I betragtning af væddemålaktiviteternes karakter (hvilket inkluderer store volumener eller undertiden sidste-øjebliks-indsatser) er det klart, at indførelsen af en præcis virkende ordning for kundekendskabskrav er en udfordring, der skal tages fat på. Brugen af detailforhandlere giver et ekstra niveau af usikkerhed med hensyn til kundekendskabskrav, idet nogle salgssteder ikke udelukkende er beregnet på spil og ikke er i stand til at gennemføre den pågældende kontrol (f.eks. barer, restauranter, supermarkeder, butikker eller tankstationer).

Konklusion:

Væddemålsaktiviteter udgør ikke en homogen forretningsmodel. Mht. sårbarhedsvurderingen er det uomtvisteligt, at nogle væddemålsoperatører nationalt er udmærket opmærksomme på de hvidvask-/terrorfinansieringsrisici, de er udsat for, og deres dertil svarende forpligtelser, men det er endnu uvist, om de er i stand til

[101] "Spillerkort" er indretninger, der bruges af leverandører af spiltjenester til at måle den tid, spillere bruger, og de indsatser, de gør. Tab og gevinster fremgår i form af "point", som spillerne samler. "Pointene" kan derefter indløses til kontanter eller varer.

at indføre nøjagtige og fyldestgørende kontroller på grund af væddemålsaktiviteternes natur (betydelige volumener af hurtige og anonyme transaktioner, ofte ved brug af kontanter). Den gældende lovgivning eller reglerne angående betingelserne for licens kunne forbedres for bedre at sikre tilstrækkelige kontroller, også selvom sårbarhedsvurderingen viser, at væddemålsoperatørerne er mere bevidste om risiciene, after at de er gået i gang med at udforme nogle risikobegrænsende foranstaltninger (f.eks. systematiske kontroller over en tærskel eller alternative betalingsværktøjer for at begrænse brugen af kontanter).

Den tilsyneladende mangel på forståelse hos de kompetente myndigheder og finansielle efterretningsenheder af, hvordan væddemålaktiviteter fungerer, er en anden hindring for god risikovurdering og vejledning mht. bekæmpelse af hvidvask af penge og af finansiering af terrorisme. Begrænsning af risiciene mht. bekæmpelse af hvidvask af penge og af finansiering af terrorisme svækkes også af det lave niveau af feedback fra finansielle efterretningsenheder.

I den henseende anses sårbarhedsniveauet for hvidvask af penge i relation til væddemålsaktiviteter for betydeligt (niveau 3).

Risikobegrænsende foranstaltninger:

1) kompetente myndigheder:

- Medlemsstaterne bør forbedre samarbejdet mellem relevante myndigheder (finansielle efterretningsenheder, retshåndhævende myndigheder, politi, sektorbestemte kontrolorganer som tilsynsmyndigheder for spil), så de bedre kan forstå de risikofaktorer, væddemålaktiviteter indebærer, og yde effektiv vejledning.
- Medlemsstaterne bør sikre løbende samarbejde mellem relevante myndigheder og væddemålsoperatører, som bør fokusere på:
    - styrkelse af afsløring af mistænkelige transaktioner og øgning af antallet og kvaliteten af rapporter om mistænkelige transaktioner
    - tilrettelæggelse af undervisningsforløb for personale og complianceansvarlige med særligt fokus på risiciene for organiserede kriminelle grupperingers infiltrering eller ejerskab, og løbende revision af risikovurderingerne vedrørende væddemålsoperatørernes produkter/forretningsmodel
    - sikring af, at tilsynsmyndighederne giver klarere vejledning om risiciene vedrørende bekæmpelse af hvidvask af penge og af finansiering af terrorisme, om kundekendskabskrav og om kravene til indberetning af mistænkelige transaktioner samt om, hvordan man konstaterer de mest relevante indikatorer til opdagelse af hvidvask af penge
    - sikring af, at de finansielle efterretningsenheder giver feedback til væddemålsoperatørerne om kvaliteten af rapporteringen om mistænkelige transaktioner og måderne, hvorpå rapporteringen kan forbedres, og om hvordan oplysningerne i rapporten bruges, helst inden for en fastsat tidsperiode.

- Udvikling af standardiserede skabeloner på EU-niveau til rapporter om mistænkelige transaktioner eller mistænkelige forhold, som tager hensyn til spilsektorens særlige karakteristika.

2) sektoren.

- Medlemsstaterne bør sikre, at væddemålsoperatører løbende arrangerer uddannelsesforløb for personale, complianceansvarlige og detailforhandlere, som særligt fokuserer på risikoen for organiserede kriminelle grupperingers infiltrering eller ejerskab, og løbende reviderer risikovurderingerne af væddemålsoperatørernes produkter/forretningsmodel.
- Europol har undertegnet et aftalememorandum med Global Lottery Monitoring System (GLMS) om at dele information og regelmæssigt rådføre sig med hinanden om undersøgelser vedrørende manipulation af sportskonkurrencer og dermed forbunden organiseret kriminalitet.
- Europol og EU-medlemsstaterne arbejder tæt sammen med UEFA's system til afsløring af væddemålssvig, der overvåger mere end 30.000 UEFA- og europæiske nationale kampe hvert år.
- Medlemsstaterne bør sikre, at væddemålsoperatører virker for i) spillerkort[102] eller brugen af elektroniske identifikationssystemer for at lette kundeidentifikationen og at begrænse brugen af kontanter, og ii) brugen af realtids-overvågningssystemer for at identificere mistænkelige transaktioner på salgsstederne.
- Medlemsstaterne bør sikre, at væddemålsoperatører udpeger en ansvarlig på stedet for bekæmpelse af hvidvask af penge, hvis det ikke allerede er sket.
- Medlemsstaterne bør sikre, at væddemålsoperatørerne gennemfører systematiske risikobaserede kundekendskabskrav i forhold til vinderne og fremmer en lavere tærskel for gevinster, der er omfattet af kundekendskabskrav (i øjeblikket 2 000 EUR, som det fremgår af artikel 11, litra d), i direktiv (EU) 2015/849).

3) Kommissionen:

Kommissionen kunne give vejledning om artikel 11, litra d), mht. gennemførelsen af kundekendskabskrav i forbindelse med "flere operationer, der ser ud til at være indbyrdes forbundne".

[102] "Spillerkort" er indretninger, der bruges af leverandører af spiltjenester til at måle den tid, spillere bruger, og de indsatser, de gør. Tab og gevinster fremgår i form af "point", som spillerne samler. "Pointene" kan derefter indløses til kontanter eller varer.

3. Bingo

Produkt
Bingo (landbaseret/offline)

Sektor
Spilsektoren

Generel beskrivelse af den pågældende sektor og det/den relevante produkt/aktivitet

Bingo, der er offline eller landbaseret, er et hasardspil, hvori spilleren bruger en spilleplade, som kan være elektronisk, og som indeholder numre. Bingo spilles ved at markere eller dække de tal, der er identiske med tal, der udtrækkes tilfældigt, hvilket kan ske manuelt eller elektronisk. Spillet vindes af den spiller, der først markerer eller dækker "rækken", hvilket sker, når alle fem tal på en vandret linje på en spilleplade er udtrukket, eller når spilleren først færdiggør "hele pladen" eller får "bingo", når alle numrene på en spilleplade er udtrukket.

Præmier kan gives i form af naturalier (gavekort), der betales straks på stedet for spillet, eller gives som pengepræmier. De kan også bestå af husholdningsartikler, pyntegenstande eller fødevarer. I nogle medlemsstater er begrænsede pengepræmier imidlertid mulige, og i andre medlemsstater der der intet, der forhindrer foranstalteren af bingotjenesten i at tilbyde rene kontantpræmier. Bingo er hovedsagelig en lokalt baseret aktivitet, der drives av SMV'er og sjældent overskrider nationale grænser. Mens bingo i de fleste medlemsstater anses for et hasardspil, betragtes det i mange andre som en form for lotteri.

Beskrivelse af risikoscenariet

En lovovertræder køber plader – traditionelt med kontanter – på hvilke der er trykt en tilfældig række tal. Spillerne markerer de numre på deres plader, som tilfældigt udtrækkes af en opråber (ansat af spiloperatøren), og vinderen er den første, der har markeret alle sine tal. En vindende plade kan købes for en højere pris ligesom en lotteriseddel eller gevinstkupon.

Trussel

Finansiering af terrorisme

Vurderingen af truslen om terrorfinansiering i relation til bingo er ikke blevet anset for at være relevant. I denne henseende er truslen om terrorfinansiering ikke en del af vurderingen.

Konklusion: ikke relevant

Hvidvask af penge

Vurderingen af truslen om hvidvask af penge i relation til bingo viser følgende:

- som det er tilfældet for alle andre spilaktiviteter, er en af de trusler, som hvidvask af penge udgør for bingo, **risikoen for organiserede kriminelle grupperingers infiltration eller ejerskab**. Trusselsniveauet i relation til risikoen for infiltrering kan variere afhængigt

af typen af operatør, der organiserer bingoaktiviteterne. I bingo synes infiltrationen at forekomme, når gadekriminelle driver barer, hvor bingoudtrækninger ikke bliver overvåget og kan bruges til hvidvask af penge (at gøre midler lovlige, selvom de har en ulovlig oprindelse)

- bortset fra risikoen for infiltrering bliver dette risikoscenarie sjældent brugt af kriminelle til at hvidvaske udbyttet af kriminalitet, da det økonomisk ikke er særlig attraktivt, idet de beløb, der spilles om, er ret små og resultatet usikkert (trækninger baseret på tilfældighed).

Konklusion:

Ud over den horisontale trussel om infiltrering og ejerskab, betragtes bingo ikke af de retshåndhævende myndigheder og andre kompetente myndigheder som en attraktiv mulighed for hvidvask af udbyttet af kriminalitet. Hasardkomponenten i bingo gør det temmelig uattraktivt og yderst usikkert. Der er ikke meget der tyder på, at kriminelle har kapaciteten til og har til hensigt at bruge det, men under alle omstændigheder ville det nok være for meget beskedne gevinstbeløb.

I denne henseende anses den trussel, hvidvask af penge udgør for bingo, som mindre betydelig (niveau 1).

Sårbarhed

Finansiering af terrorisme

Vurderingen af sårbarheden over for terrorfinansiering i relation til bingo er ikke blevet anset for at være relevant. I denne henseende er truslen om terrorfinansiering ikke en del af vurderingen.

Konklusion: ikke relevant

Hvidvask af penge

Vurderingen af sårbarheden over for hvidvask af penge i relation til bingo viser følgende:

a) risikoeksponering

Omfanget af bingoaktiviteter er ret begrænset og udgør et beskedent antal økonomiske transaktioner. Når der spilles offline, er aktiviteten hovedsagelig baseret på kontanter. Der anvendes relativt lave indsatser og gevinster, og præmierne er ofte varer i stedet for kontante penge. Den involverer et meget lavt niveau af højrisikokunder og/eller højrisikoområder.

b) risikobevidsthed

Da der ikke foreligger tilfælde, hvor bingo har været anvendt til at hvidvaske udbytte af kriminalitet, er denne komponent vanskelig at vurdere. Ligeledes har det ikke været muligt at fastslå, om de manglende sager om hvidvask af penge skyldes det høje niveau af bevidsthed om risikoen for hvidvask af penge, eller det snarere skylde det lave niveau for kriminelle organisationers ønske om at anvende dette scenarie.

c) retsgrundlag og kontroller

Bingoaktiviteter har været omfattet af EU's regler om bekæmpelse af hvidvask af penge siden gennemførelsen af det fjerde hvidvaskdirektiv. Men på grund af direktivets principper om mindsteharmonisering kan der stadig være forskelle fra medlemsstat til medlemsstat med hensyn til regulering, tilsyn med sektoren og håndhævelse af reglerne om bekæmpelse af hvidvask af penge og af finansiering af terrorisme.

Bingo findes ikke i alle medlemsstater, men hvor det gør, bør det være underlagt regler om bekæmpelse af hvidvask af penge. På nationalt plan kan bingooperatører enten være omfattet af reglerne om kasinoer eller kan være omfattet af en særlig ordning (f.eks. en fodboldklub, der ejer sin egen bingohal). Repræsentanter for sektoren har nævnt, at der er indført tærskler med henblik på systematisk identifikation, hvilket er blevet bekræftet af kompetente myndigheder, som er tilbøjelige til at bekræfte, at der er indført effektive kontroller. Endnu en gang er de forholdsvis lave beløb, der spilles om, og/eller som udgør gevinster, en faktor i den samlede sårbarhedsvurdering.

Konklusion: Bingos karakteristika gør, at det i beskeden grad er sårbart over for risikoen for hvidvask af penge. Det er i høj grad baseret på tilfældigheder, med forholdsvis lave indsatser og gevinster (ofte i form af naturalier). Skønt denne aktivitet hovedsagelig er kontantbaseret, drejer den sig ikke om særlig høje indsatsbeløb. I lande med bingoaktiviteter bør det være omfattet af regler om bekæmpelse af hvidvask af penge og af finansiering af terrorisme, og der bør eksistere effektive kontroller. Komponenten risikobevidsthed var det ikke muligt at bedømme ordentligt på grund af manglende indberetninger. I denne henseende anses sårbarheden over for hvidvask af penge som mindre betydelig (niveau 1).

Risikobegrænsende foranstaltninger:

Medlemsstaterne bør sikre, at bingooperatører løbende arrangerer uddannelsesforløb for personale og complianceansvarlige, som særligt fokuserer på risikoen for organiserede kriminelle grupperingers infiltrering eller ejerskab, og risikovurderinger af deres produkter/forretningsmodel, som bør revideres regelmæssigt. I lyset heraf bør medlemsstaterne også fortsætte overvågningen af bingoaktiviteter med henblik på at konstatere eventuelle fremtidige risici.

4. Kasinoer

Produkt
Kasino (landbaseret/offline)

Sektor
Spilsektoren

Generel beskrivelse af den pågældende sektor og det/den relevante produkt/aktivitet

I flere lande (Belgien, Tjekkiet, Frankrig, Luxembourg, Portugal og Slovakiet) er et kasino (offline/fysisk etablissement) defineret som et sted, hvor der organiseres hasardspil (uanset om det er automatisk), og hvor der finder andre kulturelle og sociale aktiviteter (teatre, restauranter) sted. I andre lande (Østrig, Danmark, Estland, Finland, Tyskland, Letland, Malta, Nederlandene og Sverige) tilbyder kasinoet ikke nødvendigvis andre sociale eller kulturelle aktiviteter, mens nogle medlemsstater (Danmark, Finland, Irland og Det Forenede Kongerige) ikke direkte har defineret, hvad kasinospil vil sige.

Kasinoer kan være statslige eller privatejede, og i nogle medlemsstater er det kun én enkelt operatør, der har licens (Finland, Østrig, Nederlandene og Sverige).

Kasinoer har været omfattet af EU's lovgivning om bekæmpelse af hvidvask af penge i mere end 10 år, og mens medlemsstaterne har mulighed for at undtage visse spiltjenester fra nogle af eller alle kravene i fjerde hvidvaskdirektiv efter en passende risikovurdering, er dette ikke tilfældet for kasinoer.

Beskrivelse af risikoscenariet

En lovovertræder køber jetoner i kasinoet ved et dertil indrettet salgssted (for kontanter eller anonyme, forudbetalte kort), og disse jetoner kan bruges i en bred vifte af spil (med klart definerede regler). Kasinopersonale (croupierer) interagerer med spillere i mange godt regulerede spil som baccarat, roulette og blackjack. Hvis den pågældende vinder, får spilleren jetoner ved bordet, som så skal veksles tilbage til kontanter ved et dertil indrettet salgssted (hvorved ulovlige midler legitimeres).

En lovovertræder kan bruge "kurerer" eller samarbejdspartnere til at købe jetoner på deres vegne med ulovlige midler. Lovovertræderen modtager jetonerne i kasinoet og veksler dem til kontanter og foregiver, at den pågældende vandt dem i de spil, der udbydes i kasinoet.

En lovovertræder kan også drage fordel af, at visse kasinospil giver et højt afkast af indsatsen (afhængigt af, om indsatserne er højrisiko eller lavrisiko). To spillere kan også samarbejde og gøre indsatser på et roulettebord på rød og sort samtidig og derved kun få 3% sandsynlighed for at miste deres samlede indsatser.
En lovovertræder kan også overføre penge fra det ene kasino til en anden (hvis dette er tilladt ifølge loven) og på den måde give en anden spiller adgang til jetoner. I sådanne tilfælde bruges kasinoer som finansielle institutioner ved at der overføres midler fra den ene konto til den anden.

Trussel

Finansiering af terrorisme

Vurderingen af) truslen om terrorfinansiering i relation til kasinoer er ikke blevet anset for at være relevant. I denne henseende er truslen om terrorfinansiering ikke en del af vurderingen.

Konklusion: ikke relevant

Hvidvask af penge

Vurderingen af den risiko, som hvidvask af penge udgør for kasinoer viser, som det er tilfældet for alle andre spilaktiviteter, **risikoen for organiserede kriminelle grupperingers infiltration eller ejerskab**. Retshåndhævende myndigheder har anført, at navnlig kasinoer kan være udsat for trusler om infiltration. Kasinoer, der drives af statsmonopoler eller offentlige virksomheder, synes at være mindre udsat for trusler om infiltrering på grund af bestemmelser om f.eks. åbenhed om de reelle ejerforhold. Dette forhold har betydning for, om organiserede kriminelle grupperinger har til hensigt og har kapacitet til at infiltrere kasinoer. Desuden har interessenter peget på, at nationale licenssystemer garanterer, at ejerforholdene (og ændringer i ejerforholdene) er i overensstemmelse med nationale love og forskrifter. Efter disse regler gennemfører nationale tilsynsmyndigheder streng kontrol af egnethed og hæderlighed samt kontrol af oprindelsen af de midler, der er tale om. De undersøger også operatører, nøglemedarbejdere og højtplacerede ansatte. Interessenterne påpeger, at kasinoer typisk har strenge systemer til forebyggelse af svig og beskytte mod al kriminel aktivitet. Alligevel mener de retshåndhævende myndigheder samlet set, at kasinoer er den mest udnyttede kanal til at hvidvaske penge gennem spilaktiviteter, selvom kasinoaktiviteter har været omfattet af tidligere EU-lovgivning om bekæmpelse af hvidvask af penge.

Konklusion:

Kasinoer anses for at være udsat for trusler om infiltrering, selvom dette risikoniveau er lavere for så vidt angår kasinoer ejet af staten eller offentlige virksomheder. De retshåndhævende myndigheder anser imidlertid alligevel kasinoer for den mest udnyttede kanal til at hvidvaske penge gennem spilaktiviteter. Dermed forekommer risikoen for, at kasinoer udnyttes til hvidvask af penge at være høj, og trusselsniveauet for hvidvask af penge mod kasinoer anses som meget betydeligt (niveau 4).

Sårbarhed

Finansiering af terrorisme

Vurderingen af sårbarheden over for terrorfinansiering i relation til kasinoer er ikke blevet anset for at være relevant. I denne henseende er sårbarheden over for terrorfinansiering ikke en del af vurderingen.

Konklusion: ikke relevant

Hvidvask af penge

Vurderingen af sårbarheden over for hvidvask af penge viser, at markedet varierer fra den ene medlemsstat til den anden.

a) risikoeksponering

Selvom sektoren har udviklet alternative betalingsmidler er brugen af kontanter vigtig i praksis, og sektoren kan under visse omstændigheder blive udsat for højrisikokunder (politisk eksponerede personer eller kunder fra tredjelande med høj risiko). Derudover er kasinoer karakteriseret ved et stort antal økonomiske transaktioner på grund af den store mængde af spilaktiviteter, de fører med sig.

b) risikobevidsthed

Optagelsen af kasinoer på listen over forpligtede enheder i det fjerde hvidvaskdirektiv samt i tidligere EU-lovgivning om bekæmpelse af hvidvask af penge har utvivlsomt bidraget til at gøre sektoren mere risikobevidst. De retsregler, der allerede gælder for kasinoer, har f.eks. skabt incitamenter til at uddanne personalet og til at forbedre kontrollerne. Kasinopersonalet bliver orienteret om og trænet i at identificere mønstre og adfærd, der anses for at være kendetegnende for trusler om hvidvask. Disse uddannelsesaktiviteter omfatter f.eks. foranstaltninger vedrørende og instrukser om håndtering af kontanter. Mange landbaserede kasinoer har udviklet inspektions- og kontrolsystemer ved eksterne og uafhængige kontrolinstitutter, hvilket reducerer sårbarheden over for hvidvask af penge og kriminelle aktiviteter. Desuden har langt størstedelen af de landbaserede kasinoer et videoovervågningssystem, der viser de områder, hvor transaktionerne gennemføres. Nogle kundekendskabsprocedurer bliver automatisk udført som led i identifikationsproceduren: alle besøgende, før de kommer ind i kasinoet, identifikation af besøgende før køb af jetoner/kuponer og identifikation, efter at en vis beløbstærskel er nået, hvilket i de fleste tilfælde er 2 000 EUR som fastsat i det fjerde hvidvaskdirektiv, men kan være lavere. Nogle kasinoer vil måske undlade at identificere kunden over en vis tærskel, når den pågældende er blevet identificeret på anden måde (dvs. ved indgangen til kasinoet eller ved køb af jetoner). Skærpede kundekendskabskrav kan finde anvendelse efter foruddefinerede højrisikokriterier, f.eks. bestemte pengebeløb, transaktioner eller strukturering af operationen.

Ifølge nogle kompetente myndigheder og finansielle efterretningsenheder er der stadig svagheder ned hensyn til omfanget af kundekendskabskravene (der ikke synes at være særlig godt forstået af sektoren) og gennemførelsen af dem, som tilsynsmyndighederne ikke betragter som tilfredsstillende i alle tilfælde: f.eks. når kontrol af ID-kort bliver udført, men kravene til journalføringen ikke bliver opfyldt eller er af ringe kvalitet, eller at kundekendskabsprocedurer gennemføres vedrørende en kunde, når han kommer ind i kasinoet, men ikke når han køber jetoner. Men selvom rapporteringen om mistænkelige transaktioner er ujævn, afhængigt af de enkelte medlemsstater, er det lave antal rapporter rimeligt begrundet, idet sektoren anses for at være stærkt reguleret og generelt godt kontrolleret. Kravet om, at der skal indhentes overordnet godkendelse af alle højrisikotransaktioner, anses for at begrænse risikoen for infiltrering. Med hensyn til rapporter om mistænkelige transaktioner har interessenter understreget den manglende tilbagemelding fra finansielle efterretningsenheder. De påpeger, at kvaliteten af

rapporteringen ville blive forbedret, hvis de finansielle efterretningsenheder ydede vejledning og feedback, helst inden for en fastsat tidsperiode. Den manglende tilbagemelding fra finansielle efterretningsenheder vedrørende rapporterne giver anledning til vanskeligheder for kasinoerne i enkelte tilfælde (hvor det er uklart, om pengene bør udbetales til en spiller, som så på sin side måske kan rejse en sag over for casinoerne) og forhindrer forbedringer af praksis vedrørende bekæmpelse af hvidvask af penge i almindelighed.

c) retsgrundlag og kontroller

Optagelsen af kasinoer på listen over forpligtede enheder i det fjerde hvidvaskdirektiv samt i tidligere EU-lovgivning om bekæmpelse af hvidvask af penge har utvivlsomt spillet en rolle for kvaliteten af de eksisterende kontroller. Det fremgår, at overordnet set formår kasinoerne at imødekomme behovet for at have flere lag kontrol, vel vidende at der det meste af tiden foregår adskillige spilaktiviteter i et casino.

Fra de kompetente myndigheders synspunkt begrænser kontrollen af egnethed og hæderlighed den væsentligste sårbarhed for kasinoer, dvs. infiltrering. Ejere (aktionærer), højtstående medarbejdere og nøglemedarbejdere bliver systematisk undersøgt af kasinooperatører, hvilket giver ret effektiv beskyttelse mod risikoen for infiltrering. På trods af et overordnet set godt billede konstaterer de retshåndhævende myndigheder stadig nogle svagheder, hvilket tyder på, at de nuværende regler ikke anvendes korrekt. Antallet af sager om hvidvask af penge, der undersøges af de retshåndhævende myndigheder, synes at vise, at der stadig er plads forbedringer.

Konklusion:

Selvom risikoen fortsat er høj (stort antal finansielle transaktioner, kontantbaserede) har den omstændighed, at kasinoer i mere end 10 år har været omfattet af reglerne om bekæmpelse af hvidvask af penge, øget bevidstheden om sektorens sårbarhed over for hvidvask af penge. Kontrollerne er mere effektive, og personalet er bedre uddannet. Imidlertid er der fortsat svagheder med hensyn til gennemførelsen af kravene vedrørende bekæmpelse af hvidvask af penge og af finansiering af terrorisme, særligt mht. kundekendskabskrav. Omfanget af rapporteringen er temmelig ujævnt fra den ene medlemsstat til den anden, hvilket kan skyldes et godt tilsynsniveau. I den henseende anses sårbarhedsniveauet for hvidvask af penge i relation til kasinoer for i moderat grad betydeligt (niveau 2).

Risikobegrænsende foranstaltninger:

1) kompetente myndigheder:

- Medlemsstaterne bør forbedre samarbejdet mellem relevante myndigheder (finansielle efterretningsenheder, retshåndhævende myndigheder, politi, sektorbestemte kontrolorganer som tilsynsmyndigheder for spil), så de bedre kan forstå de risikofaktorer, kasinoer indebærer, og yde effektiv vejledning.

- Medlemsstaterne bør sikre løbende samarbejde mellem relevante myndigheder og kasinoer, som bør fokusere på:

- styrkelse af afsløring af mistænkelige transaktioner og øgning af antallet og kvaliteten af rapporter om mistænkelige transaktioner
- tilrettelæggelse af undervisningsforløb for personale og complianceansvarlige med særligt fokus på risiciene for organiserede kriminelle grupperingers infiltrering eller ejerskab, og løbende revision af risikovurderingerne vedrørende spiloperatørernes produkter/forretningsmodeller
- sikring af, at tilsynsmyndighederne giver klarere vejledning om risiciene vedrørende bekæmpelse af hvidvask af penge og af finansiering af terrorisme, om kundekendskabskrav og om kravene til indberetning af mistænkelige transaktioner samt om, hvordan man konstaterer de mest relevante indikatorer til opdagelse af hvidvask af penge
- sikring af, at de finansielle efterretningsenheder giver feedback til kasinoerne om kvaliteten af rapporteringen om mistænkelige transaktioner, og måderne, hvorpå rapporteringen kan forbedres, og om hvordan oplysningerne i rapporten bruges, helst inden for en fastsat tidsperiode
- udvikling af standardiserede skabeloner på EU-niveau til rapporter om mistænkelige transaktioner eller mistænkelige forhold, idet der tages hensyn til spilsektorens særlige karakteristika
- anbefaling af, at der ikke udstedes certifikater for vinderkuponer i kasinoer.

- Medlemsstaterne bør pålægge de kompetente myndigheder at rapportere, om kasinoer anvender ordningerne til bekæmpelse af hvidvask af penge og af finansiering af terrorisme effektivt, især for så vidt angår effektiviteten af den kontrol, der foretages via videoovervågning, og effektiviteten af de tærskelbaserede kundekendskabskrav.

2) sektoren.

- Medlemsstaterne bør sikre, at kasinoer løbende arrangerer uddannelsesforløb for personale og complianceansvarlige, som særligt fokuserer på risikoen for organiserede kriminelle grupperingers infiltrering eller ejerskab, og løbende reviderer risikovurderingerne af deres produkter/forretningsmodel.
- Medlemsstaterne bør sikre, at kasinoer virker for i) spillerkort[103] eller brug af elektroniske identifikationssystemer for at lette kundeidentifikationen og at begrænse brugen af kontanter og ii) brugen af realtids-overvågningssystemer for at identificere mistænkelige transaktioner.
- Medlemsstaterne bør sikre, at kasinoer udpeger en ansvarlig på stedet for bekæmpelse af hvidvask af penge, hvis det ikke allerede er sket.
- Medlemsstaterne bør sikre, at kasinooperatørerne gennemfører systematiske risikobaserede kundekendskabsprocedurer i forhold til vinderne og fremmer en lavere tærskel for gevinster, der er omfattet af kundekendskabskrav (i øjeblikket 2 000 EUR, som det fremgår af artikel 11, litra d), i direktiv (EU) 2015/849).

[103] "Spillerkort" er indretninger, der bruges af leverandører af spiltjenester til at måle den tid, spillere bruger, og de indsatser, de gør. Tab og gevinster fremgår i form af "point", som spillerne samler. "Pointene" kan derefter indløses til kontanter eller varer.

3) Kommissionen:

Kommissionen kunne give vejledning om artikel 11, litra d), mht. gennemførelsen af kundekendskabskrav i forbindelse med "flere operationer, der ser ud til at være indbyrdes forbundne".

5. Spilleautomater (uden for kasinoer)

Produkt
Spilleautomater (landbaserede/offline og uden for kasinoer)

Sektor
Spilsektoren

Generel beskrivelse af den pågældende sektor og det/den relevante produkt/aktivitet

Spilleautomater (offline) baseret på en generering af tilfældige tal opdeles normalt i flere underkategorier, afhængigt af den maksimale indsats, maksimale gevinst eller den type lokaliteter, spilleautomaten kan placeres i. En yderligere sondring sker mellem traditionelle spilleautomater ("enarmede tyveknægte") og videolotteriterminaler, som er tilsluttet en central terminal og tilbyder et bredere udvalg af spil.

Markedet for spilleautomater uden for kasinoer i EU varierer fra den ene medlemsstat til den anden (eller efter region, idet tilladelser i nogle tilfælde gives og tilsyn udføres på dette niveau). I visse medlemsstater er spilleautomater uden for kasinoer forbudt, mens andre kun tillader automater med lave indsatser og gevinster.

I visse medlemsstater findes spilleautomater i en bred vifte af lokaler såsom væddemåls-butikker, shoppingcentre, barer og caféer. Disse terminaler tager imod kontanter og udleverer en kvittering, hvilket giver bevis for kilden til pengene. Hvor spilleautomater er tilladt, kan de være underlagt streng regulering for så vidt angår en fast indsats og begrænsninger i forhold til spilmuligheder. Men spilleren kan have mulighed for at interagere mere frit (f.eks. bettingterminaler med faste odds (FOBT'er), i form af elektronisk roulette, hvor spilleren kan vælge en række indstillinger og ændre indsatser).

Beskrivelse af risikoscenariet

En lovovertræder indskyder ulovlige midler (kontanter) i spilleautomater eller bruger dem til at købe poletter til maskinerne. Visse spillemaskiner tillader også kun, at en lille del af det (deponerede) beløb bruges som indsats, og så kan lovovertræderen anmode om udbetaling af de resterende midler til en bankkonto eller kontant med en kvittering (hvilket giver muligheder for at legitimere et større beløb, end der blev spillet for).

En lovovertræder anvender elektronisk roulette for at hvidvaske penge ved at placere lige store indsatser på både rød og sort samt en mindre indsats på 0; langt de fleste spil vil aldrig blive tabt, da det er en 50/50-indsats, og der vil være kvitteringer, der bekræftet gevinsten.

Endvidere kan "Ticket In Ticket Out" (*TITO*)-kuponer[104] fra automater på kasinoer, spillehaller eller væddemålsbutikker bruges til hvidvask af penge og indløses på et senere tidspunkt eller af tredjeparter.

En lovovertræder kan gøre det hele igen og/eller på flere steder for at minimere mistanke eller omgå begrænsninger på indsatser eller spilletid.

Trussel

Finansiering af terrorisme

Vurderingen af truslen om terrorfinansiering i relation til spilleautomater er ikke blevet anset for at være relevant. I denne henseende er truslen om terrorfinansiering ikke en del af vurderingen.

Konklusion: ikke relevant

Hvidvask af penge

Vurderingen af den risiko, som hvidvask af penge udgør for spilleautomater, viser, som det er tilfældet for alle andre spilaktiviteter, **risikoen for organiserede kriminelle grupperingers infiltration eller ejerskab**. Men ifølge undersøgelser foretaget af de retshåndhævende myndigheder ser det ud til, at tilfældene er ret sjældne eller ikke indberettes. Spilleautomater betragtes muligvis ikke som en særlig realistisk og attraktiv økonomisk mulighed, idet chancen for at vinde store beløb er relativt lille (resultat baseret på tilfældigheder, ofte med små indsatser og små gevinster), selvom der for nogle maskiners vedkommende findes måder, hvorpå chancerne for at vinde kan forøges, eller man endog kan undgå at spille og blot indbetale og straks få pengene tilbage.

Konklusion: Spilleautomater fremstår ikke som en attraktiv mulighed for hvidvask af penge på grund af det indbyggede chanceelement og små beløb i indsatser og gevinster kombineret med den tid og det besvær, der er forbundet med at hvidvaske pengebeløb af betydning. Visse typer spilleautomater giver dog mulighed for indskud af større indsatser og/eller giver højere gevinster, eller de lader lovovertræderen anvende kun en lille del af beløbet som indsats og anmode om udbetaling af de resterende midler (til en bankkonto eller kontant med en kvittering). I den henseende og selvom truslen fra hvidvask af penge kan variere mellem forskellige typer spilleautomater (store/små indsatser og/eller gevinster) anses den generelt for at være i moderat grad betydelig (niveau 2).

Sårbarhed

[104] "Ticket-in, ticket out (TITO)"-maskiner anvendes i spilleautomater i kasinoer til at udprinte et stykke papir med en stregkode, der repræsenterer et pengebeløb. De kan derefter indløses til kontanter i en automat.

Finansiering af terrorisme

Vurderingen af sårbarheden over for terrorfinansiering i relation til spilleautomater er ikke blevet anset for at være relevant. I denne henseende er sårbarheden over for terrorfinansiering ikke en del af vurderingen.

Konklusion: ikke relevant

Hvidvask af penge

Vurderingen af sårbarheden over for hvidvask af penge i relation til spilleautomater viser følgende:

a) risikoeksponering

I spilleautomater (landbaserede) bruges mest kontanter. De beløb, der omsættes, varierer, men er ofte temmelig små, men nogle maskiner giver mulighed for også at satse større beløb.

b) risikobevidsthed

For så vidt angår spilleautomater udenfor kasinoer er risikobevidstheden forskellig fra den ene medlemsstat til den anden, og det ser ud til, at uafhængige spilleautomatoperatører er mindre opmærksomme på deres forpligtelser mht. bekæmpelse af hvidvask af penge og af finansiering af terrorisme, da de er mindre organiserede end operatørerne i landbaserede kasinoer.

Kompetente myndigheder har endvidere bemærket de nye risici, der er forbundet med videolotteriterminaler, der udløser et stigende antal indberetninger om mistænkelige transaktioner (fordi gevinsterne generelt på ny sluses ind i den sorte økonomi).

c) retsgrundlag og eksisterende kontroller

Spilleautomater har været omfattet af EU's regler om bekæmpelse af hvidvask af penge siden gennemførelsen af det fjerde hvidvaskdirektiv). Men på grund af direktivets principper om mindsteharmonisering kan der stadig være forskelle fra medlemsstat til medlemsstat med hensyn til regulering, tilsyn og håndhævelse af reglerne om bekæmpelse af hvidvask af penge og af finansiering af terrorisme. Nogle medlemsstater har besluttet at regulere denne sektor, når den opererer selvstændigt i forhold til kasinoer. Ifølge de kompetente myndigheder og finansielle efterretningsenheder er kontrolniveauet utilstrækkeligt og sanktionsniveauet ikke tilstrækkeligt afskrækkende (f.eks. fik en bookmaker i medlemsstat X en bøde på over 100 000 EUR for at have undladt at forhindre en narkohandler i at hvidvaske over 1 mio EUR i dens butikker). Men spilleautomatoperatører er i øjeblikket ved at udvikle risikobegrænsende foranstaltninger, f.eks. forbud mod kontant udbetaling af gevinster, når de overstiger et vist beløb.

Konklusion:

For så vidt angår spilleautomater uden for kasinoer har det vist sig, at de eksisterende kontroller ikke er effektive, og at indberetningsniveauet af mistænkelige transaktioner er meget lavt, selvom risikobegrænsende foranstaltninger med henblik på at begrænse kontantudbetinger ofte begrænser risikoen for hvidvask af penge. Selvom beløbene for indsatser og gevinster ofte er relativt lave, tillader spilleautomater hurtige og anonyme (samt gentagne) transaktioner, og de er ofte kontantbaserede. Transaktioner kan også gennemføres på flere steder for at minimere mistanker eller omgå begrænsninger på indsatser eller spilletid. I denne henseende anses niveauet af spilleautomaters sårbarhed over for hvidvask af penge for i moderat grad betydelig (niveau 2).

Risikobegrænsende foranstaltninger:

1) kompetente myndigheder

- Medlemsstaterne bør forbedre samarbejdet mellem relevante myndigheder (finansielle efterretningsenheder, retshåndhævende myndigheder, politi, sektorbestemte kontrolorganer som tilsynsmyndigheder for spil), så de bedre kan forstå de risikofaktorer, spilleautomater indebærer, og yde effektiv vejledning.
- Medlemsstaterne bør sikre løbende samarbejde mellem relevante myndigheder og spilleautomatoperatører, som bør fokusere på:
    - styrkelse af afsløring af mistænkelige transaktioner og øgning af antallet og kvaliteten af rapporter om mistænkelige transaktioner
    - tilrettelæggelse af undervisningsforløb for personale, complianceansvarlige og forhandlere med særligt fokus på risiciene for organiserede kriminelle grupperingers infiltrering eller ejerskab, og løbende revision af risikovurderingerne
    - sikring af, at tilsynsmyndighederne giver klarere vejledning om risiciene vedrørende bekæmpelse af hvidvask af penge og af finansiering af terrorisme, om kundekendskabskrav og om kravene til indberetning af mistænkelige transaktioner samt om, hvordan man konstaterer de mest relevante indikatorer til opdagelse af hvidvask af penge
    - sikring af, at tilsynsmyndighederne give klarere vejledning om nye risici forbundet med videolotteriterminaler
    - sikring af, at de finansielle efterretningsenheder giver feedback til spilleautomatoperatører om kvaliteten af rapporteringen om mistænkelige transaktioner og måderne, hvorpå rapporteringen kan forbedres, og om hvordan oplysningerne i rapporten bruges, helst inden for en fastsat tidsperiode.
    - udvikling af standardiserede skabeloner på EU-niveau til rapporter om mistænkelige transaktioner eller mistænkelige forhold, som tager hensyn til spilsektorens særlige karakteristika.

2) Sektoren

- Medlemsstaterne bør sikre, at spilleautomatoperatører løbende arrangerer uddannelsesforløb for personale, complianceansvarlige og detailforhandlere, som særligt fokuserer på risikoen for organiserede kriminelle grupperingers infiltrering

eller ejerskab, og løbende reviderer risikovurderingerne af deres produkter/forretningsmodel.

- Medlemsstaterne bør sikre, at spilleautomatoperatører virker for i) spillerkort[105] eller brugen af elektroniske identifikationssystemer for at lette kundeidentifikationen og at begrænse brugen af kontanter, og ii) realtids-overvågningssystemer for at identificere mistænkelige transaktioner på salgsstederne.;
- Medlemsstaterne bør sikre, at spilleautomatoperatører udpeger en ansvarlig på stedet for bekæmpelse af hvidvask af penge, hvis det ikke allerede er sket.
  Medlemsstaterne bør sikre, at spilleautomatoperatørerne gennemfører systematiske risikobaserede kundekendskabsprocedurer i forhold til vinderne og fremmer en lavere tærskel for gevinster, der er omfattet af kundekendskabskrav (i øjeblikket 2 000 EUR, som det fremgår af artikel 11, litra d), i direktiv (EU) 2015/849).

3) Kommissionen

Kommissionen kunne give vejledning om artikel 11, litra d), mht. gennemførelsen af kundekendskabskrav i forbindelse med "flere operationer, der ser ud til at være indbyrdes forbundne".

[105] "Spillerkort" er indretninger, der bruges af leverandører af spiltjenester til at måle den tid, spillere bruger, og de indsatser, de gør. Tab og gevinster fremgår i form af "point", som spillerne samler. "Pointene" kan derefter indløses til kontanter eller varer.

6. Lotterier

Lotterier

Sektor
Spilsektoren

Generel beskrivelse af den pågældende sektor og det/den relevante produkt/aktivitet

Lotterier dækker et bredt spektrum af numeriske spil, hvor en vinder vælges tilfældigt. Lotterier spænder fra nationale lotterier, som har fået tildelt en eksklusiv licens til at drive lotterispil på en medlemsstats område (statsejede og private aktører, både profit og nonprofit, der handler på statens vegne), til små velgørenhedslotterier, der samler indtægter til velgørende formål eller nonprofitorganisationer (f.eks. velgørende organisationer, civilsamfundet, sport, kultur, kulturarv, social tryghed og social velfærd). Definitionen af et lotteri - eller kravene for at opnå licens - varierer fra den ene medlemsstat til den anden.

Nationale lotterisedler sælges sædvanligvis gennem agenter mod kontanter eller via korttransaktioner eller direkte til spilleren online. Der spilles i de fleste tilfælde for små beløb. Vinderne kan findes straks (f.eks. "skrabelodder") eller på grundlag af ugentlige trækninger (ofte stærkt promoverede eller udsendt i fjernsynet). Gevinsterne bliver udbetalt enten af agenter, når den vindende seddel forevises (små beløb) eller overføres direkte til spillerens bankkonto (større beløb og jackpot). Afkastet af indsatsen er normalt lavere end for andre spilprodukter, idet formålet er at skaffe midler til almennyttige formål (40-50 % af de opkrævede penge tilbageleveres normalt som præmier — men der findes eksempler på, at afkastet er højere. Chancen for at vinde en jackpot er meget ringe (f.eks. ligger sandsynligheden i intervallet 1 til 140 mio. for at vinde Euro Millions største jackpot).

Beskrivelse af risikoscenariet

Det relativt lave afkast til spillerne gør direkte køb af lotterisedler til en kostbar og utiltrækkende form for hvidvask af penge. Køb af lodsedler direkte med henblik på at vinde en gevinst anses derfor ikke for at være et sandsynligt risikoscenarie. Tværtimod er metoden med at købe en vinderseddel — en lovovertræder køber en lotteriseddel fra vinderen (muligvis i ledtog med salgsagenten) og indkasserer præmien med en kvittering — et mere realistisk scenarie, som retshåndhævende myndigheder har rapporteret.

Trussel

Finansiering af terrorisme

Vurderingen af truslen om terrorfinansiering i relation til Lotterier er ikke blevet anset for at være relevant. I denne henseende er truslen om terrorfinansiering ikke en del af vurderingen.

Konklusion: ikke relevant

Hvidvask af penge

Vurderingen af den trussel, hvidvask af penge udgør i relation til lotterier, viser følgende:

- som det er tilfældet for alle andre spilaktiviteter, **er der en risiko for organiserede kriminelle grupperingers infiltrering eller ejerskab.** Hvis der er tale om statsejede lotterier, er risikoen minimal, men stiger på forhandlerniveau.

- mht. andre typer trusler har lovovertrædere ifølge de retshåndhævende myndigheder kun vage hensigter om at bruge lotterier til hvidvask af udbyttet af kriminalitet. De retshåndhævende myndigheder har kun konstateret få sager, hvor eksempelvis vinderlodder er blevet fundet sammen med kontanter eller narkotika i forbindelse med beslaglæggelser. Men hvis og når dette scenarie bruges, kan der hæves store summer (f.eks. blev 1,2 mio. EUR hævet via vinderlodder i en nylig efterforskning). Men nogen planlægningskapacitet og teknisk ekspertise er påkrævet, hvilket i almindelighed kræver medvirken fra lotterioperatøren og brug af stråmænd. Dette kan begrænse kriminelles intention om at bruge dette risikoscenarie. Ligeledes giver lotterier færre muligheder for hvidvask af penge pga. lavere frekvens af trækninger, lave gennemsnitlige indsatser og gevinster (strakslodder og numeriske spil og lav udbetalingsratio). Generelt vil lotterier ikke i sig selv være specielt attraktive med henblik på hvidvask af udbytte af kriminalitet på grund af den relativt lave gevinstrate (oftest bliver kun 50% af lodseddelsalget anvendt til præmier).

Konklusion: Der har været rapporteret tilfælde af, at lotterier bruges til at hvidvaske udbytte af kriminalitet. Men det kræver planlægning og ekspertise, som kan begrænse organiserede kriminelle organisationers hensigt om og kapacitet til at benytte lotterier. Den konkrete metode med at købe vinderlodder synes dog at være et mere realistisk og rapporteret scenarie. I denne henseende anses trusselsniveauet fra hvidvask af penge mod lotterier som i moderat grad betydeligt (niveau 2).

Sårbarhed

Finansiering af terrorisme

Vurderingen af sårbarheden over for terrorfinansiering i relation til lotterier er ikke blevet anset for at være relevant. I denne henseende er truslen om terrorfinansiering ikke en del af vurderingen.

Konklusion: ikke relevant

Hvidvask af penge

Vurderingen af sårbarheden over for hvidvask af penge i relation til lotterier viser følgende:

a) risikoeksponering

Ved vurderingen af risikoeksponeringen, er det også taget i betragtning, at lotterier i mange medlemsstater er drevet af et statsmonopol. Udbetaling af større gevinster er underlagt streng kontrol, og de fleste lotterioperatører begrænser de præmiestørrelser, der kan udbetales af forhandlere. Store præmier indkasseres på lotteriets hovedkontor og/eller i banker (efter aftale mellem operatøren og den valgte bank), og dette følger strenge kontrolprocedurer både mht. præmiekravets gyldighed og vinderens identitet. Gevinster under en vis tærskel (dvs. små beløb), der varierer mellem medlemsstaterne, udbetales direkte af salgsagenter/autoriserede distributører. Hertil kommer, at spillerens anonymitet er garanteret i mange medlemsstater, hvilket gør det vanskeligere for de kriminelle at identificere indehaveren af den vindende kupon med henblik på at kunne købe den til kriminelle formål, medmindre de bliver hjulpet aktivt af medgerningsmænd.

b) risikobevidsthed

Misbrug af lotterier via køb af vinderlodder anses som et stort problem af de finansielle efterretningsenheder og de retshåndhævende myndigheder (herunder ofte i ledtog med salgsagenter), men det generelle niveau af bevidsthed er vanskeligere at vurdere. Selvom identifikationen af spillere henhører under den direkte kontrol hos de forhandlere, der er autoriseret af operatøren autorisation med konkrete sanktioner i forhold til dem, er det blevet nævnt, at lotterioperatører er aktive i kontrollen med de godkendte forhandlere og koordinerer uddannelsesprogrammer i bevidsthed/afsløringer mht. bekæmpelse af hvidvask af penge.

c) retsgrundlag og kontroller

Lotterier har været omfattet af EU's regler om bekæmpelse af hvidvask af penge siden det fjerde hvidvaskdirektiv. Men på grund af direktivets principper om mindsteharmonisering kan der stadig være forskelle fra medlemsstat til medlemsstat med hensyn til regulering, tilsyn med sektoren og håndhævelse af reglerne om bekæmpelse af hvidvask af penge og af finansiering af terrorisme.

På nationalt niveau fungerer de kompetente myndigheders tilsyn godt og udøves generelt af offentlige myndigheder. F.eks. er det blevet påpeget, at de fleste spilmyndigheder allerede har iværksat anbefalede procedurer og kontroller for at forhindre kriminelle i at bruge lotterifaciliteter til hvidvask af penge. Derudover har lotterioperatører etableret interne kontroller og øget årvågenhed i disse sager. For eksempel har de fleste medlemsstater allerede en procedure til at verificere en jackpotvinders identitet i tilfælde, hvor præmien overstiger en forudbestemt tærskel.

Konklusion: Af sårbarhedsvurderingen fremgår, at lotterier ikke i sig selv er et realistisk risikoscenarie, men at risiciene mere er relateret til (købet af) vinderkuponer. Ved eksisterende national lovgivning er der indført foranstaltninger til at kontrollere vinderes identitet, især dem med store gevinster. Trods dette udgør risikoscenariet (indkøb af) vinderlodder fortsat en væsentlig kilde til bekymring. På baggrund af dette anses sårbarhedsniveauet for lotterier over for hvidvask af penge for i moderat grad betydeligt (niveau 2).

Risikobegrænsende foranstaltninger:

1) kompetente myndigheder:

- Medlemsstaterne bør forbedre samarbejdet mellem relevante myndigheder (finansielle efterretningsenheder, retshåndhævende myndigheder, politi, sektorbestemte kontrolorganer som tilsynsmyndigheder for spil), så de bedre kan forstå de risikofaktorer, lotteriaktiviteter indebærer, og yde effektiv vejledning.
- Medlemsstaterne bør sikre et løbende samarbejde mellem relevante myndigheder og lotterioperatører, som bør fokusere på:
    - skærpet gennemførelse af kundekendskabskrav samt afsløring af mistænkelige transaktioner, især i forbindelse med vinderlodder samt øgning af antallet og kvaliteten af rapporterne om mistænkelige transaktioner.
    - tilrettelæggelse af undervisningsforløb for personale, complianceansvarlige og forhandlere med særligt fokus på risiciene for organiserede kriminelle grupperingers infiltrering eller ejerskab, og løbende revision af risikovurderingerne vedrørende deres produkter/forretningsmodel
    - sikring af, at tilsynsmyndighederne giver klarere vejledning om risiciene vedrørende bekæmpelse af hvidvask af penge og af finansiering af terrorisme, om kundekendskabskrav og om kravene til indberetning af mistænkelige transaktioner samt om, hvordan man konstaterer de mest relevante indikatorer til opdagelse af hvidvask af penge
    - sikring af, at de finansielle efterretningsenheder giver feedback til lotterioperatører om kvaliteten af rapporteringen om mistænkelige transaktioner og måderne, hvorpå rapporteringen kan forbedres, og om hvordan oplysningerne i rapporten bruges, helst inden for en fastsat tidsperiode.
    - udvikling af standardiserede skabeloner på EU-niveau til rapporter om mistænkelige transaktioner og mistænkelige forhold, som tager hensyn til spilsektorens særlige karakteristika.

2) sektoren.

- Medlemsstaterne bør sikre, at lotterioperatører løbende arrangerer uddannelsesforløb for personale, complianceansvarlige og detailforhandlere, som særligt fokuserer på risikoen for organiserede kriminelle grupperingers infiltrering eller ejerskab, og løbende reviderer risikovurderingerne af lotterioperatørernes produkter/forretningsmodel. Uddannelsen bør også indeholde oplysninger om relevante faresignaler ved tilbagevendende gevinster.
- Medlemsstaterne bør sikre, at lotterierne fremmer i) brugen af systemer til systematisk identifikation af vindere som f.eks. spillerkort[106] eller elektroniske identifikationssystemer for at lette kundeidentifikationen og ii) brugen af kontobaserede overførsel til udbetaling af store beløb.
- Medlemsstaterne bør tilskynde lotterier til at udpege en ansvarlig på stedet for bekæmpelse af hvidvask af penge, hvis det ikke allerede er sket.

[106] "Spillerkort" er indretninger, der bruges af leverandører af spiltjenester til at måle den tid, spillere bruger, og de indsatser, de gør. Tab og gevinster fremgår i form af "point", som spillerne samler. "Pointene" kan derefter indløses for kontanter eller varer.

- Medlemsstaterne bør sikre, at spilleautomatoperatørerne gennemfører systematiske risikobaserede kundekendskabsprocedurer i forhold til vinderne og fremmer en lavere tærskel for gevinster, der er omfattet af kundekendskabskrav (i øjeblikket 2 000 EUR, som det fremgår af artikel 11, litra d), i direktiv (EU) 2015/849).

3) Kommissionen:

Kommissionen kunne give vejledning om artikel 11, litra d), mht. gennemførelsen af kundekendskabskrav i forbindelse med "flere operationer, der ser ud til at være indbyrdes forbundne".

7. Poker

Produkt
Poker (landbaseret/offline)

Sektor
Spilsektoren

Generel beskrivelse af den pågældende sektor og det/den relevante produkt/aktivitet

Generel beskrivelse af den pågældende sektor (størrelse) og statistikker og det/den relevante produkt/aktivitet

Poker er et kortspil, der indebærer væddemål, og hvor vinderen af hver hånd (runde) bestemmes i henhold til kombinationerne af spillernes kort, hvoraf i hvert fald nogle forblive skjult indtil afslutningen af hånden og indsatserne.

Poker arrangeres af private eller statsejede udbydere af spilletjenester på licenserede lokaliteter (f.eks. kasinoer), private klubber eller online (afhængigt af national lovgivning). Det er enten organiseret som en turnering, hvor en pokerspiller indtræder ved at betale et fast buy-in ved starten og får et bestemt antal pokerchips (vinderen af turneringen er den person, der vinder alle pokerchips i turneringen), eller som et bordspilspil, hvor spilleren kan købe flere pokerchips, efterhånden som spillet skrider frem. I modsætning til mange andre spilleprodukter spiller deltagerne mod hinanden og ikke mod arrangøren af aktiviteten. Arrangøren modtager et fast beløb ud af omsætningen (rake) eller gevinsterne.

Poker kan også spilles i private klubber (*cercles de jeux*), som findes i visse lande, men er forbudt i andre, og der kan organiseres turneringer uden for kasinoer.

Beskrivelse af risikoscenariet

En lovovertræder køb chips på casinoet (eller på den pågældende licenserede lokalitet) på et dertil indrettet salgssted (kontant eller med anonyme forudbetalte kort) og disse chips kan overføres til en anden spiller gennem bevidste tab (folding på en vindende hånd sikrer, at medgerningsmanden modtage chipsene). Chips veksles til til kontanter eller overføres på en anden måde til kunden.

En lovovertræder (organiserede kriminelle organisationer) kan også søge at infiltrere den organisatoriske struktur i de licenserede lokaliteter, hvor pokerspil eller turneringer organiseres (f.eks. kasinoer eller private klubber) eller direkte eller indirekte ansøge om tilladelse til at arrangere en pokerturnering, som kan være åben eller kræver invitation.

Trussel

Finansiering af terrorisme

Vurderingen af sårbarheden over for terrorfinansiering i relation til poker er ikke blevet anset for at være relevant. I denne henseende er truslen om terrorfinansiering ikke en del af vurderingen.

Konklusion: ikke relevant

Hvidvask af penge

Vurderingen af den trussel, hvidvask af penge udgør i relation til poker, viser følgende:

- som for alle andre spilaktiviteter, **er der en risiko for organiserede kriminelle grupperingers infiltrering eller ejerskab.**

- denne kanal opfattes som temmelig attraktiv, selvom den kræver moderate niveauer af planlægning (medvirken) eller teknisk ekspertise (spilletrategien som sådan) for at benytte sig af ulovlig turneringer eller for bevidst tabe, således at en medgerningsmand kan vinde.

Konklusion: Ud over risikoen for, at en virksomhed, der har en licens til at arrangere pokerspil eller -turneringer i fysiske lokaliteter, kan være infiltreret (hvilket er en horisontal trussel, som også gælder for andre udbydere af spilletjenester), er det i nogle medlemsstater muligt at arrangere individuelle turneringer, hvilket kan resultere i, at kriminelle organisationer arrangerer pokerspil/-turneringer lovligt. Pokerspillets karakter af alle-mod-alle (muligheden for bevidste tab/at sikre en anden spiller får gevinsterne) gør poker tiltrækkende for hvidvask af penge, selvom det kræver nogen ekspertise og planlægning. I denne henseende anses truslen fra hvidvask af penge mod pokeraktiviteter som betydelig (niveau 3).

Sårbarhed

Finansiering af terrorisme

Vurderingen af sårbarheden over for terrorfinansiering i relation til poker er ikke blevet anset for at være relevant. I denne henseende er truslen om terrorfinansiering ikke en del af vurderingen.

Konklusion: ikke relevant

Hvidvask af penge

Vurderingen af sårbarheden over for hvidvask af penge i relation til poker viser følgende

a) risikoeksponering

For det meste arrangeres pokerspil i licenserede kasinoer. "Private" pokerklubber er forbudt og betragtes som illegale aktiviteter i de fleste medlemsstater. Men selv når det spilles i kasinoer, er poker sårbart over for hvidvask af penge, da det involverer kontantbaserede transaktioner, og at spillere spiller mod andre spillere, det såkaldte "peer-to-peer element" (der omfatter bevidst tab eller at sikre gevinster går til en anden spiller). Pokerspil giver mulighed for, at et betydeligt antal hurtige og anonyme transaktioner gennemføres mellem spillere (chips købes jævnligt for kontanter).

b) risikobevidsthed

Bevidsthedsniveauet er vanskeligt at vurdere på dette stadium, da pokerspil for det meste arrangeres i kasinoer. Udfører en konkret analyse er vanskelig.

c) retsgrundlag og kontroller

Pokeraktiviteter (uden for kasinoer) har været omfattet af EU's regler om bekæmpelse af hvidvask af penge siden gennemførelsen af fjerde hvidvaskdirektiv. Men på grund af direktivets principper om mindsteharmonisering kan der stadig være forskelle mellem medlemsstaterne med hensyn til regulering, tilsyn og håndhævelse af reglerne om bekæmpelse af hvidvask af penge og af finansiering af terrorisme.

Spillerne spiller mod andre spillere, og der er ingen registrering af "hvem-tabte-til-hvem". Der er også opstået uautoriserede private pokerklubber, der er velorganiserede og konkurrerer med den lovlige sektor. Finansielle efterretningsenheder mener, at disse klubber kun har beskeden kapacitet til at opdage mistænkelige transaktioner, især fordi sektoren selv ikke er opmærksom på risiciene og/eller ikke er tilstrækkeligt reguleret/overvåget på nationalt plan.

Konklusion:
Under hensyn til elementet af "alle-mod-alle", den tilsyneladende manglende registrering og ordentlige overvågning, og at sektoren selv ikke er opmærksom på risiciene og/eller udstyret til at bekæmpe misbrug i form af hvidvask af penge anses niveauet for pokers sårbarhed over for hvidvask af penge betydeligt (niveau 3).

Risikobegrænsende foranstaltninger:

1) kompetente myndigheder:

- Medlemsstaterne bør forbedre samarbejdet mellem relevante myndigheder (finansielle efterretningsenheder, retshåndhævende myndigheder, politi, sektorbestemte kontrolorganer som tilsynsmyndigheder for spil), så de bedre kan forstå de risikofaktorer, poker indebærer, og yde effektiv vejledning.
- Medlemsstaterne bør sikre et løbende samarbejde mellem relevante myndigheder og pokeroperatører, som bør fokusere på:
    - styrkelse af kundekendskabskravene og afsløringen af mistænkelige transaktioner og øgning af antallet og kvaliteten af rapporter om mistænkelige transaktioner
    - tilrettelæggelse af undervisningsforløb for personale og complianceansvarlige med særligt fokus på risiciene for organiserede kriminelle grupperingers infiltrering eller ejerskab, og løbende revision af risikovurderingerne vedrørende deres produkter/forretningsmodel
    - sikring af, at tilsynsmyndighederne giver klarere vejledning om risiciene vedrørende bekæmpelse af hvidvask af penge og af finansiering af terrorisme, om kundekendskabskrav og om kravene til indberetning af mistænkelige transaktioner samt om, hvordan man konstaterer de mest relevante indikatorer til opdagelse af hvidvask af penge
    - sikring af, at de finansielle efterretningsenheder giver feedback til pokeroperatører om kvaliteten af rapporteringen om mistænkelige transaktioner , og måderne, hvorpå rapporteringen kan forbedres, og om hvordan oplysningerne i rapporten bruges, helst inden for en fastsat tidsperiode

- udvikling af standardiserede skabeloner på EU-niveau til rapporter om mistænkelige transaktioner og mistænkelige forhold, som tager hensyn til spilsektorens særlige karakteristika.

2) sektoren.

- Medlemsstaterne bør sikre, at pokeroperatører løbende arrangerer uddannelsesforløb for personale, complianceansvarlige og detailforhandlere, som særligt fokuserer på risikoen for organiserede kriminelle grupperingers infiltrering eller ejerskab, og løbende reviderer risikovurderingerne af væddemålsoperatørernes produkter/forretningsmodel.
- Medlemsstaterne bør sikre, at kasinoer virker for spillerkort eller brug af elektroniske identifikationssystemer for at lette kundeidentifikationen
- Medlemsstaterne bør sikre, at pokeroperatørerne udpeger en ansvarlig på stedet for bekæmpelse af hvidvask af penge, hvis det ikke allerede er sket.
- Medlemsstaterne bør sikre, at spilleautomatoperatørerne gennemfører systematiske risikobaserede kundekendskabsprocedurer i forhold til vinderne og fremmer en lavere tærskel for gevinster, der er omfattet af kundekendskabskrav (i øjeblikket 2 000 EUR, som det fremgår af artikel 11, litra d), i direktiv (EU) 2015/849).

3) Kommissionen:

Kommissionen kunne give vejledning om artikel 11, litra d), mht. gennemførelsen af kundekendskabskrav i forbindelse med "flere operationer, der ser ud til at være indbyrdes forbundne".

8. Onlinespil

Produkt
Onlinespil

Sektor
Spilsektoren

Generel beskrivelse af den pågældende sektor og det/den relevante produkt/aktivitet

I denne rapports forstand betyder onlinespil enhver tjeneste, som indebærer, at der gøres en indsats med pengeværdi i hasardspil, herunder med et element af dygtighed, f.eks. lotterier, kasinospil, pokerspil og væddemålstransaktioner, der leveres på afstand med ethvert middel, ad elektronisk vej eller med enhver anden teknologi, der letter kommunikationen, og sker på individuel anmodning fra en ydelsesmodtager.

Alle spilprodukter er tilgængelige online. Disse omfatter i) spil, hvor kunden indskyder en indsatsmod spiltjenesteudbyderen mod faste odds (f.eks. lotterier, sportsvæddemål, roulette osv.), og ii) spilaktiviteter, hvor kunderne kan spille imod hinanden, og hvor tjenesteyderen får en lille kommission for at stille aktiviteten til rådighed, normalt en procentandel af nettogevinsten for hver kunde i hvert spil (f.eks. poker og væddemålsbørser, hvor kunderne både kan gøre og modtage indsatser).

En yderligere opdeling i forskellige onlinespilprodukter er imidlertid ikke blevet anset for nødvendig med henblik på denne rapport, da de relevante risici, trusler og sårbarheder primært synes at være nyttet til karakteren af onlinetransaktioner snarere end til konkrete former for onlinespil.

Beskrivelse af risikoscenariet

onlinespil kan dreje sig om ethvert produkt i spilsektoren eller en kombination af disse. Udover nogle af de risici, der er konstateret for hver enkelt sektor offline, kan der være yderligere risici, som er forbundet med den mangel på kontakt ansigt til ansigt, der skyldes brugen af internettet. Samtidig tilbyder elektroniske spil en betydelig risikobegrænsende funktion – muligheden for at spore alle transaktioner.

En lovovertræder bruger spillewebsteder til at deponere ulovlige midler og til at anmode om udbetaling af gevinster eller en saldo, der ikke er spillet for.

Lovlige onlinespillekonti bliver krediteret med sorte midler (indbetaling) efterfulgt af spil med kun små beløb, hvorefter de resterende midler overføres til en anden spiller (eller en anden onlinespiloperatør). De resterende midler bliver udbetalt, som var de lovlige spilindtægter.

Kriminelle organisationer kan bruge adskillige "smølfer"[107], der spiller direkte mod hinanden og bruger sorte penge. En af "smølferne" modtager alle midlerne som tilsyneladende vinder, der så får udbetalt kontanterne, som om de var lovlige spilindtægter.

Kriminelle organisationer kan købe online kasinokonti, der indeholder midler allerede uploadet af ikke-kriminelle spillere til en højere pris end den reelle.

Kriminelle organisationer kan også opfinde og satse på fiktive (ikke-eksisterende) kampe eller arrangementer for at sikre gevinster.

Trussel

Finansiering af terrorisme

Vurderingen af truslen om terrorfinansiering i relation til onlinespil er ikke blevet anset for at være relevant for denne rapport. Derfor er denne trussel ikke en del af vurderingen.

Konklusion: ikke relevant

Hvidvask af penge

Vurderingen af sårbarhed over for hvidvask af penge i relation til onlinespil viser følgende:

- som for alle andre spilaktiviteter, **er der en risiko for organiserede kriminelle grupperingers infiltrering eller ejerskab.** Retshåndhævende myndigheder har adskillige eksempler på sådanne tilfælde.

- hertil kommer, at organiserede kriminelle grupperinger let kan få adgang til en sådan kanal, i hvilken det er billigt og praktisk for dem at etablere deres aktiviteter. Onlinespil udgør et attraktivt redskab til at hvidvaske udbytte af kriminalitet. Det kan muliggøre, at kriminelle penge kan let konverteres til lovlige indtægter fra spil. Det involverer en stor mængde transaktioner og store pengestrømme. Europol anførte, at nye sager viste, at nogle kriminelle netværk brugte de lovlige online væddemåls- og spilkredsløb tilhørende virksomheder i visse medlemsstater til hvidvask af penge.

Onlinespil i virtuelle aktiver udgør en oplagt mulighed for cyberkriminelle, og denne teknik er blevet anvendt i angreb med ransomware. Blandt de kendte typer aktiviteter findes følgende:

- Onlinespillekonti bliver krediteret med sorte midler (indkassering) efterfulgt af spil med et lille beløb, hvorefter det resterede beløb overføres til en anden spiller (eller en anden spiloperatør). De resterende midler bliver udbetalt som lovlige spilindtægter.
- Brugen af "smølfer", der spiller direkte mod hinanden og bruger sorte penge. En af "smølferne" modtager alle midlerne som tilsyneladende vinder, der så får udbetalt dem som lovlige spilindtægter.
- Købet af online kasinokonti, der indeholder midler allerede uploadet af ikke-kriminelle spillere til en højere pris end den reelle.

[107] En *smølf* er en erfaren spiller, der bruger en ny konto til at spille "anonym" på en spilserver for at forlede andre spillere til at tro, at han er nybegynder i spillet. Målet er at oprette nye konti ved at starte fra bunden, således at man kan konfrontere spillere på lavere niveau.

- Operatøren bruges som kontantintensiv virksomhed til at blande sorte penge fra kriminelle aktiviteter med rene penge fra lovlige kunder.
- Kriminelle fikser spille-odds og resultater, så "smølfer" kan satse sorte penge på de forudvalgte tabende resultater til fordel for onlinekasinoet ("ghost matches").
- Kriminelle bruger tredjeparter, der fungerer som "smølfer" og opretter fiktive kundekonti til at satse og tabe sorte penge over internettet. Alle spillede midler medregnes som udbytte fra online kasinoet, og skyldige afgifter bliver betalt.

Derudover findes der forskellige typer indsatser i onlinemiljøet, der ikke findes offline. Der er en særlig høj risiko for garderede indsatser i onlinespil, hvor en spiller bruger flere konti til at placere indsatser på alle de mulige udfald og dermed reducerer risikoen for tab. For så vidt angår online poker er der også en konkret risiko for aftalt spil.

- risici i forbindelse med manglende kontakt ansigt til ansigt, selvom anonymiteten kan minimeres ved ordentlige kontrol- og verifikationsforanstaltninger samt sporbarhed og sporing af elektroniske transaktioner afhængigt af tilsynsniveauet fra de relevante myndigheders side.

Konklusion: Retshåndhævende myndigheder anser onlinespil for at være et potentielt attraktivt redskab til at hvidvaske penge, som kræver et moderat niveau af ekspertise og udgør en realistisk løsning. Ligeledes synes onlinespil at tilbyde en prisbillig mulighed for at hvidvaske penge. I denne henseende anses truslen fra hvidvask af penge mod onlinespil som betydelig (niveau 3).

Sårbarhed

Finansiering af terrorisme

Vurderingen af sårbarheden over for terrorfinansiering i relation til onlinespil er ikke blevet anset for at være relevant. I denne henseende er den trussel, der udgøres af terrorfinansieringen, ikke en del af vurderingen.

Konklusion: ikke relevant.

Hvidvask af penge

Vurderingen af sårbarhed over for hvidvask af penge i relation til onlinespil viser følgende

a) risikoeksponering

Risikoeksponeringen mht. onlinespil er karakteriseret ved to komponenter:

- det forhold, at forretningsrelationer ikke foregår ansigt til ansigt (betragtes som højrisiko både i EU-reglerne og i Den Finansielle Aktionsgruppes krav), og
- muligheden for at anvende mindre sporbare betalingsmåder på online platformen (dvs. anonyme/forudbetalte e-penge eller endda virtuel valuta, hvor det er tilladt).

Faktisk giver onlinespil mulighed for aktivitet i hele verden alle dage, døgnet rundt. Det involverer en stor mængde transaktioner og store pengestrømme. Det involverer ikke

fysiske produkter og gør det vanskeligere at opdage noget mistænkeligt. Selvom onlinespil ikke er kontantbaseret, er det tæt forbundet med brugen af andre produkter som e-penge eller virtuelle valutaer, som viser deres eget sæt af risici for hvidvask af penge. Risikoeksponeringen over for anonyme/forudbetalte kort er nu blevet reguleret gennem de begrænsninger, der er indført i det fjerde hvidvaskdirektiv og i den kommende gennemførelse af det femte hvidvaskdirektiv, som i væsentlig grad vil reducere muligheden for at anvende sådanne betalingsmidler. Derudover vil udbydere af vekslingstjenester mellem virtuelle valutaer og fiat-valutaer samt udbydere af virtuelle tegnebøger[108] blive anset for at være forpligtede enheder efter det femte hvidvaskdirektiv. De procedurer kundekendskabsprocedurer, de skal anvende, skulle også skabe mere gennemsigtighed i relation til onlinespil. Det forhold, at onlinespil ikke sker ansigt til ansigt, øger graden af anonymitet, selvom initiativer som eIDAS også skulle bidrage til en delvis begrænsning af de risici, der er forbundet med denne dimension af forretningen ved at gøre det lettere at gennemføre "kend din kunde"-procedurer Desuden har de retshåndhævende myndigheder (herunder EUROPOL) bemærket en øget tendens til oprettelsen af ikke-licenserede spil-websteder, der ikke er omfattet af kundekendskabskrav og krav om journalføring og indberetninger. De bliver ikke revideret af en tilsynsmyndighed. Det kan have stor indvirkning på EU's indre marked, når disse ikke-licenserede spilwebsteder bliver stiftet uden for EU og let kommer i forbindelse med EU-kunder via internettet.

Samtidig skal der også mht. disse sårbarheder tages hensyn til, at der ved onlinespil også kan benyttes bankkonti, hvor kunden allerede er identificeret og underkastet grundlæggende kundekontrol.

b) risikobevidsthed

Bevidsthedsniveauet i onlinespilsektoren skulle være steget, siden sektoren blev omfattet af EU's regler om bekæmpelse af hvidvask af penge, da den blev dækket af kravene om bekæmpelse af hvidvask af penge og af finansiering af terrorisme, indberetningsniveauet for mistænkelige transaktioner er ganske god, og der findes automatiske kontroller. Nogle nationale lovgivninger bestemmer, at midlerne for så vidt angår elektroniske tegnebøger sendes tilbage til spilleren på samme konto. Hertil kommer, at når der anvendes forudbetalte kort, er det generelt kun små beløb, der er tale om.

I store dele af sektoren er der givet undervisning i bekæmpelse af hvidvask af penge til alle medarbejderne i en virksomhed. Medarbejderne bliver også uddannet i de praktiske spørgsmål som f.eks. hvad der kan give mistanke, hvordan det forelægges for den compliance-ansvarlige, og hvordan man tackler problemerne på det operationelle niveau. Repræsentanter for onlinespil operatørerne har bemærket, at de finansielle efterretningsenheder ikke giver feedback vedrørende de rapporter om mistænkelige transaktioner, der indgives, hvilket giver anledning til vanskeligheder for operatørerne i de enkelte tilfælde (hvor det er uklart, om pengene bør udbetales til en spiller, som så på sin side måske kan rejse en sag over for operatørerne) og forhindrer, at der sker forbedringer af praksis vedrørende bekæmpelse af hvidvask af penge i almindelighed. Dette kan endda afholde nogen fra fremtidig rapportering. Der er også en fornemmelse af konflikt med

[108] En enhed, der leverer tjenester til at beskytte private krypteringsnøgler på vegne af deres kunder og at besidde, gemme og overføre virtuelle valutaer

databeskyttelsesreglerne, hvilket kan nedbringe rapporteringsniveauet. De har imidlertid også fremhævet, at de kompetente myndigheder giver risikovurderinger med henblik på at hjælpe forpligtede enheder med at forbedre deres forståelse af risiciene. Mens den samlede risikobaserede tilgang ligger klar, beklager nogle operatører manglen på klare retningslinjer for, hvornår og hvordan de skal bringe deres forpligtelser mht. bekæmpelse af hvidvask af penge og af finansiering af terrorisme i anvendelse. I mange tilfælde er der således uoverensstemmelse mellem de kompetente myndigheders forståelse af risiciene og det realitetstjek, der er foreslået af onlinespiloperatørerne.

c) retsgrundlag og kontroller

Hele sektoren for onlinespil har været omfattet af EU's regler om bekæmpelse af hvidvask af penge siden gennemførelsen af fjerde hvidvaskdirektiv. Men på grund af direktivets principper om mindsteharmonisering kan der stadig være forskelle fra medlemsstat til medlemsstat med hensyn til regulering, tilsyn med sektoren og håndhævelse af reglerne om bekæmpelse af hvidvask af penge og af finansiering af terrorisme.

Nogle operatører, der har licens i én eller flere medlemsstater, tilbyder også spiltjenester i andre medlemsstater uden tilladelse. Derudover driver spilarrangører etableret uden for EU-landende uautoriseret virksomhed i EU (det vil sige uden at have fået licens i et EU-land og dermed uden for EU-kontrol).

Der er nogle tilfælde, hvor onlinespilplatformen befinder sig i én medlemsstat og den e-pengeudsteder, der stille midlerne til rådighed, befinder sig i en anden medlemsstat. Sommetider har platforme licens i ét område, men driver virksomhed i et andet gennem et mellemled (som både kan være et forretningssted og ikke være det). I disse tilfælde finder nogle myndigheder det ikke altid klart, hvor rapporteringen skal finde sted (værtslandets/hjemlandets finansielle efterretningsenheder) og hvor tilsynsvirksomheden bør foregå (værtslandets/hjemlandets tilsynsmyndigheder). Derfor mener kompetente myndigheder og forpligtede enheder, at de eksisterende retsregler ikke altid giver tilstrækkelig klarhed over, hvilken myndighed der er kompetent til at anvende krav vedrørende bekæmpelse af hvidvask af penge og af finansiering af terrorisme.

Der er ingen forpligtelse til gensidig anerkendelse af autorisationer udstedt af medlemsstaterne i Det Europæiske Økonomiske Samarbejdsområde. På grund af de vide skønsbeføjelser, medlemsstaterne har til at regulere spil, herunder onlinespil, og at tilsyn og håndhævelse henhører under de nationale myndigheders område, varierer de eksisterende regler og kontroller.

Konklusion:

Trods adskillige risikobaserede foranstaltninger, som mange online operatører allerede har iværksat (f.eks. uddannelse i bekæmpelse af hvidvask af penge for medarbejdere, kundekendskabskrav og "kend din kunde"-procedurer), er eksponeringen for hvidvask af penge i onlinespil stadig ganske stor, da spillet omfatter vigtige faktorer som , at spillet ikke finder sted ansigt til ansigt, samt store og komplekse mængder af transaktioner og pengestrømme. Selvom der ikke er baseret på kontanter, er det nært knyttet til brugen af e-penge,og digitale og virtuelle valutaer, hvilket f.eks. også øger graden af anonymitet for kunderne. Som det er anerkendt i mange medlemsstater, har onlinespiloperatører udviklet en høj grad af

selvregulering og risikovurdering, også selvom deres samarbejde med de kompetente myndigheder og finansielle efterretningsenheder kunne forbedres. Operatørerne mener, at de ikke får klar vejledning om, hvordan man på den rette måde tager hånd om risiciene, især den manglende tilbagemelding fra finansielle efterretningsenheder om rapporter om mistænkelige transaktioner. I den henseende anses sårbarhedsniveauet over for hvidvask af penge i relation til onlinespil for betydeligt (niveau 3).

Risikobegrænsende foranstaltninger:

1) kompetente myndigheder/kontrolorganer:

- Medlemsstaterne bør forbedre samarbejdet mellem relevante myndigheder (finansielle efterretningsenheder, retshåndhævende myndigheder, politi, sektorbestemte kontrolorganer som tilsynsmyndigheder for spil), så de bedre kan forstå de risikofaktorer, onlinespil indebærer, og yde effektiv vejledning.
- Medlemsstaterne bør sikre løbende samarbejde mellem relevante myndigheder og onlinespiloperatører, som bør fokusere på:
    - styrkelse af kundekendskabskravene og afsløringen af mistænkelige transaktioner og øgning af antallet og kvaliteten af rapporter om mistænkelige transaktioner, især i tilfælde, hvor onlinespilplatforme bruges grænseoverskridende
    - tilrettelæggelse af undervisningsforløb for personale og complianceansvarlige med særligt fokus på risiciene for organiserede kriminelle grupperingers infiltrering eller ejerskab, og løbende revision af risikovurderingerne vedrørende deres produkter/forretningsmodel
    - sikring af, at tilsynsmyndighederne giver klarere vejledning om risiciene vedrørende bekæmpelse af hvidvask af penge og af finansiering af terrorisme, om kundekendskabskrav og kravene til indberetning af mistænkelige transaktioner, samt om, hvordan man konstaterer de mest relevante indikatorer mht. til opdagelse af risici for hvidvask af penge
    - øge bevidstheden hos onlinespiloperatører om nye risici, som kan øge sektorens sårbarhed, f.eks. brugen af anonyme e-penge eller virtuel valuta eller fremkomsten af uautoriserede onlinespiloperatører
    - øge bevidstheden og øge kontrolorganers og de kompetente myndighedernes kapacitet og ekspertise til at vurdere risici i onlinemiljøet og inden for cybersikkerhed og til at opdage og forhindre hvidvask af penge, og i den henseende kunne udnyttelse af ressourcer i fællesskabe med andre medlemsstater (f.eks. organisering af fælles uddannelse) overvejes.
- Medlemsstaterne tilskyndes til at kræve, at de kompetente tilsynsmyndigheder, hvor dette er hensigtsmæssigt, offentliggør en rapport om de sikkerhedsforanstaltninger, onlinespiloperatørerne har gennemført for at begrænse risiciene ved forretningsforbindelser, der ikke foregår ansigt til ansigt (online identifikation og kontroller, overvågning af transaktioner).
- Medlemsstaterne bør sikre, at de finansielle efterretningsenheder giver feedback til onlinespiloperatører om kvaliteten af rapporteringen om mistænkelige

transaktioner og måderne, hvorpå rapporteringen kan forbedres, og om hvordan oplysningerne i rapporten bruges, helst inden for en fastsat tidsperiode.

- Medlemsstaterne bør udvikle standardiserede skabeloner på EU-niveau til rapporter om mistænkelige transaktioner og mistænkelige forhold, som , tager hensyn til spilsektorens særlige karakteristika.
- Medlemsstaterne bør sikre, at særlige sikkerhedsforanstaltninger for forretningsforhold, der ikke foregår ansigt til ansigt, bruges som elektronisk identifikation (E-IDAS identifikation, elektronisk signatur).
- Medlemsstaterne bør sørge for vejledning om samspillet mellem kundekendskabskrav og regler for databeskyttelse og om indberetning.

2) sektoren.

- Medlemsstaterne bør sikre, at onlinespiloperatører løbende arrangerer uddannelsesforløb for personale og complianceansvarlige, som særligt fokuserer på risikoen for organiserede kriminelle grupperingers infiltrering eller ejerskab, og løbende reviderer risikovurderingerne af deres produkter/forretningsmodel. En sådan uddannelse bør gøres obligatorisk for visse grupper af ansatte på et oplysningsniveau, der er passende for deres stilling.
- Medlemsstaterne bør sikre, onlinespiloperatørerne gennemfører systematiske risikobaserede kundekendskabsprocedurer i forhold til vinderne og fremmer en lavere tærskel for gevinster, der er omfattet af kundekendskabskrav (i øjeblikket 2 000 EUR, som det fremgår af artikel 11, litra d), i direktiv (EU) 2015/849).
- Medlemsstaterne bør sikre, at onlinespiloperatører udpeger en ansvarlig på stedet for bekæmpelse af hvidvask af penge, hvis det ikke allerede er sket.
- Medlemsstaterne kunne sikre, at kunderne ikke får lov til at åbne flere konti hos samme operatør (og også forbyde overførsler mellem kundekonti), medmindre kontiene er på forskellige brands, som operatørerne kan linke til. Hvis denne regel brydes, kunne operatøren forbeholde sig retten til at blokere og/eller slette spillerens ekstra konto og overføre alle midlerne til en enkelt konto.
- Medlemsstaterne kunne også fastsætte en forpligtelse til, at spillerens kontonavn skal svare til navnet på det betalingskort eller andre betalingsmetoder, der bruges til at indsætte/hæve midler, og sikre, at spillerens konto ikke kan overdrages, dvs. at det skal være forbudt for spillere at sælge, overdrage eller overføre konti til eller erhverve konti fra andre spillere.

3) Kommissionen:

Kommissionen kunne give vejledning om artikel 11, litra d), mht. gennemførelsen af kundekendskabskrav i forbindelse med "flere operationer, der ser ud til at være indbyrdes forbundne".

NONPROFITORGANISATIONER

1. Indsamling og overførsel af midler via en nonprofitorganisation (NPO)

Produkt

Indsamling og overførsel af midler via en nonprofitorganisation

Sektor

Nonprofitorganisationer

Generel beskrivelse af den pågældende sektor og det/den relevante produkt/aktivitet

NPO'er kan have mange forskellige juridiske former, afhængigt af det land, hvor de er etableret. Financial Action Task Force (FATF) har derfor vedtaget en funktionel definition af en NPO, som anvendes af Europa-Kommissionen i forbindelse med denne supranationale risikovurdering. **Denne definition er "**en juridisk person eller et arrangement eller en organisation, der primært beskæftiger sig med at rejse eller udbetale midler til eksempelvis velgørende, religiøse, kulturelle, uddannelsesmæssige, sociale eller solidariske formål, eller til at udføre andre former for "gode gerninger"".[109]

Der eksisterer en bred vifte af NPO-delsektorer, herunder udviklingsbistand, humanitær bistand, idræt, fortalervirksomhed osv.

For humanitære NPO'ers vedkommende er formålet at redde og bevare livet for mennesker, som er ramt af naturkatastrofer eller menneskeskabte katastrofer, under fuld respekt af den humanitære folkeret og principperne for humanitær indsats (neutralitet, upartiskhed, menneskelighed og uafhængighed[110]). Humanitære NPO'er kan være aktive i og uden for Europa og deltage i forskellige operationelle sammenhænge.

Megen humanitær hjælp ydes i områder, der oplever væbnet konflikt eller anden form for vold, eller tager sig af konsekvenserne af disse. Humanitære organisationer kan også operere i regioner og lande, hvor personer og enheder, der er udpeget som "terrorister", er til stede og sandsynligvis vil fortsætte deres aktiviteter. Den humanitære bistandssektor rummer en lang række organisationer med varierende grader af operationel og organisatorisk kapacitet, og en stor del af NPO'erne modtager institutionelle humanitære

---

[109] Denne definition anvendes i en fortolkende note til henstilling 8:
http://www.fatf-gafi.org/publications/fatfgeneral/documents/plenary-outcomes-june-2016.html#npo
Det bemærkes, at der ikke findes nogen fælles juridisk definition af en NPO i EU, og at deres former og definitioner varierer meget stærkt på nationalt plan. Den Finansielle Aktionsgruppe fokuserer imidlertid på **tjenesteydende organisationer** og indbefatter ikke NPO'er, der beskæftiger sig med meningstilkendegivelser/fortalervirksomhed, i henstilling 8. Henstilling 8 beskæftiger sig kun med risikoen for finansiering af terrorisme i relation til NPO'er, og ikke hvidvask af penge.

[110] Ifølge det humanitære principom upartiskhed, skal humanitær hjælp udelukkende ydes på grundlag af behov, uden diskriminering mellem eller inden for de berørte populationer.

bistandsmidler, herunder fra EU og fra medlemsstater, der står for administrationen af EU-midler. Disse er underlagt en strengt kontraktlig ordning med en høj grad af sikkerhed.[111]

Beskrivelse af risikoscenariet[112]

- NPO'ers kan etableres, eller eksisterende NPO'er kan bruges, til at rejse penge. Kriminelle midler sendes så til NPO'erne og:

  - medsammensvorne NPO'oer kan forsætligt støtte en terrorgruppe eller kriminel organisation

  - lovlige NPO'er kan blive udnyttet af udenforstående

  - lovlige NPO'er kan blive udnyttet af folk i organisationen.

- Kriminelle kan bruge NPO'er til at give penge til lokal terrorvirksomhed eller kan søge at bruge NPO'er til at lette grænseoverskridende finansiering ved at sende penge til områder, hvor NPO'erne arbejder tæt på områder med terroristaktiviteter, og:

  - medsammensvorne NPO'er kan forsætligt støtte en terrorgruppe eller en kriminel organisation

  - lovlige NPO'er kan blive udnyttet af udenforstående

  - lovlige NPO'er kan blive udnyttet af folk i organisationen.

Generel bemærkning

I denne risikovurdering opfattes NPO'er som defineret i FATF-henstilling 8. Risikoscenariet dækker en NPOs indsamling af midler og overførsel af midler fra denne til projektpartnere/modtagere.

Det skal understreges, at en vurdering af hele sektoren er kompleks øvelse på grund af dens samlede mangfoldighed, og fordi hver NPO undersektor involverer et forskelligt niveau af risiko/fare.

Da vurderingen vedrører hvidvask og terrorfinansiering, som påvirker det indre marked og grænseoverskridende aktiviteter, gælder den for indsamling og overførsel af midler i det indre marked samt for indsamling af midler i EU med benblik på overførsel til tredjelande.

[111] EU's humanitære bistandsmidler forvaltes af Europa-Kommissionen og kanaliseres via partnere, herunder NPO'er, som udvælges på grundlag af særlige juridiske, finansielle og operationelle kriterier, og som har underskrevet en rammeaftale om partnerskab. Donorer og NPO'er har det fælles mål at sikre, at hjælpen skal nå de mest trængende og ikke omdirigeres andetsteds hen. Der er en risiko ved at arbejde i miljøer, hvor udpegede terrorgrupper kan være til stede, men denne risiko stammer fra de omgivelser, hvori der arbejdes, og ikke fra den arbejdende enheds juridiske status.

[112] I overensstemmelse med de internationale forpligtelser, som Kommissionen har påtaget sig med henblik på at fremme større effektivitet, gives humanitær bistand i stigende grad som kontantoverførsler. Dette gør det muligt for modtagerne og deres familier at dække deres mest presserende behov med værdighed og fleksibilitet og indfører en slags normalitet i deres splintrede liv. Sådanne pengeoverførsler i forbindelse med humanitære hjælpeaktioner er ikke omfattet af denne vurdering.

Trussel

Finansiering af terrorisme

Vurdering af truslen om terrorfinansiering i relation til NPO'ers indsamling og overførsel af midler viser, at der ikke er tale om en metode, der ofte anvendes af terroristgrupper. Når man ser på antallet af registrerede NPO'er, er det meget få, der er blevet misbrugt. I sjældne tilfælde kan NPO'er imidlertid være infiltreret af terroristgrupper, hvilket kan udgøre en væsentlig trussel, især for så vidt angår finansiering af udenlandske terrorkrigere.

Generelt er indsamling og overførsel af midler gennem NPO'er reguleret af forskellige nationale og nogle gange regionale love. Overholdelse af disse love kræver nogen teknisk ekspertise og involverer forskellige niveauer af gennemsigtighed og ansvarlighed. Due diligence procedurer for NPO registrering, autorisation og adgang til finansielle tjenesteydelser i EU er blevet skærpet. Terrorister, der har som mål at finansiere terroraktiviteter under dække af en NPO er nødt til at forstå disse procedurer, og kravene kan afholde dem fra at bruge en NPO.

Nogle NPO aktiviteter vil kunne indebære en større risiko for så vidt angår kilder til midler (ukendte/kontante/internationale kilder/højrisikolande), typer af aktiviteter eller modtagere (ukendte/højrisikolande/højrisikokunder/brug af uformelle kanaler til at sende penge til udlandet). Risikoen øges, hvis der ikke findes formelle bankkanaler til pengeoverførsler til og fra NPO'er. De vigtigste årsager til brugen af uformelle pengeoverførselssystemer er, at bankerne i stigende grad er blevet uvillige til at levere finansielle tjenesteydelser til NPO'er (en tendens, der kaldes bank derisking) og et fald i korrespondentbankvirksomhed. Risikoen stammer derfor til dels fra finansiel udstødelse. Nye teknologiske værktøjer som crowdfunding- og blockchainsystemer kan misbruges af NPO-sektoren, og kontrolorganerne kan blive nødt til at vurdere og håndtere de dermed forbundne risici. Omvendt kan disse nye værktøjer kan også bruges til at øge sporbarheden af midler.[113]

Arbejdet i humanitære NPO'er kan foregå i områder, der til tider er højrisikable, og hvor ikke-statslige væbnede grupper eller enkeltpersoner, der er udpeget som terrorister, er til stede. De konkrete risici afhænger af forskellige faktorer, f.eks. hvor professionel en NPO er, og forholdene i netop det land, herunder de politiske dynamikker i den pågældende konflikt.

[113] Nogle velgørenheds- og pengeindsamlende organisationer udbytter specifikt muslimske samfund for økonomisk støtte under dække af humanitær bistand, f.eks. til at støtte familier og forældreløse børn efter "martyrer", og til at opføre moskeer og brønde. Der er et stort potentiale for pengeindsamling blandt jihadiske sympatisører. I de fleste tilfælde gives opfordringen til at donere i moskeer, via websteder, web-fora og crowdfunding-platforme, der befinder sig i Europa, og de giver kun få oplysninger om den endelige anvendelse af midlerne, som ofte hæves i kontanter. Nogle få opfordringer til donationer anmodede udtrykkeligt om, at donationer blev givet i bitcoin.

Konklusion: NPO-landskabet er meget varieret. Selvom NPO'er kun har været infiltreret i meget få tilfælde, og at mere konkret viden generelt er nødvendig for at få adgang til midler, der er indsamlet eller overført af NPO'er til finansiering af terroristvirksomhed anses trusselsniveauet for terrorfinansiering som betydeligt (niveau 3).

For så vidt angår NPO'er, der modtager institutionelle midler bl.a. fra EU eller de medlemsstater, der har ansvaret for administrationen af EU-midler, anses trusselsniveauet for mindre betydeligt (niveau 1).

Hvidvask af penge

Vurderingen af truslen om hvidvask af penge i relation til indsamling og overførsel af midler gennem NPO'er er blevet vurderet i forbindelse med terrorfinansieringssystemer i relation til indsamling og overførsel af midler gennem NPO'er med henblik på at finansiere terroraktiviteter. I den sammenhæng er truslen om hvidvask af penge ikke blevet undergivet en særskilt vurdering.[114]

Konklusion: I denne henseende anses trusselsniveauet over for hvidvask af penge for i moderat grad betydeligt (niveau 2).

For så vidt angår NPO'er, der modtager institutionelle midler bl.a. fra EU eller de medlemsstater, der har ansvaret for administrationen af EU-midler, anses trusselsniveauet for mindre betydeligt (niveau 1).

Sårbarhed

Finansiering af terrorisme

Risikovurderingen mht. sårbarheden over for terrorfinansiering gennem NPO'ers indsamling og overførsel af midler er beskrevet nedenfor.

Generelle bemærkninger

En risikoanalyse af NPO-sektoren fra et sårbarhedsperspektiv er vanskelig på grund af sektorens mangfoldighed.

a) risikoeksponering

[114] I en nylig sag var der tale om en organiseret kriminel gruppering, der bleve ledet af en katolsk prælat med officiel residens i Rom, som samtidig tilbragte det meste af tiden med at rejse verden rundt og tilbyde andre organiserede kriminelle grupperinger hvidvask af penge: Prælaten og hans partnere var i stand til at tilbyde deres "kunder" velgørenhedsorganisationers bankkonti som juridisk instrument til at flytte midler rundt i verden uden at vække mistanke. De italienske myndigheder havde mistanke om, at de midler, som blev kanaliseret gennem disse bankkonti, kom fra skatteunddragelse, svig i samhandelen inden for Fællesskabet og momssvig samt alvorlige forbrydelser (som handel med narkotika).

Som nævnt ovenfor kan nogle NPO'er være udsat for risici. Mindre beløb foreligger i kontanter, hvilket gør det vanskeligt for medlemsstaternes retshåndhævende myndigheder og finansielle efterretningsenheder at opspore kilderne til finansiering og overførsler til udlandet. Risikoen øges også, når der ikke findes officielle bankkanaler til NPO-pengeoverførsler. Som det blev understreget tidligere, benyttes uformelle pengeoverførsler normalt alene, fordi bankerne i tiltagende grad er blevet uvillige til at levere finansielle tjenesteydelser til NPO'er(en tendens der kaldes bank derisking), og på grund af et fald i korrespondentbankvirksomheden. Risikoen stammer derfor til dels fra finansiel udstødelse.

Arbejdet i humanitære NPO'er kan foregå i områder, der til tider er højrisikable, og hvor ikke-statslige væbnede grupper eller personer, der er udpeget som terrorister, er til stede. De konkrete risici afhænger imidlertid af forskellige faktorer, f.eks. hvor professionel en NPO er, og forholdene i netop det land, herunder de politiske dynamikker i den pågældende konflikt.

b) risikobevidsthed

Risikobevidstheden er på vej op i NPO-sektoren. NPO'erne foretager deres egne risikovurderinger, der tager hensyn til geografisk beliggenhed, typen af aktivitet, organisationens hidtidige engagement i området og relationer til andre sektorer. De er begyndt at udvikle kontrol- og due diligence-foranstaltninger for overførsel og indsamling af midler (sanktionslister, screening og ændringer af straffelovgivningen har alt sammen hjulpet). Sektoren er også i færd med at udvikle peer-learning-udvekslinger om due diligence-praksis, åbenhed og ansvarlighed og risikostyring samt bevidstgørelse om terrorfinansiering. NPO'er (navnlig de humanitære) bliver mere og mere bevidste om risici, navnlig i tilfælde, hvor de finansielle transaktioner finder sted uden for det finansielle system. Der er også større samarbejde og opsøgende arbejde over for banksektoren med henblik på at facilitere sikre og regulerede kanaler for legitime humanitære sager. Det øger gennemsigtigheden og medvirker til at skærme NPO'er mod terroristers misbrug af dem og tillader samtidig, at der ydes humanitær bistand til de regioner, der har størst behov.

Sektoren er også engageret i selvregulering, og der er ved at blive udviklet adfærdskodekser i fundraising- og tjenesteydelsessektorerne, som ofte omfatter styring, rapportering, kontrol med midlernes anvendelse og principper som "kend din donorer" og "kend dine modtagere".

Som svar på donorernes krav og for at sikre, at bistanden når frem til de tiltænkte modtagere, investerer NPO'er i stigende grad i stærke compliance- og interne revisionsfunktioner samt kapacitetsopbygning inden for relevante emner som bekæmpelse af bestikkelse og korruption. NPO'er, der modtager humanitære bistandsmidler fra EU og fra de medlemsstater, der er ansvarlige for administrationen af EU-midlerne, er underlagt en strengt kontraktlig ordning med et antal sikkerhedsforanstaltninger.

NPO-fællesskabet er livsvigtigt for ydelse af humanitær bistand i hele verden. For at beskytte de legitime mål for denne type bistand kan der være behov for mere information om terrorfinansieringsrisici i NPO-sektoren for at øge risikobevidstheden.

c) Retsgrundlag og kontroller

NPO-sektoren er reguleret på nationalt og i nogle tilfælde regionalt plan (civilretligt og skatteretligt). Der findes ingen centrale organisatoriske rammer, og reglerne er ikke harmoniseret på EU-plan. NPO'er er ikke direkte omfattet af reglerne om bekæmpelse hvidvask af penge og af finansiering af terrorisme på EU-plan, men er indirekte omfattet via forpligtelserne for de enheder, der har NPO'er som kunder, og via medlemsstaternes forpligtelser vedrørende reelle ejerstrukturer. Betingelser for registrering og drift af NPO'er varierer fra land til land. Kompetente myndigheder hælder mod det synspunkt, at de eksisterende kontroller af indsamling og overførsel af midler inden for EU er ret grundige. Nogle svagheder blev nævnt vedrørende overførsel af midler til steder uden for EU.

Ud over kravene vedrørende bekæmpelse af hvidvask af penge og af finansiering af terrorisme er humanitære NPO'er styret af principperne om medmenneskelighed, upartiskhed, neutralitet og uafhængighed. Derudover er bestemte kategorier af humanitære NPO'er, især dem, der er blevet vurderet af Europa-Kommissionen, underlagt løbende kontrol i partnerskabs levetid og de konkrete humanitære indsatser. Disse kontroller, der omfatter detaljerede rapporter om indsatser, forpligtelser vedrørende journalføring og regelmæssig revision både i hovedkvarteret og i marken, rækker ud over de strikte støtte- og egnethedskriterier, der er kontrolleret gennem en grundig udvælgelsesproces forud for undertegnelsen af rammeaftalen om partnerskab.

I næsten alle medlemsstater er NPO'er underlagt en form for statsligt tilsyn, det være sig af skattemyndighederne, kontrolorganer inden for velgørenhed eller andre former for tilsynsmyndigheder. Mht. de juridiske rammer er det nødvendigt at finde en balance mellem terrorbekæmpelsesdagsordenen og de legitime mål for humanitære NPO'er.[115]

<u>Konklusion:</u> NPO'ernes risikoeksponering er påvirket af arten af deres aktiviteter, og der er varierende grader af risikobevidsthed. De relevante juridiske og skattemæssige regler og national praksis er mangfoldig, men synes at give kontrol, og man bør anerkende den konkrete indretning af den humanitære sektor som beskrevet ovenfor. I denne henseende anses sårbarhedsniveauet over for finansiering af terrorisme for i <u>moderat grad betydeligt</u> (niveau 2).

For så vidt angår NPO'er, der modtager institutionelle midler bl.a. fra EU eller de medlemsstater, der har ansvaret for administrationen af EU-midler, anses trusselsniveauet for <u>mindre betydeligt</u> (niveau 1).

Hvidvask af penge

Vurderingen af truslen om hvidvask af penge i relation til indsamling og overførsel af midler gennem NPO'er er blevet vurderet i forbindelse med terrorfinansieringssystemer i relation til indsamling og overførsel af midler gennem NPO'er med henblik på at finansiere terroraktiviteter. I den sammenhæng er truslen om hvidvask af penge ikke blevet undergivet en særskilt vurdering.

[115] For eksempel indeholder præamblen til Europa-Parlamentets og Rådets direktiv (EU) 2017/541 af 15. marts 2017 om bekæmpelse af terrorisme og om erstatning af Rådets rammeafgørelse 2002/475/RIA og ændring af Rådets afgørelse 2005/671/RIA en undtagelse for humanitære aktioner, der gennemføres af upartiske humanitære organisationer.

<u>Konklusion</u>: I denne henseende anses niveauet af sårbarhed over for hvidvask af penge for i <u>moderat grad betydeligt</u> (niveau 2).

For så vidt angår NPO'er, der modtager institutionelle midler bl.a. fra EU eller de medlemsstater, der har ansvaret for administrationen af EU-midler, anses sårbarhedsniveauet også for <u>mindre betydeligt</u> (niveau 1).

Risikobegrænsende foranstaltninger:

<u>1) Kommissionen</u>

- Fortsat samarbejde med NPO'er, der modtaget EU-støtte, om de relevante fællesskabsretlige regelsæt, samt om hvordan man kan identificere risici og opfylde kravene til rettidig omhu.
- Fortsat deltagelse i udveksling af synspunkter med mange interessenter inden for alle faggrene, herunder den finansielle sektor, der er involveret i forretninger med NPO'er.
- Fortsat samarbejde med og vejledning til humanitære NPO'er, der modtager EU-støtte, om risikoen for hvidvask af penge og terrorfinansiering samt kravene til rettidig omhu, idet der skal tages hensyn til bedste praksis hos humanitære organisationer.

<u>2) kompetente myndigheder</u>

- Medlemsstaterne bør sikre en bedre NPO-deltagelse i nationale risikovurderinger og udarbejde informations- og bevidstgørelsesprogrammer udformet med henblik på at modvirke risikoen for misbrug, og bør støtte NPO'erne gennem bevidsthedsskabende materiale til NPO'erne (såvel på nationalt plan som på EU-plan).
- Medlemsstaterne bør også yderligere analysere de risici, NPO-sektoren står overfor.

1. Investeringer i professionel fodbold og transfer-aftaler vedrørende professionelle fodboldspillere

Produkt
Investeringer i og transferaftaler vedrørende professionelle fodboldspillere

Sektor
Professionel sport

Generel beskrivelse af den pågældende sektor og det/den relevante produkt/aktivitet

Sportsbranchen er en af de mange sektorer, som kan være attraktive for kriminelle til hvidvask af penge og fortjener mere opmærksomhed på grund af dens sociale og kulturelle betydning, de store beløb, der præger pengetransaktionerne, samt stigningen i antallet af involverede personer.

Ligesom mange andre forretningsområder er sport og spil blevet misbrugt af kriminelle til at hvidvaske penge og hente illegale indtægter. Som i kunstverdenen er kriminelle i sportsverdenen ikke altid er motiveret af økonomisk vinding. Social prestige, at optræde sammen med berømtheder samt udsigten til at få med autoritetspersoner at gøre kan også tiltrække private investorer med tvivlsomme hensigter.

Beskrivelse af sektoren

Fodbold spilles af mere end 265 millioner mennesker i verden. Ifølge Fédération Internationale de Football Association (FIFA) er der 38 millioner behørigt registrerede professionelle spillere og omkring 301.000 klubber. Fodbold har oplevet ekstraordinær vækst siden begyndelsen af 1990'erne som følge af flere tv-rettigheder og sponsorater. Markedet for professionelle spillere har oplevet en hidtil uset internationalisering med stadigt større overførsler af ressourcer på tværs af kontinenter.

I fodbold kan billedkontrakter, reklamekontrakter og sponsorkontrakter være værktøjer for kriminel praksis, især skatteunddragelse, idet de penge, der er aftalt ifølge disse kontrakter, almindeligvis overføres til konti tilhørende virksomheder i tredjelande. Dette medfører en alvorlig risiko for svig, da det er let at undgå at angive de modtagne penge, også selvom dette kræver brug af tredjeparter i forbindelse med forskellige økonomiske transaktioner.

Den mest almindelige form for kontantbetalinger sker til andre lande, som tillader, at det endelige bestemmelsessted for betalingerne skjules. Billedrettigheder bruges også til at skjule de beløb, der faktisk bliver betalt til spillerne.

Hertil kommer, at gambling er direkte forbundet med fodbold gennem indsatser på spil og kampe.

Relevante aktører

Fodbold administreres af FIFA, som er baseret i Zürich, Schweiz. Det er et privat selskab, der er omfattet af schweizisk lov, og som kontrollerer hele fodboldverdenen gennem et forbundssystem. FIFA har kompetence til at fremme og udvikle fodbold i hele verden. Hvert land har en samarbejdspartner, der skal følge FIFA's regler og love. FIFA har et klart ansvar for at sikre sportssektorens integritet og omdømme.

Derfor godkendte FIFA i 2004 et sæt etiske regler (senere revideret flere gange),[116] der gav hjemmel til oprettelsen af det nye etiske udvalg, hvoraf det er et centralt medlem. Som led i sit arbejde for at styrke etikken i sporten tilbyder FIFA teknisk bistand gennem Early Warning Systems GmbH, en virksomhed, der er oprettet direkte med henblik på at overvåge sportsvæddemål og at forebygge negative konsekvenser af uetisk adfærd i fodboldkampe.

Som tilsynsorgan, som nøje overvåger fodboldsektoren, hvilket omfatter dets administration af klubber, der ofte har gæld, som er uforenelig med deres faktiske finansieringsevne, består FIFA af seks forbund: Asian Football Confederation i Asien og Australien (AFC), Confédération Africaine de Football (CAF), Confederation of North, Central American and Caribbean Association Football (CONCACAF), Confederation Sudamericana de Fútbol (CONMEBOL), Oceania Football Confederation (OFC) og Union of European Football Associations (UEFA). UEFA er langt det største af de seks kontinentale forbund.

FIFA bruger Transfer Matching System (TMS) til at tilvejebringe information om international transfer af spillere, hvilket tidligere var begrænset til forretningsmæssige interessenter. Gennem dette system registreres mere end 30 typer oplysninger, online, spillerhistorie, klubber involveret i forretningen, betalinger, værdier, kontrakter og andre slags oplysninger.

De nationale forbund har et ansvar for at opretholde disciplinen samt koordinere og administrere fodbolden i deres respektive lande. Disse nationale organisationer betragtes som de centrale kontrolorganer i deres lande, men de skal stadig overholde de konkrete regler, som FIFA fastsætter. De nationale forbund kan igen opdeles i regionale enheder. Klubberne anses for celler, som er grundstammen i de regionale enheder.

I løbet af FIFA's historie har forbundets vedtægter undergået mange ændringer, som har moderniseret vedtægterne og gjort dem til et stadig mere omfattende værk. FIFA fastlægger de grundlæggende love for international fodbold, heriblandt en række regler omkring transferer, ulovlig brug af stoffer og en lang række andre emner. Disse vedtægter blev godkendt på FIFA's 59. kongres i Nassau, Bahama-øerne, den 3. juni 2009 og trådte i kraft den 2. august samme år. Ændringer af FIFA's vedtægter kan kun ske på en kongres,

[116] Den 12. august 2018 trådte FIFA's nye Code of Ethics (CoE) i kraft.

og det kræves, at der er et 75 % flertal af nationale forbund til stede og med ret til at deltage i afstemningen. Dette gør, at FIFA vedtægter og gennemførelsesregler svarer til en forfatning for det styrende organ for international fodbold.

Beskrivelse af risikoscenariet

Det første dokument fra EU, der anerkendte idrættens betydning, blev offentliggjort i juli 2007 (EU's Hvidbog om idræt).[117] Det hedder heri: "Idrætten er dog også stillet over for nye trusler og udfordringer i det europæiske samfund, f.eks. det kommercielle pres, udnyttelsen af unge sportsudøvere, doping, racisme, vold, korruption og hvidvask[...] af penge". Mange faktorer har medført brug af ulovlige midler i fodbold, ikke mindst dens komplekse organisation og manglende gennemsigtighed.

I marts 2013 vedtog Europa-Parlamentet en beslutning ommatchfixing og korruption inden for sporten.[118] Dette blev fulgt op af en beslutning den 11. juni 2015 omafsløringer af korruption på højt niveau i FIFA[119]og en beslutning den 2. februar 2017 om en integreret tilgang til sportspolitikken: god forvaltning, tilgængelighed og integritet.[120] I plenarmødet i juli 2016 stillede CULT-udvalget en mundtlig forespørgsel til Kommissionen om matchfixing og anmodede om et fuldt tilsagn om at ratificere Europarådets konvention om manipulation af idrætskonkurrencer.[121] Kommissærens svar understregede Kommissionens støtte til konventionen som et værdifuldt værktøj i kampen mod matchfixing, da den udgør et solidt grundlag for paneuropæisk koordinering og samarbejde i den kamp. Samarbejde mellem medlemsstaterne og institutionerne er imidlertid nødvendig for at sikre, at konventionen træder i kraft i EU.

Social status er også en faktor, der fremmer tiltrækningskraften og fører til, at der investeres store summer penge uden synligt eller forklarligt økonomisk udbytte eller gevinst, bortset fra den sociale prestige, der følger af at investere i professionel sport. Den popularitet, der er forbundet med professionel idræt og især professionel fodbold, kan være et redskab for lovovertrædere til at skabe legitimitet omkring sig ved at optræde side om side med berømtheder, virksomhedsledere eller autoritetspersoner.

Fodbold er en yderst relevant kandidat til studier på grund af dens hurtige transformation fra en populær sport til en global industri med stor økonomisk betydning. I betragtning af

---

[117] *Hvidbog om idræt*; Europa-Kommissionen, Bruxelles, 11.7.2007, COM(2007) 391 final.

[118] Europa-Parlamentets beslutning af 14. marts 2013 om matchfixing og korruption inden for sporten (2013/2567(RSP)). Kan ses på: https://eur-lex.europa.eu/legal-content/DA/TXT/?uri=CELEX%3A52007DC0391

[119] Europa-Parlamentets beslutning af 11. juni 2015 om de seneste afsløringer af korruption på højt niveau i FIFA (2015/2730(RSP). Kan ses på: Www.europarl.europa.eu/sider/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2015-0233+0+DOC+XML+V0//DA

[120] Europa-Parlamentets beslutning af 2. februar 2017 om en integreret tilgang til sportspolitikken: god forvaltning, tilgængelighed og integritet. Kan ses på: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=DA&reference=P8-TA-2017-0012

[121]**Konventionen om manipulation af idrætskonkurrencer (Macolin-konventionen)** blev åbnet for undertegnelse den 18. september 2014 på Europarådets 13. konference for ministre med ansvar for sport i Macolin, Schweiz: https://www.coe.int/en/web/sport/about-the-convention-on-the-manipulation-of-sports-competitions

dets sociale betydning har den været et middel til formidling af kulturelle og universelle værdier.

Mange sager har vist, at fodboldbranchen har været præget af ulovlig praksis, herunder hvidvask af penge, korruption og narkotika.

Manglende gennemsigtighed vedrørende transfer af spillere og de reelle ejere eller ledere af fodboldklubber kan føre til, at branchen bliver domineret af en håndfuld mennesker og giver anledning til alvorlig bekymring med hensyn til forebyggelse og bekæmpelse af hvidvask af penge.

Ligeledes er anvendelsen af personer, der ikke er professionelle i finansverdenen, f.eks. familiemedlemmer, advokater, konsulenter og regnskabskyndige som middel til at oprette strukturer til at flytte ulovlige midler også blevet observeret af Den Finansielle Aktionsgruppe (FATF). Den betaling, der er stipuleret i sådanne billedkontrakter (for udnyttelse af en spillers personlige fremtræden som en del af en omfattende reklamekampagne) bliver ofte overført til konti tilhørende virksomheder i tredjelande med alvorlig risiko for svig. Reklame- og sponsoraftaler kan også anvendes til hvidvask af penge. Organiseret kriminalitet kan sponsorere idræt og skabe en bro til lovlige forretninger. Den mest almindelige form for betalinger involveret steder placeret i udlandet, altid som en måde, hvorpå mak kan skjule den sidste destination.

Desuden er FIFA-data hverken offentlige eller lette at skaffe, og ikke-schweiziske myndigheder vil være nødsaget til at anmode om internationalt retligt samarbejde, da FIFA har hovedkontor i Schweiz.

Trussel

Finansiering af terrorisme

Vurderingen af truslen om terrorfinansiering, der kommer fra indsamling og overførsel af midler inden for fodboldsektoren, viser, at denne metode til finansiering af terrorisme ikke bruges ofte af terrorgrupper. Der findes ingen kendte tilfælde af terrorfinansiering via penge, der har bevæget sig gennem fodboldsektoren.

Konklusion: I denne henseende anses trusselsniveauet fra terrorfinansiering i relation til fodbold for at være i moderat grad betydeligt (niveau 2).

Hvidvask af penge

I nogle medlemsstater undersøger myndighederne fodboldklubber i forbindelse med bekymringer for, om sektoren bliver brugt til at vaske sorte penge, og at klubberne underrapporterer mistænkelig adfærd.[122]

[122] https://kyc360.com/news/uk-football-clubs-in-live-money-laundering-investigations/

Metoder

De organiserede kriminelle grupperingers fremgangsmåder kan illustreres gennem adskillige nylige eksempler:

- I maj 2016 sprængte det portugisiske politi (Polícia Judiciária) med støtte fra Europol under Operation *Matrioskas* en tværnational organiseret kriminel gruppering, der især bestod af russiske statsborgere, og som var fokuseret på hvidvask af penge gennem fodbold. Dette kriminelle netværk, der har været aktivt i hvert fald siden 2008, menes at være en celle i en stor russiske mafia-klan, der har det direkte ansvar for hvidvask af adskillige millioner euro i mange EU-lande, hvoraf de fleste menes at stamme fra mangeartede kriminelle aktiviteter, der har fundet sted uden for EU-området.

  Grupperingens kendte fremgangsmåde var at finde EU-fodboldklubber i økonomiske vanskeligheder, derpå infiltrere dem med sponsorer, der kunne sørge for tiltrængte kortsigtede donationer eller investeringer.

  Efter at have vundet tillid gennem donationer iscenesætter disse velgørere købet af klubberne. Køb af de pågældende klubber faciliteres af personer, der fungerer som stråmænd for uigennemsigtige og sofistikerede netværk af holdingselskaber, der altid ejes af skuffeselskaber registreret i udlandet og i højrisikotredjelande. Som følge heraf forbliver de reelle ejere og dem, der i sidste ende kontrollerer klubben, uidentificerede, hvilket også gælden den sande oprindelse af de midler, der blev brugt til at købe den.

  Når klubberne er kommet under den russiske mafias kontrol, muliggør de omfattende finansielle transaktioner, det grænseoverskridende pengestrømme og den mangelfuld ledelse, at de bliver brugt til at vaske sorte penge hvide (som regel via over- eller under-værdiansættelsen af spillere på transfermarkedet og handler med tv-rettigheder) og til væddemålsaktiviteter (både til at generere ulovligt udbytte gennem matchfixing eller gennem ren hvidvask af penge). Ved hjælp af denne metode foretog den kriminelle gruppe først en række donationer til og investeringer i en klub, der havde spillet i den øverste portugisiske fodboldliga, indtil den fik økonomiske problemer i 2012, hvor den røg ned i lavere divisioner. I juli 2015 købte gruppen derefter klubben.

  Den politimæssige efterforskning gik i gang pga. opdagelse af kraftige fareindikatorer i forhold til de mistænkte. Især opstod der mistanke på grund af de mistænktes høje levestandard, hvor de benyttede meget værdifulde aktiver registreret i tredjeparters navne (brug af stråmænd). De importerede store mængder kontanter fra Rusland til Portugal i strid med EU's kontantregler (brug af pengekurerer), og oprettede og brugte uigennemsigtige net af skuffeselskaber, som tjente til at skjule identiteten af deres ejere.

  Siden juli 2015 er der samlet klare beviser for, at denne gruppe kriminelle fungerer som en kriminel sammenslutning, der deltager i hvidvask af penge, skattesvig, korruption og forfalskning af dokumenter og samtidig planlægger forskellige former for transnational kriminalitet.

- Europæiske fodboldklubber, som kriminelle organisationer har erhvervet, kan yderligere bruges til at hvidvaske penge gennem væddemålsaktiviteter i fixede fodboldkampe.
- Idrætskorruption og matchfixing er ofte udført af kriminelle netværk med forbindelse til narkotikahandel, ulovlig tobakssmugling og indbrud.
- En organiseret kriminel gruppering havde oprettet forskellige websteder som del af en onlinebetting platform, der brugtes til at placere indsatser på manipulerede sportsbegivenheder, som fandt sted i mange europæiske lande. Lovovertræderne er mistænkt for at være involveret i forsøg på at fixe professionelle fodboldkampe i blandt andre lande Serbien, Nordmakedonien og Tjekkiet. De organiserede kriminelle, der står bag disse aktiviteter, har tidligere satset primært på det asiatiske marked, hvor de var sikret en betydelig økonomisk gevinst ved at kende slutresultatet af kampene. Ringen udviklede synergier med andre større kriminelle grupperinger i forskellige lande for at kunne investere penge tjent på anden alvorlig kriminalitet, herunder narkotikahandel.

<u>Konklusion</u>: I denne henseende anses trusselsniveauet fra hvidvask af penge mod fodbold for at være betydeligt (niveau 3).

Sårbarhed

Finansiering af terrorisme

Vurderingen af sårbarhed over finansiering af terrorisme i relation til professionel fodbold viser følgende:

a) risikoeksponering

Som det er anført ovenfor, er der en iboende risiko forbundet med fodboldklubber og fodbold-relaterede aktiviteter, hvor en del af midlerne betales med kontanter, hvilket gør det vanskeligt at spore kilden til midlerne, men også til overførslerne (når de sendes til udlandet) fra de retshåndhævende myndigheders og finansielle efterretningsenheders synsvinkel

b) risikobevidsthed

Fodboldsektoren har en central organisatorisk ramme, men regler, der finder anvendelse på sektoren, er ikke harmoniseret på EU-plan og varierer fra den ene medlemsstat til den anden. Sektorens centraliserede organisation forekommer at være begrænset med hensyn til myndighedernes muligheder for at yde effektiv rådgivning eller bistand. Risikobevidstheden er voksende i sektoren.

c) retsgrundlag og kontroller

Sektoren er ikke omfattet af reglerne om bekæmpelse af hvidvask af penge og af finansiering af terrorisme på EU-niveau. Dækning med regler om bekæmpelse af hvidvask af penge og af finansiering af terrorisme er overladt til medlemsstaternes skøn. De eksisterende krav vedrørende bekæmpelse af hvidvask af penge og af finansiering af

terrorisme kan ikke nødvendigvis anses for tilstrækkelige til at tage hånd om sektorens særlige behov, og de eksisterende kontroller varierer afhængigt af medlemsstaten.

Konklusion: I denne henseende anses sårbarhedsniveauet over for terrorfinansiering i relation til professionel fodbold for at være i moderat grad betydeligt/betydeligt (niveau 2/3).

Hvidvask af penge

Vurderingen af sårbarhed over for hvidvask af penge i relation til professionel fodbold viser følgende:

a) risikoeksponering

FIFA's forsøg på at få oplysninger gennem Transfer Matching Systemet har indtil nu været effektivt, men det er ikke nok. Det er et afgørende værktøj til at indhente oplysninger om international transfer af spillere, som tidligere var begrænset til kun at omfatte forretningsmæssige interessenter. Men FIFA's indsatsen, som undertiden fokuserer på rent kommercielle og private interesser, bør ikke erstatte myndighedernes arbejde.

Der bør fastsættes visse forpligtelser, som at kræve af klubber, forbund og forbundssammenslutninger, – og dem, der yder rådgivning, revision, bogføring og konsulentydelser på dette område – at de underretter de finansielle efterretningsenheder om mistænkelige transaktioner. Klubber anvendes ifølge FATF bevidst til at hvidvaske penge, og derfor skal der gøres mere. FIFA-data er ikke offentlige og er vanskelige at skaffe, og derfor vil myndighederne være tvunget til at anmode om internationalt retligt samarbejde for at få adgang til dataene, da FIFA har hovedkontor i Schweiz.

b) risikobevidsthed

Ud over betydningen af at indsamle oplysninger, er det af afgørende betydning for myndighederne at opspore aktiver, der stammer fra kriminelle aktiviteter inden for sport og spil.

FIFA's indsats alene er ikke nok til at forhindre ulovlig praksis. Foreninger, forbudt og forbundssammenslutninger skal gå ind i arbejdet og etablere ordentlige referencer eller vejledninger inden for fodbold, og yde den nødvendige støtte til klubberne gennem faglig uddannelse med henblik på at gøre det lettere at rapportere mistænkelige transaktioner.

c) retsgrundlag og kontroller

Tavshedspligt kan ikke påberåbes som grundlag for at undlade indberetning af mistænkelige aktiviteter, hvilket følger af FATF's henstilling nr. 9. Faktisk er pligten for professionelle, der ikke er tilknyttet den finansielle sektor, ligeledes beskrevet i FATF's henstilling nr. 18, 21 og 22, et vigtigt redskab til at bekæmpe lederes misbrug af god praksis i forbindelse med ansættelse af spillere. Den lovgivning, der går ind for autonomi i organiseringen og driften af sportsorganisationer, bør ligeledes kræve en effektiv finansiel og administrativ gennemsigtighed og beskrive, hvorledes lederne hæfter civilretligt og strafferetligt.

Konklusion: sektoren er i øjeblikket sårbar over for hvidvask af penge. Sektorens bevidsthedsniveau mht. risiciene for hvidvask af penge synes at være højere end for terrorfinansiering, og sektorens evne til at sørge for at afsætte ressourcer og uddannelse på dette område er stadig temmelig lille. De gældende retsregler har øget de kontroller, som anvendes i sektoren, men disse er fortsat utilstrækkelige. I den henseende anses af sårbarhed over for hvidvask af penge i relation til professionel fodbold for i moderat grad betydelig/betydelig (niveau 2/3).

Risikobegrænsende foranstaltninger:

Europa-Parlamentet har opfordret medlemsstaterne til at indføre forbrydelsen sportssvig.[123] Derudover godkendte FIFA's eksekutivkomité i 2014 reglerne om arbejde med formidlere.[124]

Bilaget til Kommissionens beslutning om en ordning for samarbejde mellem Europa-Kommissionen og Det Europæiske Fodboldforbund (UEFA)[125] omtaler udtrykkeligt ønsket fra begge parters side om at undgå, at fodboldsektoren udnyttes til hvidvask af penge. UEFA har forpligtet sig til at engagere sig i denne proces for at hjælpe Kommissionen med at vurdere risiciene for hvidvask af penge i fodboldsektoren.

Medlemsstaterne bør ligeledes blandt andet overveje:

- at fastsætte, hvordan spilleragenter (herunder fysiske personer eller juridiske enheder, der fremmer, formidler, handler, lejer eller forhandler atleternes transferrettigheder) har pligt til at indberette mistænkelige transaktioner. Enkeltpersoner, virksomheder, foreninger, forbund, sammenslutninger af forbund og klubber, der er involveret i af fremme, forhandle, markedsføre eller handle med atleter bør også være omfattet af dette krav i forbindelse med forhandlinger
- at kræve, at fodboldklubberne opbevarer alle kontrakter og relaterede formidlingskontrakter i mindst 5 år
- at kræver fuld identifikation af investorer, også selvom selskaber i landet repræsenterer dem
- at stille større krav til kontrol og registrering af oprindelsen af kontohavere og modtagerne af de penge, der overføres til skattely. Der bør udarbejdes yderligere mekanismer i et forsøg på at få tredjelande til at fremkomme med alle oplysninger til tiden, når der anmodes om det
- at tilbyder undervisning til klubber og transferagenter i forbund og sammenslutninger af forbund og enhver anden kontrolinstans, med det formål at styrke deres roller

[123] Europa-Parlamentets beslutning af 23. oktober 2013 om organiseret kriminalitet, korruption og hvidvaskning af penge: henstillinger om foranstaltninger og initiativer (endelig betænkning) (2013/2107(INI)), EUT C 208 af 10.6.2016, s. 89. Kan ses på: https://eur-lex.europa.eu/legal-content/DA/TXT/?uri=CELEX%3A52013IP0444

[124] https://www.fifa.com/about-fifa/who-we-are/news/fifa-executive-committee-approves-regulations-working-with-intermediarie-2301236

[125] Europa-Kommissionen, Bruxelles, 19.2.2018, C(2018) 876 final.

- at kræve af klubber, forbund og sammenslutninger af forbund, at de under trussel om sanktioner overholder Registration of National or International Players Transfers. De skal give fuldstændige oplysninger om transaktionen og nærmere redegøre for dens finansielle opbygning og vedhæfte agentens kontrakt og legitimationsbevis for agenten og spilleren til transferaftalen mellem købere og sælgere
- at indføre en forpligtelse til at gennemføre en uafhængig revision i idrætsforbundene og sammenslutninger af forbund.

Særligt for så vidt angår agenter bør medlemsstaterne:

- kræve, at personer, der fungerer som agenter for atleter, selv slægtninge eller advokater, får en licens med henblik på at undgå den manglende gennemsigtighed i forbindelse med deres aktiviteter
- regulere retsgrundlaget for fodboldagenter med henblik på at inddrag al handel uden for klubberne
- kræve, at spilleragenter skal have licens, så der bliver større gennemsigtighed i deres handler
- regulere og overvåge alle aktiviteter udøvet af spilleragenter for at sikre, at de har den nødvendige licens eller autorisation
- etablere retlige begrænsninger for at drive forretning som spilleragent og kræve, at agenter bliver registreret med et detaljeret CV i en kontrolinstans ud over FIFA
- blokere alle med straffedomme og dem, som har tabt civile sager angående svig, skatteunddragelse eller andet civilretligt ansvar på statsligt, kommunalt eller føderalt plan
- kræve, at agenter informerer alle kunder om deres kontrahenter.

FRIHANDELSZONER

1. Frihavne

Produkt

Frihavne

Sektor

Frihandelszoner, frizoner – told, direkte beskatning

Generel beskrivelse af den pågældende sektor og det/den relevante produkt/aktivitet

Frihandelszoner er en type særlig økonomisk zone, dvs. et område, hvor forretnings- og handelslovgivningen er anderledes end i resten af landet. I en frihandelszone eller i en særlig økonomisk zone kan varer landes, opbevares, behandles, fremstilles eller omformes og genudføres i henhold til særlige toldregler og generelt uden at blive pålagt told. Frihandelszoner er normalt organiseret omkring store havne, internationale lufthavne og landegrænser – områder med mange geografiske fordele for handel.

Frihandelszoner er også kendt som **frizoner,** et toldarrangementet der bliver brugt i vidt omfang over hele verden til at lette handelen. Der er regler om dem i Kyoto-konventionen (specifikt bilag D), som EU og 115 andre parter har undertegnet. I den i 1999 reviderede Kyoto-konvention defineres de som "en del af en aftaleparts territorium, hvor alle indførte varer for så vidt angår importafgifter og skatter generelt anses for at befinde sig uden for toldområdet".

EU-toldkodeksen indeholder også bestemmelser om frizoner.[126] En EU-medlemsstat kan udpege en del af sit eget toldområde som frizone. Frizoner skal være indhegnet, og tilførsels- og fraførselssteder skal være underlagt toldtilsyn. Oprettelse af dem kræver forudgående godkendelse fra toldmyndighederne, der på forhånd skal modtage anmeldelse om de aktiviteter, der skal gennemføres, og kan pålægge forbud eller begrænsninger.

I frizonerne kan medlemsstaterne anvende:

- lettelser og fritagelser for moms og punktafgifter, efter de konkrete regler, der gælder i EU-lovgivningen på afgiftsområdet, og
- de ordninger for direkte beskatning, som de finder passende, under overholdelse af:
    - EU's statsstøtteregler (som generelt finder anvendelse på frizoner), og

[126] Artikel 243 i Europa-Parlamentets og Rådets forordning (EU) nr. 952/2013 af af 9. oktober 2013 om EU-toldkodeksen (EUT L 269 af 10.10.2013, s. 1).

- adfærdskodeksen for erhvervsbeskatning[127] (som de har aftalt at anvende for at begrænse skadelig skattepraksis).

Beskrivelse af sektoren

Frihavne er lagre i frizoner, der oprindelig var tænkt som steder til opbevaring af varer i transit. De er blevet populære med henblik på opbevaring af substitutionsaktiver, herunder kunstværker, ædelstene, antikviteter, guld og vin — ofte permanent. Ud over sikker lagring tilbyder de udskydelse af importafgifter og indirekte skatter som moms og brugerafgifter samt en høj grad af diskretion.

I 2016 udgjorde opbevaring på lagre 30 % af de samlede aktiviteter i frihandelszonerne og de oplagrede aktiver havde en anslået værdi af 536 mia. USD.[128]

I EU:

Der er 82 frizoner i EU.[129] Den eneste frihavn (dvs. en frihandelszone, der har specialiseret sig i opbevaring af værdifulde luksusvarer) er Luxembourg Freeport, som blev indviet i september 2014 og kun har fem pendanter andre steder i verden: i Genève, Monaco, Singapore, Beijing og Delaware (USA).

De andre frizoner er beliggende i 22 medlemsstater. De kan inddeles i forskellige kategorier af særlige økonomiske zoner, de er godkendt af Kommissionen, og anvendes hovedsageligt som logistik- og handelsknudepunkter, ikke specielt med henblik på formueforvaltning eller opbevaring af luksusvarer.

Beskrivelse af risikoscenariet

Frihandelszoner udgør forsat en forfalskningstrussel, idet de gør det muligt for falsknere at lande forsendelser, tilpasse eller på anden måde manipulere med last eller tilhørende papirer og derefter genudføre-varerne uden toldmyndighedernes indgriben og således skjule varernes sande oprindelse og art samt identiteten af den oprindelige leverandør.

I øjeblikket er der ca. 3.500 frizoner og særlige økonomiske zoner i verden. Frihandelszoner servicerer ikke kun skibstrafikken – mange befinder sig ved internationale lufthavne og landegrænser, hvorfra godset kan transporteres over land.

Der bliver stadig fundet svagheder i adskillige frihandelszoner, og nogle har været brugt i en i serie af organiseret kriminalitet, herunder:

- narkotikahandel

[127] Gruppen vedrørende Adfærdskodeksen (erhvervsbeskatning) blev oprettet af Ecofin den 9. marts 1998. Dens hovedfunktion er at vurdere de skatteforanstaltninger, der falder ind under anvendelsesområdet for adfærdskodeksen for erhvervsbeskatning fra december 1997 og føre tilsyn med udvekslingen af oplysninger om disse foranstaltninger.
[128] https://www.cps.org.uk/files/reports/original/161114094336-TheFreePortsOpportunity.pdf
[129] Frizoner, der er i drift i Unionens toldområde, som meddelt Kommissionen af medlemsstaterne: https://ec.europa.eu/taxation_customs/sites/taxation/files/resources/documents/customs/procedural_aspects/imports/free_zones/list_freezones.pdf

- ulovlig handel med elfenben
- menneskesmugling og
- forfalskninger.

Organiserede kriminelle bander, der misbruger frihandelszonerne, er ofte polykriminelle, f.eks. fører de aktiviteter, der gennemføres af organiserede kriminelle bander med hensyn til immaterialretskrænkelser, ofte momssvindel, korruption og hvidvask af penge med sig-.

Lovlige virksomheder ejet af lovovertrædere er nøglen til hvidvaskaktiviteter. De muliggør handelsbaserede systemer, som ikke ret tit indebærer fysisk transport af kontanter og giver en facade for pengeoverførsler.

I de fleste EU-frihavne og toldoplag (med undtagelse af Luxembourg Freeport) er præcise oplysninger om de endelige reelle ejere af godset ikke tilgængelige. Det femte direktiv om bekæmpelse-af hvidvask af penge omfatter udtrykkeligt frihavnsoperatører og andre aktører på kunstmarkedet, da de vil blive "forpligtede ikke-finansielle enheder" fra 10. januar 2020 og fremefter og dermed underlagt de samme kundekendskabskrav som f.eks. ejendomsmæglere-og advokater. De vil også indtage rollen som portvogtere for -bekæmpelse af hvidvask af penge, da de vil skulle indberette mistænkelige transaktioner til de finansielle efterretningsenheder.

Værdien af de oplagrede varer i frihavne skønnes at beløbe sig til mange milliarder euro. På grund af diskretions- og fortrolighedsklausuler (beslægtet med bankhemmelighed) oplyser ejerne af frihavne ikke værdien af de varer, der opbevares på deres lokaliteter, således som de er angivet af kunderne, så det er vanskeligt at give et præcist estimat.

Med schweiziske frihavne som vejledning anslog *The Economist i september 2012*, at frihavne i Genève og Zürich opbevarede "værdier for langt over 10 mia. USD i malerier, skulpturer, guld, tæpper og andre genstande".[130] I 2016 vurderede den schweiziske regering, at landets frihavne opbevarede værdier for omkring 100 mia. EUR.[131]

Trussel

Den Finansielle Aktionsgruppe (FATF) mener, at frihandelszoner som f.eks. frihavne giver bedre økonomiske muligheder, men savner effektiv retshåndhævelse og myndighedstilsyn.[132]

Frihavne opfattes som faciliteter, som beskytter deres kunders identitet og finansielle aktiviteter, i høj grad på samme måde som private banker. De er blevet beskrevet som

[130] https://www.economist.com/finance-and-economics/2012/09/01/paint-threshold
[131] https://www.finews.com/news/english-news/23238-swiss-freeports-move-to-crack-down-on-art,-loot
[132] *Money-laundering vulnerabilities of free-trade zones*: http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20vulnerabilities%20of%20Free%20Trade%20Zones.pdf

institutioner, der er undtaget fra pligten til indsamling og indberetning af værdifulde oplysninger om mulige tilfælde af skatteunddragelse, bestikkelse og hvidvask af penge.[133]

Finansiering af terrorisme

Frihavne betjener sig af flere begrænsninger, som hindrer lokale myndigheder i at undersøge ejendom, der opbevares på deres lokaliteter.

Nylig sag, der illustrerer *fremgangsmåden*:

I december 2016 beslaglagde de schweiziske myndigheder kulturelle værdigenstande, der var blevet røvet fra Syrien, Libyen og Yemen og blev opbevaret i Genèves frihavne, som stiller højsikrede lagerbygninger til rådighed, hvor genstande kan opbevares uden beskatning. De plyndrende havde bragt de konfiskerede genstande til Schweiz via Qatar. Tre af genstandene var fra oldtidsbyen Palmyra (Syrien), som står opført på UNESCO's verdensarvsliste, og som systematisk blev destrueret af ISIL (Da'esh) jihadister, der havde erobret den i maj 2015.

Konklusion: Truslen om finansiering af terrorisme i relation til frihavne anses for betydelig (niveau 3).

Hvidvask af penge

EU-baserede kriminelle bruger hovedsagelig producenter med hjemsted i udlandet og organiserer derefter indførsel, transport, oplagring og distribution af forfalskede varer i EU. Der findes imidlertid også aktive producenter af forfalskede varer i EU. Produktionen hjælpes frem ved hjælp af falske etiketter og emballage, der importeres fra lande uden for EU, og er ofte iscenesat af organiserede kriminelle bander. Der er tegn på, at denne form for kriminalitet er stigende.

Organiserede kriminelle bander involveret i svindel med punktafgifter er stærkt afhængige af brugen af lovlige forretningsstrukturer. Dette indebærer:

- etablering af stråmandsvirksomheder
- at de er i ledtog med nøglemedarbejdere i told og toldoplag, og
- samarbejde med transportvirksomheder og distributører.

Nylige sager, der illustrerer *fremgangsmåden*:

1. I 2015 afslørede de lækkede Panama-papirer, at en fremtrædende privat kunstsamler, David Nahmad, var den endelige reelle ejer af et maleri af Modigliani, *Siddende mand med stok*. Nahmad havde købt kunstværket på en Christie's-auktion i 1996 til en anslået værdi af 25 mio. USD gennem sit International Art Center (IAC) i Panama og opmagasineret det i Genève Freeport.

[133] http://www.taxjustice.net/wp-content/uploads/2013/04/TJN-141124-CRS-AIE-End-of-Banking-Secrecy.pdf

Maleriet tiltrak sig offentlighedens opmærksomhed, da barnebarnet af en jødisk antikvitetshandler, Oscar Stettiner, hævdede, at nazisterne havde stjålet det under besættelsen af Paris i 1939. De schweiziske myndigheder beslaglagde det i første omgang, men gav det senere tilbage til Nahmad, da sagsøgeren ikke var i stand til at bevise ejerskab, da den beskrivelse af kunstværket, som var blevet brugt til at bestyrke påstanden, var for vag.

2. En FATF-rapport fra oktober 2013 om *Hvidvask af penge-og finansiering af terrorisme gennem handel med diamanter* beskriver, hvordan kriminelle bruger diamanter som en form for valuta til at gøre deres transaktioner vanskeligere at spore.[134]

   I rapporten gives som eksempel en sag om bedrageri vedrørende diamanter for 800 mio. EUR begået i Genève Freeport i 2005. En kurervirksomhed med base i Antwerpen brugte Freeport til at smugle ædelsten, som den senere solgte på det sorte marked i Antwerpen via offshore-skuffeselskaber

Konklusion: Truslen om hvidvask af penge i relation til frihavne anses for betydelig (niveau 3).

Sårbarhed

Finansiering af terrorisme

Vurderingen af sårbarhed over finansiering af terrorisme i relation til frihavne viser følgende:

a) risikoeksponering

Frihavne bidrager til hemmeligholdelse. Med deres favorisering ligner de offshore-finanscentre, tilbyder en høj grad af sikkerhed og diskretion og muliggør transaktioner uden at tiltrække opmærksomhed fra kontrolmyndigheders side eller fra de myndigheder, der arbejder med direkte beskatning. En angivelse af værdien er nødvendig for varer, der opbevares i en frihavn eller et toldoplag, men dette sker normalt i form af en egen-erklæring fra ejeren eller dennes repræsentant, og i de fleste tilfælde bliver den ikke kontrolleret.

Varer i frihavne eller under toldoplag kan teknisk set være "i transit", selvom der ikke er nogen tidsbegrænsninger i de fleste frihavne af denne art. Varer kan komme ind i en frihavn, befinde sig dér permanent (og stige i værdi) og blive handlet et ubegrænset antal gange uden nogensinde at blive beskattet.

Ud over diskretionen, store pengetransaktioner, de retshåndhævende myndigheders manglende fortrolighed med værdierne og kunstens flytbarhed, gør altsammen kunstmarkedet til et egnet redskab for ulovlig aktivitet ved brug af frihavne. Efterhånden som andre pengevaskteknikker kommer under større bevågenhed, siges det, at menneskesmuglere, narkosmuglere og våbenhandlere i stigende grad vender sig mod kunstmarkedet.

b) risikobevidsthed

[134] http://www.fatf-gafi.org/media/fatf/documents/reports/ML-TF-through-trade-in-diamonds.pdf

Fra den 10. januar 2020 vil frihavnsoperatører og andre aktører på kunstmarkedet, f.eks. auktionshuse og gallerier, blive "forpligtede ikke-finansielle enheder" efter det femte hvidvaskdirektiv. Som portvogtere mht. bekæmpelse af hvidvask af penge skal de indberette mistænkelige transaktioner til de finansielle efterretningsenheder og gennemføre undersøgelser i tilknytning til kundekendskabskrav med henblik på at identificere de endelige reelle ejere af oplagrede varer.

Efter "Bouvier-sagen"[135] besluttede de nationale myndigheder ensidigt at anvende kravene til bekæmpelse af hvidvask af penge på Luxembourg Freeport, men der måtte gives operatørerne en respitperiode på et år til at opdatere deres registre og tilpasse deres procedurer til de nye krav. Det viser, at risikobevidstheden er under stadig udvikling, og at gennemførelsen af den nye ordning vil kunne kræve en betydelig indsats fra de licenshavende operatørers side med henblik på at tilpasse deres praksis, så de kan fastslå de endelige reelle ejere af varer, der indbringes af deres kunder.

c) retsgrundlag og kontroller

Da frihavne er underlagt EU-regler og nationale regler om bekæmpelse af hvidvask af penge, er de i højere grad reguleret i EU end andre steder.

Det vigtigste område, hvorpå frihavnsordninger er forskellige, er retningslinjerne for videregivelse af oplysninger – lokale regler er i den henseende mere byrdefule nogle steder end andre.

Konklusion: Når frihavne bruges anonymt, er de i sagens natur sårbare i forhold til finansiering af terrorisme. Bevidstheden i sektoren er voksende, men er stadig ikke tilstrækkelig. Sårbarhedsniveauet over for finansiering af terrorisme i relation til frihavne anses derfor for betydeligt (niveau 3).

Hvidvask af penge

Sårbarheden over for hvidvask af penge er ikke vurderet separat, men på grundlag af de faktorer, der er beskrevet ovenfor. Imidlertid kræver den store forekomst af sager om korruption, skatteunddragelse, kriminel aktivitet og hvidvask af penge, der er afsløret og behandlet af de retshåndhævende myndigheder, nøje overvejelser.

Konklusion: Frihavne er i sagens natur sårbare over for hvidvask af penge, når de bruges anonymt. Sektorens bevidsthed om risikoen for hvidvask af penge synes at være højere end for terrorfinansiering, men dens struktur og dens evne til at stillede målrettede ressourcer og uddannelse til rådighed er mangelfuld. Sårbarhedsniveauet over for hvidvask af penge i relation til frihavne anses for meget betydeligt (niveau 4).

Risikobegrænsende foranstaltninger:

Der er plads til forbedring af reguleringen af frihavnene i EU.

For at undgå forvirring bør Kommissionen tage stilling til følgende terminologiske uoverensstemmelser i det femte hvidvaskdirektiv og EU's toldkodeks:

[135] https://www.newyorker.com/magazine/2016/02/08/the-bouvier-affair

- Det femte hvidvaskdirektiv nævner udtrykkeligt frihavne, men toldkodeksen dækker dem kun som en slags frizone, og
- i toldkodeksen er frizoneproceduren næsten juridisk ligestillet med toldoplag. Det rejser spørgsmålet om, hvorvidt toldoplag og toldfri lagre er (eller burde være) omfattet af hvidvaskdirektivet. Da markedet for toldoplag er langt større end markedet for frihavne, bør dette spørgsmål afklares i god tid, før det femte hvidvaskdirektiv skal være gennemført (januar 2020).

Medlemsstaterne bør:

- gennemføre regelmæssige uafhængige revisioner af godkendte frizoneoperatørers compliancefunktioner mht. bekæmpelse af hvidvask af penge og sikre en passende og konsekvent håndhævelse af de procedurer og det opsyn vedrørende bekæmpelse af hvidvask af penge, der allerede er fastslået i loven.
- sikre, at godkendte frizoneoperatører regelmæssigt videregiver oplysninger til de relevante myndigheder, der varetager bekæmpelse af hvidvask af penge, om endelige reelle ejere og ændringer i ejerforholdene for aktiver i frihavnen
- fastsætte en rimelig, forretningsmæssigt hensigtsmæssig tidsfrist for oplagring af gods i frihavne, og
- opfordre det europæiske kunstmarked som en af hovedkunderne i frihavne til selv-regulering og til at forbedre dets gennemsigtighed, især da kunsttransaktioner fortsat indebærer en stor risiko for hvidvask af penge pga. deres uigennemsigtighed og den subjektive karakter af vurderingerne af aktiverne.

1. Ordninger for tildeling af statsborgerskab og opholdsret til investorer

Produkt
"Gyldne visa" og "gyldne pas"

Sektor
Statsborgerskab/opholdsret

Generel beskrivelse af den pågældende sektor og det/den relevante produkt/aktivitet

Der har i de seneste år været en stigende tendens til, at lande indfører ordninger for tildeling af statsborgerskab til investorer og opholdsret til investorer. Formålet er at tiltrække investeringer til et bestemt land ved at give investorer statsborgerskab eller opholdsret i landet. Sådanne ordninger har givet anledning til bekymring om visse dermed forbundne risici, navnlig sikkerhedsmæssige risici, hvidvask af penge, skatteunddragelse-undgåelse[136] og korruption.

Ordninger for tildeling af statsborgerskab til investorer betegnes ofte CIP ("citizenship investment programs"), "statsborgerskab til salg" eller "gyldne pas". De gør det muligt for udlændinge at blive naturaliseret som borger i et land til gengæld for en investering, hvis visse kriterier er opfyldt. Statsborgerskabsordninger for investorer er forskellige fra opholdsretsordninger for investorer ("gyldne visa"), som har til formål at tiltrække investeringer til gengæld for opholdsrettigheder i det pågældende land.

Grundlaget for disse ordninger er legitim økonomisk overskud og diversificering for værtsnationen,[137] men der er rapporteret tilfælde af misbrug.

På samme måde som med hensyn til at få et statsborgerskab nr. 2 er fordelene bl.a., at det bliver lettere at rejse, have ophold og gøre forretninger. Det kan også være et middel til at flytte aktiver ud af deres oprindelsesland, især hvis de bor i et ustabilt politisk eller økonomisk klima, eller hvis deres velstand er erhvervet på en tvivlsom måde. Disse ordninger kan også bruges til at undgå blive retsforfulgt eller dømt i deres oprindelseslande. Mange CIP-lande er offshore-finanscentre, hvis strukturer giver sikkerhed, diskretion og skattebegunstigelser. De kan også tilbyde personer større frihed til at handle i og med globale finanscentre på grund af deltagerens (erhvervede) status som lokal, der derfor er genstand for mindre kontrol.

Beskrivelse af sektoren i EU

[136] Mulige misbrug er f.eks. skatteunddragelse gennem misbrug af dobbelt hjemsted og skatteunddragelse – at etablere et selskab uden fysisk tilstedeværelse for at drage fordel af skatteincitamenter og små bopælskrav i den medlemsstat, der tilbyder statsborgerskab til investorer.
[137] Den første ordning for tildeling af statsborgerskab til investorer blev indført af Saint Kitts og Nevis i 1984 som et middel til at styrke økonomien. Succesen fik mange andre lande til at følge trop.

I EU har tre medlemsstater (Bulgarien, Cypern og Malta) **ordninger for tildeling af statsborgerskab til investorer**, ifølge hvilke der gives statsborgerskab på mindre strenge betingelser end i forbindelse med almindelige naturaliseringsprocedurer, navnlig uden reelt forudgående ophold i det pågældende land.[138] Sådanne ordninger har konsekvenser for Den Europæiske Union som helhed, eftersom enhver, der er statsborger i en medlemsstat, samtidig er unionsborger. Selvom der er tale om nationale ordninger, markedsføres de da også ofte udtrykkeligt som et middel til at opnå unionsborgerskab sammen med alle de rettigheder og privilegier, der er knyttet hertil, herunder navnlig retten til fri bevægelighed.

Ordninger for tildeling af opholdsret til investorer findes i 20 EU-lande:[139] Bulgarien, Tjekkiet, Estland, Irland, Grækenland, Spanien, Frankrig, Kroatien, Italien, Cypern, Letland, Litauen, Luxembourg, Malta, Nederlandene, Polen, Portugal, Rumænien, Slovakiet og Det Forenede Kongerige. Disse ordninger er forbundet med de samme risici som ordninger for tildeling af statsborgerskab til investorer. De påvirker desuden andre medlemsstater, eftersom en gyldig opholdstilladelse giver tredjelandsstatsborgere visse rettigheder, herunder ret til at bevæge sig frit i især Schengenområdet.

Europa-Parlamentet udtrykte i sin beslutning af 16. januar 2014[140] bekymring for, at nationale ordninger, der kan omfatte "direkte salg, direkte eller indirekte", af EU-statsborgerskab, undergraver selve begrebet unionsborgerskab; Det opfordrer Kommissionen til at vurdere de forskellige nationale ordninger på baggrund af europæiske værdier og ånden og bogstavet i EU's lovgivning og praksis.

I sin 2017-rapport om unionsborgerskab[141] bebudede Kommissionen en rapport om de nationale ordninger for unionsborgerskab til investorer. Rapporten beskrev Kommissionens indsats på området og undersøgte gældende national lovgivning og praksis samt gav vejledning til medlemsstaterne. Som forberedelse til rapporten bestilte Kommissionen en undersøgelse af lovgivning og praksis i forbindelse med statsborgerskab og bopæl i alle relevante medlemsstater[142] og afholdt en høring med medlemsstaterne.

---

[138] Investorerne skal investere mellem 800.000 og 2 mio. EUR.

[139] De to lister overlapper hinanden, idet tre lande — Bulgarien, Cypern og Malta — befinder sig på begge lister.

[140] Europa-Parlamentets beslutning af 16. januar 2014 om EU-borgerskab til salg (2013/2995(RSP)): http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0038&language=DA&ring=P7-RC-2014-0015

[141] Rapport fra Kommissionen til Europa-Parlamentet, Rådet, Det Europæiske Økonomiske og Sociale Udvalg og Regionsudvalget, *Styrkelse af borgernes rettigheder i en Union med demokratiske forandringer: 2017-rapport om unionsborgerskab* (COM(2017) 030 final). Kan ses på: https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=51132

[142] Faktaundersøgelse. Milieu Law and Policy Consulting, *Factual Analysis of Member States' Investor Schemes granting citizenship or residence to third-country nationals investing in the said Member State*, Bruxelles 2018.

Rapporten tager også hensyn til andre relevante kilder, herunder de seneste publikationer om emnet[143], og den blev offentliggjort i januar 2019.[144]

Efter offentliggørelsen af rapporten nedsatte Kommissionen en ekspertgruppe fra medlemsstaterne at undersøge de specifikke risici, der knytter sig til ordninger for tildeling af statsborgerskab til investorer, og de aspekter af gennemsigtighed og god forvaltningspraksis med hensyn til gennemførelsen af både statsborgerskabs- og opholdsretsordninger for investorer. Inden udgangen af 2019 forventes gruppen af eksperter at udforme et sæt fælles sikkerhedskontrolforanstaltninger for ordninger for tildeling af statsborgerskab til investorer, herunder specifikke risikostyringsprocedurer, der tager højde for risici vedrørende sikkerhed, hvidvask af penge, skatteunddragelse og korruption.

Trussel

Tredjelandsstatsborgere kan have legitime grunde til at investere i en medlemsstat[145], men kan også være ude i ulovligt ærinde, f.eks. at unddrage sig retshåndhævende myndigheders undersøgelse og retsforfølgelse i deres hjemland beskytte deres aktiver mod indefrysnings- og beslaglæggelsesforanstaltninger. Ordninger for tildeling af statsborgerskab eller opholdsret til investorer skaber derfor en række risici for medlemsstaterne og for EU som helhed, navnlig sikkerhedsmæssige risici, herunder muligheden for, at organiserede kriminelle grupper fra tredjelande infiltrerer EU, samt risiko for hvidvask af penge, korruption og skatteunddragelse. Sådanne risici skærpes på grund af de grænseoverskridende rettigheder, der er forbundet med unionsborgerskabet eller opholdsretten i en medlemsstat.

Den manglende gennemsigtighed og forvaltning af ordningerne giver også anledning til bekymring. Både statsborgerskabs- og opholdsretsordninger er kommet i offentlighedens søgelys efter påstande om dertil knyttet misbrug og korruption i nogle medlemsstater.[146] Endvidere er proceduren for screening af ansøgere ofte udliciteret til private virksomheder, og hvor der er en permanent risiko for interessekonflikt og korruption. Øget

---

[143] Se navnlig European Parliamentary Research Service, *Citizenship and residency by investment schemes in the EU: State of play, issues and impacts*, oktober 2018.
http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2018)627128
Transparency International/Global Witness, *European Getaway — Inside the Murky World of Golden Visas*, oktober 2018, https://www.transparency.org/whatwedo/publication/golden_visas

[144] Rapport fra Kommissionen til Europa-Parlamentet, Rådet, Det Europæiske Økonomiske og Sociale Udvalg og Regionsudvalget, *Ordninger for tildeling af statsborgerskab og opholdsret til investorer i Den Europæiske Union* COM(2019) 12 final.
https://ec.europa.eu/info/sites/info/files/com_2019_12_final_report.pdf

[145] I henhold til TEUF artikel 63 finder princippet om frie kapitalbevægelser anvendelse mellem medlemsstaterne indbyrdes og mellem medlemsstaterne og tredjelande. Artikel 65 tillader, at kapitalens frie bevægelighed begrænses af hensyn til den offentlige orden, den offentlige sikkerhed eller af hensyn til beskatning.

[146] For eksempel fortalte en østrigsk politiker i 2009 en mulig russisk investor, at han kunne få østrigsk statsborgerskab i bytte for en investering på 5 mio. EUR og en donation til hans parti. En detaljeret beskrivelse af indberetninger om misbrug eller fejlagtig anvendelse af ordningerne findes i den undersøgelse, der er nævnt i fodnote 5.

gennemsigtighed og indførelse af passende risikostyring, kontrolsystemer og tilsynsmekanismer kan bidrage til i videst muligt omfang at afbøde nogle af disse risici.

Ordninger for tildeling af statsborgerskab eller opholdsret i EU kan misbruges til skatteformål på en række måder. Personer kan hævde at have hjemsted i en af disse jurisdiktioner, hvorimod deres reelle skattemæssige hjemsted muligvis kan være i en anden jurisdiktion (misbrug af dobbelt hjemsted). Skatteoplysninger, der gives i henhold til aftaler mellem jurisdiktioner om udveksling af oplysninger, kan risikere at blive sendt til den forkerte hjemstedsjurisdiktion. Med hensyn til skatteundgåelse kan ledelsen af forretningsstrukturer oprettes i EU-lande med statsborgerskabs- eller opholdsretsordninger, som har små bopælskrav, der ikke er i overensstemmelse med internationale regler om modvirkning af skatteundgåelse, f.eks. ikke kræver væsentlige forretningsaktiviteter, og/eller hvor forretningsstrukturen kan drage fordel af skatteordninger, der gør det lettere at foretage aggressiv skatteplanlægning.

Desuden er der risiko for, at konkurrence blandt medlemsstaterne om klienter, der ønsker at erhverve statsborgerskab eller bopæl gennem investeringer, udløser et "kapløb mod bunden" mht. standarder for due diligence og gennemsigtighed.

Finansiering af terrorisme

Vurderingen af truslen om terrorfinansiering i relation til gyldne visa/pas har blotlagt følgende problemområder:

- **Sikkerhedstjek**: Der er visse sikkerhedsmæssige forpligtelser efter EU-retten, der skal opfyldes før udstedelsen af et visum eller en opholdstilladelse til udenlandske investorer. Der mangler imidlertid tilgængelige oplysninger om den praktiske gennemførelse og skønnet i forbindelse med den måde, hvorpå medlemsstaterne behandler sikkerhedsproblemer.

- **Krav om fysisk tilstedeværelse:** Opholdstilladelser opnået gennem investering med begrænset eller intet krav om investors fysiske tilstedeværelse i den pågældende medlemsstat kan have konsekvenser for anvendelsen af status som fastboende udlænding i EU og de rettigheder, der er forbundet med det, og måske endda give en hurtig vej til nationalt og dermed EU statsborgerskab.

- **Mangel på gennemsigtighed:** Rapporten fremhæver mangel på gennemsigtighed og tilsyn med ordningerne, især for så vidt angår overvågning og fraværet af statistikker om, hvor mange mennesker der får opholdstilladelse gennem sådanne ordninger.

Konklusion: I den beskrevne sammenhæng anses trusselsniveauet mht. terrorfinansiering i relation til gyldne visa/pas som betydeligt/meget betydeligt (niveau 3/4).

Hvidvask af penge

Eksempler på lande, der har tiltrukket velhavende personer involveret i hvidvasksystemer:

I de senere år er Cypern blevet et finansielt tilflugtssted for ukrainske og russiske oligarker og et knudepunkt for systemer til hvidvask af penge. Dette skyldes til dels landets effektive ordning for tildeling af statsborgerskab til investorer. Velhavende udlændinge kan blive statsborgere på mindre end 6 måneder til gengæld for at investere 2 mio. EUR Næsten halvdelen af de 2 000 pas, der er udstedt ifølge ordningen inden for de sidste 2 år, blevet erhvervet af russere. En sådan investering kan legitimere hvidvaskede penge, og cypriotisk statsborgerskab kan gøre det lettere at overføre penge til landet og rundt på det europæiske finansmarked. Cypern er også populært, da det er et land med skatteincitamenter.

Maltesisk statsborgerskab er ligeledes populært blandt velhavende russere. Saudiarabere har også investeret i ordningen. F.eks. Waleed al-Ibrahim, formanden for Middle East Broadcasting Center. Al-Ibrahim blev arresteret i november 2017 i forbindelse med en korruptionsudrensning.[147]

Pas fra caribiske øer er også indblandet i at gøre det muligt at hvidvaske penge. En person tilknyttet den aserbajdsjanske "laundromat-skandale" var pakistansk statsborger, der også havde St Kitts og Nevis-statsborgerskab. Det er sandsynligt, at formålet med dette statsborgerskab var at skjule aktiver.

Gyldne visa bruges også til at undgå sanktioner

Siden indførelsen af EU's og USA's økonomiske sanktioner, visumforbud og indefrysning af aktiver i forhold til Rusland efter landets invasion af Ukraine og ulovlige annektering af Krim i 2014 har der været en kraftig stigning i russiske ansøgninger efter ordningerne for tildeling af statsborgerskab til investorer; dette har givet anledning til risiko for undgåelse af sanktioner, ud over den potentielle hvidvask af ulovlige midler.

Nordkoreanske borgere har også tidligere været i stand til at skaffe sig alternative pas, som de efterfølgende har brugt til at drive forretning uden for Nordkorea – der blev fundet to nordkoreanere, der brugte pas fra Kiribati og Seychellerne til at drive virksomhed i Hong Kong og Japan. Begge lande har angiveligt annulleret ordningerne, men man regner med, at deres pas blev udstedt efter den angivelige annullationsdato.

Endelig har Comorernes ordning for tildeling af statsborgerskab til investorer fået dårlig presseomtale. I begyndelsen af januar 2018 annullerede Comorernes regering 170 pas, som angiveligt var udstedt til udlændinge på utilbørlig måde, herunder til mange iranere, i den tidligere regerings embedsperiode. Comorernes myndigheder har konstateret, at mindst to udenlandske indehavere af pas fra Comorerne af de US-amerikanske myndigheder hævdedes at have tilsidesat sanktionerne mod Iran (selvom statsborgerskabet på Comorerne i intet af de to tilfælde i sig selv syntes at have haft direkte indflydelse på undgåelsen).

[147] Se generelt: www.transparency.org/whatwedo/publication/golden_visas
Også:
https://www.maltatoday.com.mt/news/national/83539/russian_nationals_dominate_list_of_global_rich_who_are_now_maltese#.XSxUtCBS-Uk
http://www.independent.com.mt/articles/2018-12-30/local-news/Turkish-billionaires-and-Russian-industry-moguls-meet-Malta-s-new-citizens-6736201441

Den primære risiko i forbindelse med disse ordninger er således **eksponering for hvidvask af penge.** Der er en klar og konkret risiko for, at nogle kunder kan have fået lavere risikoevalueringer (bestemt af deres nationalitet), end det er forsvarligt. Dette kan påvirke niveauet af de gennemførte kundekendskabskrav og/eller overvågningen i forhold til transaktionen. Det kan resultere i godkendelse af transaktioner, der tilsyneladende er godartede, men som burde have være undersøgt nærmere pga. de underliggende omstændigheder.

Konklusion: I lyset af det scenarie, der er beskrevet ovenfor, anses trusselsniveauet i forhold til hvidvask af penge i relation til gyldne visa/pas som betydeligt/meget betydeligt (niveau 3/4).

Sårbarhed

Finansiering af terrorisme

Vurderingen af sårbarheden over for terrorfinansiering i relation til gyldne visa/pas har blotlagt følgende problemområder:

a) risikoeksponering

De to primære problemområder, der er vurderet af de europæiske institutioner, er sikkerhed samt gennemsigtighed og information. Med hensyn til sikkerhed blev det konstateret, at de kontroller, der gennemføres i forhold til ansøgerne, ikke er tilstrækkeligt grundige, og at EU's egne centraliserede informationssystemer f.eks. Schengen-informationssystemet ikke anvendes så systematisk, som de burde. I forhold til gennemsigtighed og information mangler der klar information om, hvordan ordningerne administreres, herunder om antallet af ansøgninger, der er modtaget, imødekommet eller afvist, samt ansøgernes oprindelse. Derudover udveksler medlemsstaterne ikke oplysninger om ansøgere til ordningerne, og de underretter heller ikke hinanden om afviste ansøgere.

b) risikobevidsthed

De involverede nationale myndigheder synes ikke at være klar over de problemer, der er forbundet med ordningerne, eller i værste fald påtager de sig gerne de medfølgende risici til gengæld for forventede investeringer.[148]

Nylige skandaler, der er beskrevet i medierne, tyder på, at nogle EU-lande ikke har gjort det til standardprocedure at gennemføre skærpede kontroller af ansøgerne, deres familiemedlemmer og oprindelsen af deres midler.

c) retsgrundlag og kontroller

Sikkerhedstjek: Der er visse sikkerhedsmæssige forpligtelser efter EU-retten, der skal opfyldes før udstedelsen af et visum eller en opholdstilladelse til udenlandske investorer. Der mangler imidlertid tilgængelige oplysninger om den praktiske gennemførelse og

[148] IMF Working Paper, WP/15/93, Too Much of a Good Thing?: Prudent Management of Inflows under Economic Citizenship Programs, af Xin Xu, Ahmed El-Ashram og Judith Gold https://www.imf.org/external/pubs/ft/wp/2015/wp1593.pdf

skønnet i forbindelse med den måde, hvorpå medlemsstaterne behandler sikkerhedsproblemer.

Krav om fysisk tilstedeværelse: Opholdstilladelser opnået gennem investering med begrænset eller intet krav om investors fysiske tilstedeværelse i den pågældende medlemsstat kan have konsekvenser for anvendelsen af status som fastboende udlænding i EU og de rettigheder, der er forbundet med det, og måske endda give en hurtig vej til nationalt og dermed EU statsborgerskab.

Konklusion: I den sammenhæng anses sårbarhedsniveauet mht. terrorfinansiering i relation til gyldne visa/pas som betydeligt/meget betydeligt (niveau 3/4).

Hvidvask af penge

Vurderingen af sårbarheden over for hvidvask af penge hviler på de samme faktorer som ovenfor beskrevet og behandles ikke særskilt. Ikke desto mindre er det nødvendigt specifikt at vurdere den høje sårbarhed i lyset af de høje niveauer af korruption, skatteunddragelse, kriminalitet og hvidvask af penge, som de retshåndhævende myndigheder har afsløret og behandlet.

Konklusion: I den sammenhæng anses sårbarhedsniveauet i forhold til hvidvask af penge i relation til gyldne visa/pas som meget betydeligt (niveau 4).

Risikobegrænsende foranstaltninger:

De beskrevne ordninger er af fælles EU-interesse, da enhver, der får statsborgerskab i en medlemsstat, samtidig får **EU-statsborgerskab.** En medlemsstats beslutning om at tildele statsborgerskab til gengæld for investeringer giver automatisk rettigheder i forhold til andre medlemsstater, navnlig retten til fri bevægelighed, adgang til EU's indre marked til at udøve økonomiske aktiviteter samt retten til at stemme og blive valgt i europæiske og lokale valg. I praksis annonceres disse ordninger ofte som et middel til at opnå unionsborgerskab, sammen med alle de rettigheder og privilegier, der er forbundet med det.

Udover de basale etiske overvejelser om salg af statsborgerskab og den foruroligende tanke, at nogle medlemsstater profiterer af salget af et fælles europæisk gode, er der en særskilt og iboende række risici forbundet med disse ordninger.

<u>Kommissionen:</u>

Kommissionen vil **overvåge det bredere spørgsmål om overholdelse af EU-retten**, som statsborgerskabs- og opholdsretsordninger for investorer rejser, og vil træffe de nødvendige foranstaltninger. Af denne grund skal medlemsstaterne navnlig sikre, at:

- alle obligatoriske grænse- og sikkerhedskontroller udføres systematisk
- kravene ifølge direktiverne om tredjelandsstatsborgeres status som fastboende udlænding og retten til familiesammenføring overholdes

- midler, der betales af ansøgere om statsborgerskab og opholdsret for investorer, vurderes efter **EU's regler om bekæmpelse af hvidvask af penge**

- **direktiv 2018/822/EU**[149], som bestemmer, at mellemmænd skal indgive oplysninger om indberetningspligtige grænseoverskridende skatteordninger til deres nationale myndigheder,[150] får virkning fra 2020
- Kommissionen vil overvåge de skridt, medlemsstaterne tager for at håndtere problemerne med gennemsigtighed og styring i forvaltningen af ordningerne. Den har nedsat en **gruppe af eksperter fra medlemsstaterne** for at forbedre ordningernes gennemsigtighed, styring og sikkerhed. Gruppen har især til opgave at:
    - etablere et system til udveksling af oplysninger og høringer om antallet af modtagne ansøgninger, oprindelsesland og antallet af medlemsstaternes tildelte og afviste statsborgerskaber og opholdstilladelser gennem investeringer
    - udvikle et fælles sæt af sikkerhedskontroller for statsborgerskabsordninger for investorer, herunder specifikke risikostyringsprocedurer, inden udgangen af 2019

Endelig vil Kommissionen, som følge af at tredjelande etablerer tilsvarende ordninger, der kan have sikkerhedsmæssige konsekvenser for EU, overvåge statsborgerskabsordninger gennem investeringer i kandidatlande og potentielle kandidatlande som led i EU-tiltrædelsesprocessen. Den vil ligeledes overvåge virkningen af sådanne ordninger i EU-visumfrie lande som led i mekanismen til suspension af visumfritagelsen.

Medlemsstaterne:

Medlemsstaterne bør sikre gennemskuelighed og god administration i forbindelse med gennemførelsen af ordningerne, navnlig i forhold til den infiltration af EU's økonomi, der gennemføres af organiserede kriminelle grupperinger fra lande uden for EU, samt risikoen for hvidvask af penge, korruption og skatteunddragelse. Medlemsstaternes indsats bør omfatte:

- årlig rapportering, der gøres tilgængelig for offentligheden.
- at det sikres, at rapporterne indeholde oplysninger om antallet af modtagne ansøgninger, oprindelseslande og antallet af statsborgerskaber og opholdstilladelser, der udstedes og afvises – tillige med identitet og oprindelsesland for de nyligt godkendte fastboende og statsborgere

[149] Rådets direktiv (EU) 2018/822 af 25. maj 2018 om ændring af direktiv 2011/16/EU for så vidt angår obligatorisk automatisk udveksling af oplysninger på beskatningsområdet i forbindelse med indberetningspligtige grænseoverskridende ordninger, EUT L 139 af 5.6.2018, s. 1.
[150] Administrativt samarbejde om (direkte) beskatning i EU: https://ec.europa.eu/taxation_customs/business/tax-cooperation-control/administrative-cooperation/enhanced-administrative-cooperation-field-direct-taxation_en.

- at der udarbejders opdelte statistikker om ordninger for opholdstilladelse for investorer, således at det konkrete grundlag for opholdstilladelse eller den valgte investeringsmulighed kan konstateres
- at der indføres en risikostyringsprocedure, herunder en passende identifikation, klassificering begrænsning af risici, hvilket koordineres af en dertil udpeget national myndighed. Overvågning af planens gennemførelse
- at der gennemføres en årlig revision med henblik på at vurdere gennemførelsen af planen for risikobegrænsning
- i forbindelse med **risikoen for skatteundgåelse og skatteunddragelse** findes der værkstøjer inden for EU's rammer for administrativt samarbejde (direktiv 2011/16/EU[151]), især spontan udveksling af oplysninger, hvilket f.eks. vil muliggøre, at de kompetente myndigheder i den medlemsstat, der benytter ordningen med statsborgerskab/opholdstilladelse for investorer, underretter den medlemsstat, hvor den, der opnår fordelene af sådan en ordning, har ophold.

Medlemsstaterne bør også afklare og offentliggøre kriterier for vurdering af ansøgninger og de sikkerhedstjek, der udføres som del af ordningen, og sikre regelmæssige efterfølgende kontrol med overholdelsen af disse kriterier, især for så vidt angår de investeringer, ansøgeren foretager. De bør også indføre en procedure for tilbagekaldelse af tilladelser, hvis kriterierne ikke længere skulle være opfyldt.

Sidst, men ikke mindst bør medlemsstaterne også sørge for fuldstændig gennemsigtighed angående de procedurer, der følges med hensyn til at overdrage administrationen af disse ordninger til private virksomheder, herunder oplysninger om de disse virksomheders reelle ejere. Disse private virksomheder bør under ingen omstændigheder inddrages i selve efterprøvningen af de oplysninger og dokumenter, ansøgerne fremlægger. Denne kontrol bør fortsat ligge i hænderne på de ansvarlige statslige organer, ikke hos private virksomheder.

BILAG 2 – EU'S RETSREGLER OM BEKÆMPELSE AF HVIDVASK AF PENGE OG FINANSIERING AF TERRORISME

EU's lovgivning om finansielle tjenesteydelser og tilsyn, som er relevant for området for bekæmpelse af hvidvask af penge og finansiering af terrorisme, med hjemmel i TEUF artikel 53 og artikel 114:

- Direktiv (EU) 2015/2366 om betalingstjenester i det indre marked, om ændring af direktiv 2002/65/EF, 2009/110/EF og 2013/36/EU og forordning (EU) nr. 1093/2010 og om ophævelse af direktiv 2007/64/EF.

[151] https://ec.europa.eu/taxation_customs/business/tax-cooperation-control/administrative-cooperation/enhanced-administrative-cooperation-field-direct-taxation_en

- Direktiv 2009/110/EF om adgang til at optage og udøve virksomhed som udsteder af elektroniske penge og tilsyn med en sådan virksomhed, ændring af direktiv 2005/60/EF og 2006/48/EF og ophævelse af direktiv 2000/46/EF.
- Direktiv 2014/65/EU om markeder for finansielle instrumenter og om ændring af direktiv 2002/92/EF og direktiv 2011/61/EU.
- Direktiv 2013/36/EU om adgang til at udøve virksomhed som kreditinstitut og om tilsyn med kreditinstitutter og investeringsselskaber, om ændring af direktiv 2002/87/EF og om ophævelse af direktiv 2006/48/EF og 2006/49/EF.

Der er vedtaget yderligere EU-lovgivning på området for bekæmpelse af hvidvask af penge og af finansiering af terrorisme i henhold til artikel 114 og artikel 33 TEUF i relation til kontrol med bevægelser af likvide midler ved EU's ydre grænser:

- Forordning (EU) 2018/1672 om kontrol med likvide midler, der føres ind i eller ud af Unionen, og om ophævelse af forordning (EF) nr. 1889/2005 (den nye forordning om kontrol med likvide midler).

Yderligere forebyggende foranstaltninger:

- Direktiv (EU) 2018/1673 EU om strafferetlig bekæmpelse af hvidvask af penge.
- Forordning (EU) 2019/880 om indførsel og import af kulturgenstande.[152]

Andre områder af relevans for bekæmpelse af hvidvask af penge og af finansiering af terrorisme er dækket af EU-lovgivning vedtaget på området for bekæmpelse af finansiering af terrorisme i henhold til artikel 215 TEUF, artikel 75 TEUF og 352 TEUF – hvorved der pålægges målrettede økonomiske sanktioner:

- Rådets forordning (EF) nr. 2580/2001 om specifikke restriktive foranstaltninger mod visse personer og enheder med henblik på at bekæmpe terrorisme.
- Rådets forordning (EF) nr. 881/2002 om indførelse af visse specifikke restriktive foranstaltninger mod visse personer og enheder, der har tilknytning til Usama bin Laden, Al-Qaida-organisationen og Taliban, og om ophævelse af Rådets forordning (EF) nr. 467/2001 om forbud mod udførsel af visse varer og tjenesteydelser til Afghanistan, om styrkelse af flyveforbuddet og om udvidelse af indefrysningen af midler og andre økonomiske ressourcer over for Taliban i Afghanistan.
- Rådets forordning (EU) nr. 267/2012 om restriktive foranstaltninger over for Iran og om ophævelse af forordning (EU) nr. 961/2010

EU-lovgivning vedtaget på området for bekæmpelse af hvidvask af penge og af finansiering af terrorisme i henhold til TEUF-bestemmelser inden for området med frihed, sikkerhed og retfærdighed

[152] Europa-Parlamentets og Rådets forordning (EU) 2019/880 af 17. april 2019 om indførsel og import af kulturgenstande, PE/82/2018/REV/1, EUT L 151 af 7.6.2018, s. 1. .

- Rådets afgørelse 2000/642/RIA om samarbejdsordninger mellem medlemsstaternes finansielle efterretningsenheder for så vidt angår udveksling af oplysninger.
- Rådets afgørelse 2007/845/RIA om samarbejde mellem medlemsstaternes kontorer for inddrivelse af aktiver om opsporing og identificering af udbyttet fra strafbart forhold eller andre formuegoder forbundet med kriminalitet.
- Rådets rammeafgørelse 2001/500/RIA om hvidvaskning af penge, identifikation, opsporing, indefrysning eller beslaglæggelse og konfiskation af redskaber og udbytte fra strafbart forhold.
- Direktiv (EU) 2017/541 om bekæmpelse af terrorisme og om erstatning af Rådets rammeafgørelse 2002/475/RIA og ændring af Rådets afgørelse 2005/671/RIA.
- Rådets rammeafgørelse 2005/212/RIA om konfiskation af udbytte, redskaber og formuegoder fra strafbart forhold.
- Rådets rammeafgørelse 2003/577/RIA om fuldbyrdelse i Den Europæiske Union af kendelser om indefrysning af formuegoder eller bevismateriale.
- Rådets rammeafgørelse 2006/783/RIA om anvendelse af princippet om gensidig anerkendelse på afgørelser om konfiskation.
- Direktiv 2014/41/EU om den europæiske efterforskningskendelse i straffesager.
- Direktiv 2014/42/EU om indefrysning og konfiskation af redskaber og udbytte fra strafbart forhold i Den Europæiske Union.

BILAG 3 – ORDLISTE

Akronymer og forkortelser vedrørende bekæmpelse af hvidvask af penge	
Akronym	**Betydning**
	Automatisk clearingcenter
	Bekæmpelse af hvidvask af penge og af finansiering af terrorisme
	International database for bekæmpelse af hvidvask af penge
	Asien/Stillehavs-gruppen vedrørende Hvidvask af Penge
API	Autoriserede betalingsinstitutter
	Aktivbeskyttende trust
	Undergrundsoverførselstjeneste
	Pengeautomat
BO	Reel ejer
BSA	Lov om bankhemmelighed
CCR	Forordning om kontrol med likvide midler
CCTV	TV-overvågning
CDD	Kundekendskabskrav
CIP	Kundeidentifikationsprogram
CTR	Rapport om pengetransaktion
DNFBPs	Udpegede ikke-finansielle virksomheder og erhverv
EAG	De Eurasiske Gruppe vedrørende bekæmpelse af hvidvask af penge og finansiering af terrorisme
EBA	Den Europæiske Banktilsynsmyndighed http://www.eba.europa.eu/
ECB	Den Europæiske Centralbank
ECEF	Elektrisk mappe til fortsatte undersøgelser
EDD	Skærpede kundekendskabskrav
EFT	Elektronisk pengeoverførsel

EGMLTF	Ekspertgruppen vedrørende Hvidvask af Penge og Finansiering af Terrorisme (E02914)
Egmontgruppen	Egmontgruppen af finansielle efterretningsenheder (uformelt internationalt net af FIU'er)
EIOPA	Den Europæiske Tilsynsmyndighed for Forsikrings- og Arbejdsmarkedspensionsordninger https://eiopa.europa.eu/
ESAs	De tre europæiske tilsynsmyndigheder (EBA, EIOPA og ESMA)
ESAAMLG	Gruppen til Bekæmpelse af Hvidvask af Penge for det Østlige og Sydlige Afrika
ESMA	Den Europæiske Værdipapir- og Markedstilsynsmyndighed https://www.esma.europa.eu/
FATF	Den Finansielle Aktionsgruppe www.fatf-gafi.org FATF blev nedsat af G7-Gruppen af industrilande i 1989 med henblik på at fremme etableringen af nationale og globale foranstaltninger til bekæmpelse af hvidvask af penge. Det er et internationalt politikudformende organ, som fastlægger standarder for bekæmpelse af hvidvask og foranstaltninger mod terrorfinansiering i hele verden. Dens henstillinger har ikke lovskraft. Fem og tredive lande og to internationale organisationer er medlemmer. I 2012 gennemreviderede FATF sine 40 + 9 henstillinger og reducerede dem til 40. http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html FATF udarbejder årlige typologirapporter, der viser de aktuelle tendenser og metoder i forbindelse med hvidvask af penge og terrorfinansiering.
FI	Finansieringsinstitut
FinCEN	Retshåndhævende net vedrørende økonomisk kriminalitet
FinTech	Teknologibaserede og teknologistøttede finansielle tjenesteydelser
FIU	Finansielle efterretningsenheder
FSRB	Regionalt Organ i stil med Den Finansielle Aktionsgruppe
FTF	Udenlandske terrorkrigere

GAFILAT	Finansiel handlingsgruppe om hvidvask af penge i Latinamerika
GDP	Bruttonationalprodukt
IA	Konsekvensvurdering
IBC	International Business Company
IVTS	Uformelt værdioverførselssystem
KYC	Kend din kunde
KYE	Kend din medarbejder
LEA	Retshåndhævende myndighed
MER	Gensidig evalueringsrapport
ML	Hvidvask af penge
MENAFATF	Den Finansielle Aktionsgruppe for Mellemøsten og Nordafrika
MLAT	Gensidig retshjælpstraktat
MLRO	Den ansvarlige for indberetning af hvidvask af penge.
MONEYVAL	Europarådets ekspertkomité for Evaluering af Foranstaltninger til Bekæmpelse af Hvidvask af Penge https://www.coe.int/en/web/moneyval Komitéen hed tidligere PC- R-EV og blev etableret i 1997 af Europarådets ministerkomité med henblik på at foretage selvevaluering og gensidig evaluering af eksisterende foranstaltninger mod hvidvask i europarådslande, der ikke er medlemmer af FATF. MONEYVAL er et underudvalg under Europarådets Europæiske Udvalg for Strafferetlige Spørgsmål (CDPC).
MOU	Aftalememorandum
MSB	Pengeservicevirksomhed
MVTS	Penge- eller værdioverførselstjenester
NPO	Nonprofitorganisationer
NRA	National risikovurdering
OCG	Organiseret kriminalitetsgruppering

OECD	Organisationen for Økonomisk Samarbejde og Udvikling http://www.oecd.org/ International organisation, som bistår stater i forbindelse med spørgsmål om den økonomiske udvikling i den globale økonomi. OECD huser FATF's sekretariat i Paris.
OFC	Offshore finanscenter
PEP	Politisk eksponeret person
PIC	Privat investeringsselskab
PSD	Direktiv om betalingstjenester
RBA	Risikobaseret metode
ROE	Undersøgelsesrapport
SAR	Rapport om mistænkelige aktiviteter
SNRA	Supranational risikovurdering
SPSP	Udbyder af små betalingstjenester
STR	Indberetninger af mistænkelige transaktioner
TBML	Forretningsbaseret hvidvask af penge
TCSP'er	Udbydere af tjenester til truster og selskaber
TF	Finansiering af terrorisme
TI	Transparency International https://www.transparency.org/ Ikke-statslig organisation med hjemsted i Berlin dedikeret til at øge statslig ansvarlighed og begrænse både international og national korruption. TI blev etableret i 1993 og er aktiv i omkring 100 lande. TI offentliggør "korruptionsnyheder" på sit websted hver dag og tilbyder et arkiv af korruptionsrelaterede nyhedsartikler og rapporter. TI's Corruption Online Research and Information System, eller CORIS, er måske den mest omfattende verdensomspændende database om korruption. TI er bedst kendt for sit årlige korruptionsindeks (CPI), som rangordner lande efter korruption blandt offentligt ansatte; dets indeks over bestikkelsesbetalere (BPI) rangordner de førende eksportlande efter deres tilbøjelighed til bestikkelse. TI's årlige verdensdækkende korruptionsrapport kombinerer CPI og BPI og klassificerer alle lande efter deres samlede

	korruptionsniveau. Listerne hjælper finansielle institutioner med af fastslå den risiko, der er forbundet med en bestemt jurisdiktion.
Ufr	Endelig reel ejer
UCITS	Institutter for kollektiv investering i værdipapirer
UTR	Rapport om usædvanlig transaktion

BILAG 4 – BIBLIOGRAFI

1/ Kommissionens dokumenter

Februar 2016 - Meddelelse fra Kommissionen til Europa-Parlamentet og Rådet om en handlingsplan med henblik på at styrke bekæmpelsen af finansiering af terrorisme
https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52016DC0050

Februar 2019 — Arbejdsdokument fra Kommissionens tjenestegrene om flytningen af kapital og om betalingsfriheden (SWD(2019) 94 final)
https://ec.europa.eu/.../documents/2019-capital-market-monitoring-analysis_en.pdf

Juli 2016 — Ledsagende konsekvensanalyse til forslaget til Europa-Parlamentets og Rådets direktiv om ændring af direktiv (EU) 2015/849 om forebyggende foranstaltninger mod anvendelse af det finansielle system til hvidvask af penge eller finansiering af terrorisme og om ændring af direktiv 2009/101/EF.
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016SC0223&from=EN

November 2016 — Indledende konsekvensanalyse — Import af kulturgenstande.
http://ec.europa.eu/smart-regulation/roadmaps/docs/2017_taxud_004_cultural_goods_synthesis_en.pdf

December 2016 — Ledsagende konsekvensanalyse til forslag til Europa-Parlamentets og Rådets forordning om kontrol med likvide midler, der indføres til eller forlader Unionen og ophævelse af forordning (EF) nr. 1889/2005
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016SC0470&from=EN

Januar 2017 – Indledende konsekvensanalyse – Forslag til et EU-initiativ om begrænsninger af kontante betalinger.
http://ec.europa.eu/smart-regulation/roadmaps/docs/plan_2016_028_cash_restrictions_en.pdf

Januar 2017 - Styrkelse af borgernes rettigheder i en Union med demokratiske forandringer 2017-rapport om unionsborgerskab
https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52017DC0030

Juni 2017 – Arbejdsdokument fra Kommissionens tjenestegrene om forbedring af samarbejdet mellem de finansielle efterretningsenheder
https://ec.europa.eu/newsroom/document.cfm?doc_id=45318

December 2017 - Identifikation af markeds- og reguleringsmæssige hindringer for grænseoverskridende udvikling af crowdfunding i EU
https://ec.europa.eu/info/publications/171216-crowdfunding-regulatory-obstacles-crossborder-development_en

Marts 2018 - Kommissionens forslag til forordning om europæiske europæiske crowdfundingtjenesteudbydere.
https://ec.europa.eu/info/publications/180308-proposal-crowdfunding_en

Marts 2018 - FinTech handlingsplan: For en mere konkurrencedygtig og innovativ finanssektor i Europa
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0109

Januar 2019 - Ordninger for tildeling af statsborgerskab og opholdsret til investorer i Den Europæiske Union
https://ec.europa.eu/info/sites/info/files/com_2019_12_final_report.pdf

Marts 2019 - Meddelelse Fra Kommissionen til Europa-Parlamentet, Det Europæiske Råd, Rådet og Den Europæiske Centralbank Uddybning af Europas Økonomiske og Monetære Union: Status fire år efter de fem formænds rapport.
https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-migration/20190306_com-2019-126-report_en.pdf

2/ Europa-Parlamentets dokumenter

2018 – EP / ECON-Udvalget: The supervisory approach to anti-money laundering: an analysis of the Joint Working Group's reflection paper
http://www.europarl.europa.eu/RegData/etudes/IDAN/2018/624424/IPOL_IDA(2018)624424_EN.pdf

2018 – EP / ECON-Udvalget: Money laundering - Recent cases from a EU banking supervisory perspective
http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_IDA(2018)614496

2018 – EP / ECON-Udvalget: Virtuelle valutaer. Monetary Dialogue July 2018
http://www.europarl.europa.eu/cmsdata/149902/KIEL_FINAL%20publication.pdf

2018 – EP / ECON-Udvalget: Virtuelle valutaer i Eurosystemet: kommende udfordringer. Monetary Dialogue July 2018
http://www.europarl.europa.eu/cmsdata/150541/DIW_FINAL%20publication.pdf

2018 – EP / TERR-Udvalget: Virtual currencies and terrorist financing: assessing the risks and evaluating responses
http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf

2018 - Citizenship and residency by investment schemes in the EU: State of play, issues and impacts
www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2018)627128

3/ Eurostatrapporter

Statistik over personlige pengeoverførsler, Statistik forklaret, Eurostat - 2017.
http://ec.europa.eu/eurostat/statistics-explained/index.php/Personal_remittances_statistics

Handbook on the compilation of statistics on illegal economic activities in national accounts and balance of payments – 2018 edition.
https://ec.europa.eu/eurostat/documents/3859598/8714610/KS-05-17-202-EN-N.pdf/eaf638df-17dc-47a1-9ab7-fe68476100ec

4/ Europolrapporter

Europolrapport: Why is cash still a king? 2015.
https://www.europol.europa.eu/publications-documents/why-cash-still-king-strategic-report-use-of-cash-criminal-groups-facilitator-for-money-laundering

Europol 2016, Vurdering af truslen fra internetorganiseret kriminalitet (IOCTA) 2016.
https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016

The European Union (EU) Serious and Organised Crime Threat Assessment (SOCTA), 2017.
https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017

Europol Financial Intelligence Group, Report '*From suspicion to action'*, 2017.
https://www.europol.europa.eu/publications-documents/suspicion-to-action-converting-financial-intelligence-greater-operational-impact

5/ Andre organer på unionsniveau

ECB, rapporter om betalingsstatistik.

ECB 2014 Working paper on consumer cash usage.
https://www.ecb.europa.eu/pub/pdf/scpwps/ecbwp1685.pdf

January 2017 — ESAs joint opinion on the risks of money laundering and terrorist financing affecting the Union's financial sector.
http://www.eba.europa.eu/documents/10180/1759750/ESAS+Joint+Opinion+on+the+risks+of+money+laundering+and+terrorist+financing+affecting+the+Union%E2%80%99s+financial+sector+%28JC-2017-07%29.pdf

2017 - European Supervisory Authorities' Joint Guidelines, the Risk-Based Supervision Guidelines.
https://esas-joint-committee.europa.eu/Publications/Guidelines/Joint%20Guidelines%20on%20risk-based%20supervision_EN%20%28ESAs%202016%2072%29.pdf

2019 – EBA Report with advice for the European Commission on crypto-assets
https://eba.europa.eu/documents/10180/2545547/EBA+Report+on+crypto+assets.pdf

2019 – ESMA Advice to the European Union Institutions on Initial Coin Offering and Crypto-Assets
https://www.esma.europa.eu/press-news/esma-news/crypto-assets-need-common-eu-wide-approach-ensure-investor-protection

6/ FATF- og Moneyval-rapporter:

2009 – Money Laundering and terrorist financing risks in the securities sector, FATF.
http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20and%20TF%20in%20the%20Securities%20Sector.pdf

2013 – The role of Hawala and other similar services providers in money laundering and terrorist financing, FATF.
http://www.fatf-gafi.org/media/fatf/documents/reports/Role-of-hawala-and-similar-in-ml-tf.pdf

2013 (joint report with Egmont) – Money laundering and terrorist financing ML and TF through trade in diamonds, FATF.
http://www.fatf-gafi.org/media/fatf/documents/reports/ML-TF-through-trade-in-diamonds.pdf

2013 – Money Laundering and Terrorist Financing — Vulnerabilities of Legal Professionals, FATF.
http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20and%20TF%20vulnerabilities%20legal%20professionals.pdf

2013 – The use of online gambling for money laundering and the financing of terrorism purposes (Moneyval).
https://www.coe.int/t/dghl/monitoring/moneyval/Activities/MONEYVAL(2013)9_Onlinegambling.pdf

2015 – Typologies report on Laundering the Proceeds of Organised Crime, Moneyval.
http://www.coe.int/t/dghl/monitoring/moneyval/Activities/MONEYVAL(2015)20_typologies_launderingtheproceedsoforganisedcrime.pdf

2015 – Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL), FATF.
http://www.fatf-gafi.org/media/fatf/documents/reports/Financing-of-the-terrorist-organisation-ISIL.pdf

2018 – Financing of Recruitment for Terrorist Purposes
http://www.fatf-gafi.org/publications/methodsandtrends/documents/financing-recruitment-terrorist-purposes.html

2018 – G20 commitment to implement FATF standards and support for work on crypto assets.
http://www.fatf-gafi.org/media/fatf/documents/reports/FATF-Report-G20-FM-CBG-July-2018.pdf

2018 – Moneyval's Annual report for 2017
https://rm.coe.int/moneyval-annual-report-2017-eng/16808af3c2

2019 – Risk-based Approach for Trust and Company Service Providers
http://www.fatf-gafi.org/publications/fatfrecommendations/documents/rba-trust-company-service-providers.html

2019 – Guidance for a Risk-based Approach for the Accounting Profession
http://www.fatf-gafi.org/publications/fatfrecommendations/documents/rba-accounting-profession.html

2019 – Risk-based Approach for Legal Professionals
http://www.fatf-gafi.org/publications/fatfrecommendations/documents/rba-legal-professionals.html

2019 – Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers.
http://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html

7/ Andre eksterne informationskilder

Assessing the risk of money laundering in Europe — Final Report of project IARM — 31. maj 2017
http://www.transcrime.it/iarm/wp-content/uploads/sites/5/2017/05/ProjectIARM-FinalReport.pdf

Transparency International/Global Witness, European Getaway 2018 – Inside the Murky World of Golden Visas.
www.transparency.org/whatwedo/publication/golden_visas

8 / Fortrolige oplysninger

Der er modtaget oplysninger fra Europol (fortrolige).

9 / Mundtlige og skriftlige bidrag fra følgende interessenter

Kommissionen hørte i juli 2018 medlemsstaterne ved hjælp af et spørgeskema med bilag om:

- nationale risikobegrænsende foranstaltninger
- skabeloner for data om finansielle forhold og retsforfølgning mht. hvidvask af penge og terrorfinansiering, og
- nye risici.

Ved udgangen af 2018 havde Kommissionen modtaget 23 svar. Efterfølgende blev medlemsstaterne yderligere hørt i særlige møder i Ekspertgruppen vedrørende Hvidvask af Penge og Finansiering af Terrorisme den 10. december 2018 og den 11. februar 2019.

I november-december 2018 gennemførte Kommissionen fire workshops med interessenter fra den private-sektor, én med repræsentanter for de finansielle institutioner, to med "udpegede ikke-finansielle virksomheder og erhverv" (DNFBP'er) og én med civilsamfundet (NPO'er) og universitetsverdenen. Anden fase af denne møderunde fandt sted i januar 2019. De mundtlige indlæg fra den private sektor blev suppleret med 15 skriftlige svar.

Nationale sammenslutninger var repræsenteret gennem deres respektive europæiske forbund:

- Accountancy Europe
- Antwerp World Diamond Centre private foundation
- Association for Financial Markets in Europe
- BEUC - Den Europæiske Forbrugerorganisation
- Civil society Europe
- Confédération Fiscale Européenne
- COFACE Families Europe - Sammenslutningen af Familieorganisationer i EU
- Sammenslutningen af Notarer i Den Europæiske Union
- Cultural Action Europe - Det Europæiske Forum for Kunst og Kulturarv
- Electronic Money Association
- Den Europæiske Sammenslutning af Andelsbanker
- Den Europæiske Sammenslutning af Offentlige Banker
- European Association of Real Estate Professions
- European Banking Industry Committee
- Den Europæiske Banksammenslutning
- European Bars (CCBE)

- European Casino Association
- European Federation of Building Societies
- European Federation of Jewellery (EFJ)
- European Foundation Centre
- European Fundraising Association (EFA)
- European Gaming and Amusement Federation
- European Gaming and Betting Association
- European Lotteries
- European Money Association
- European Pari Mutuel
- European Payment Institutions Federation
- Human Security Collective
- Insurance Europe
- Den Internationale Røde Kors Komité
- Det Fælles Forskningscenter for Grænseoverskridende Kriminalitet (TRANSCRIME)
- Law Society of England and Wales
- Leaseurope
- Mastercard
- Moneygram Europe
- NGO Voice
- Open Society Foundation
- PayPal
- Remote Gambling Association
- STEP
- SWIFT
- Università Catolica del Sacro Cuore
- Taxadvisers Europe
- Transparency International EU
- The Association for Financial Markets in Europe (AFME)
- The Council of Bars and Law Societies of Europe
- Trust Europe Affairs (virtual currencies)
- Voice
- Visa
- Western Union Europe.