FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Risikovurdering – hvitvasking og terrorfinansiering

OFFENTLIG VERSJON

JULI 2019

Innhold

1 Innledning

Finanstilsynets hovedmål er å bidra til finansiell stabilitet og velfungerende markeder. For å kunne operasjonalisere hovedmålene, inneholder tilsynets strategi følgende fem delmål:

1. Solide og likvide finansforetak
2. Robust infrastruktur
3. Investorbeskyttelse
4. Forbrukervern
5. Effektiv krisehåndtering
6. Kriminalitetsbekjempelse

Det følger av finanstilsynsloven at tilsynet skal se til at de institusjoner det har tilsyn med, virker på betryggende måte i samsvar med lov og forskrifter samt med den hensikt som ligger til grunn for institusjonenes opprettelse, dens formål og vedtekter.

Finanstilsynets tilsyn er risikobasert. I tilsynet med overholdelsen av finansreguleringen prioriteres ressursbruken ut fra hvilke regler som bygger opp under tilsynets hovedmål og delmål. Risikovurderingen er det overordnede verktøyet for Finanstilsynets risikobaserte tilsyn på hvitvaskingsområdet. På bakgrunn av denne foretas det en risikoklassifisering av rapporteringspliktige under tilsyn for utvelgelse og prioritering av tilsynsobjekter.

Forebygging av hvitvasking og terrorfinansiering er et viktig samfunnsmessig mål, og etterlevelse av hvitvaskingsloven er derfor viktig for den alminnelige tilliten til finansnæringen.

Med unntak av inkassoforetak, gjeldsinformasjonsforetak, pensjonskasser, regulerte markedsplasser og oppgjørssentraler, omfattes alle foretak under tilsyn av hvitvaskingsloven. I 2018 ble også vekslings- og oppbevaringstjenester av virtuell valuta underlagt Finanstilsynets hvitvaskingstilsyn, i tillegg til agenter av utenlandske betalingsforetak.

Lovens formål er å forebygge og avdekke transaksjoner med mulig tilknytning til utbytte av straffbare handlinger eller med mulig tilknytning til terrorhandlinger. Banker og andre foretak under tilsyn har plikt til å gjennomføre kundetiltak, undersøke mistenkelige forhold tilknyttet sine kunder og transaksjoner, og å rapportere til ØKOKRIM der undersøkelsene ikke avkrefter mistanken om at et forhold kan ha tilknytning til utbytte av en straffbar handling.

Finanstilsynet følger opp foretakenes overholdelse av de nevnte pliktene i vurderingen av konsesjonssøknader, på stedlig tilsyn og gjennom tematilsyn. Det legges også vekt på å gi generell veiledning om de pliktene som følger av regelverket. Tilsynet er basert på risikovurderingen som er beskrevet i punkt 2. I vurderingene er det blant annet sett hen til EU-kommisjonens overnasjonale risikovurdering av 2017, veiledninger og anbefalinger foretatt av EU, Financial Action Task Force (FATF) og Det internasjonale valutafondet (IMF).

Risikovurderingen dekker alle tilsynsområder som er omfattet av hvitvaskingsloven. Finanstilsynet har utarbeidet veiledninger til etterlevelse av hvitvaskingsregelverket for det enkelte tilsynsområde. Disse vil oppdateres ved behov.

2 Oppsummering

Risikoen for hvitvasking og terrorfinansiering varierer betydelig mellom tilsynsområdene, men anses som særlig høy i banker, betalingsforetak og hos tilbydere av vekslings- og oppbevaringstjenester av virtuell valuta.

Kundetiltak og løpende oppfølging av kundeforholdet skal foretas på grunnlag av en vurdering av risiko for transaksjoner med tilknytning til utbytte av straffbare handlinger eller tilknytning til terrorfinansiering, der risikoen vurderes ut fra type kunde, kundeforholdet, produkt eller transaksjon mv.

Manglende eller mangelfull etterlevelse av hvitvaskingsregelverket vil kunne medføre at et foretaks iboende risiko øker, til tross for at virksomheten som drives i utgangspunktet har moderat eller lav risiko. Finanstilsynets vurdering er at rapporteringspliktige på de fleste områder under Finanstilsynets tilsyn har forbedringspotensial når det gjelder å etterleve hvitvaskingsregelverket.

Mange av foretakene under tilsyn har en lovbestemt plikt til å oppbevare midler fra sine kunder på klientkontoer. Dette gjelder betalingsforetak, eiendomsmeglingsforetak, advokater som driver eiendomsmegling samt forsikringsformidlingsforetak. I tillegg kommer banker som tilbyr klientkontoer, samt regnskapsførere og revisorer med oppdragsgivere som benytter klientkontoer i sin virksomhet. Etter Finanstilsynets oppfatning foreligger det en særlig risiko for hvitvasking i tilknytning til bruk av klientkontoer. Internasjonale erfaringer viser at hvitvasking kan skje ved at fiktive lån settes opp mellom to parter for å skape finansielle transaksjoner til/fra klientkontoer, noe som legitimerer overføringer av midler med ulovlig opprinnelse. Klientkontoer kan videre misbrukes ved at utbetalinger fra klientkontoen foretas til personer eller foretak som ikke er part i handelen.

Risikoen for at foretaket blir benyttet til hvitvasking og terrorfinansiering kan øke med økt bruk av eksterne tjenestetilbydere, enten disse er innkjøpte systemer, utkontrakterte tjenester eller der den rapporteringspliktige bygger på kundetiltak utført av tredjeparter. Risikoen øker der den rapporteringspliktige ikke har tilstrekkelig kjennskap til det innkjøpte systemet eller tjenestens svakheter og derfor ikke klarer å avhjelpe disse med egne tiltak. Risikoen øker også der de innkjøpte systemene eller tjenestene ikke tilpasses tilstrekkelig til virksomhetens risikovurdering. Når den rapporteringspliktige lar tredjeparter utføre forpliktelser etter hvitvaskingsloven, plikter den rapporteringspliktige å ha tilstrekkelig oppfølging av disse. Manglende oppfølging gjør at foretakene utsetter seg for større risiko for å bli benyttet til hvitvasking og terrorfinansiering.

Fremvekst av kryptovalutaer og vekslingstjenester knyttet til virtuelle valutaer kan øke risikoen for hvitvasking og terrorfinansiering i samfunnet generelt. I Norge er vekslings- og oppbevaringstjenester for virtuelle valutaer rapporteringspliktige etter hvitvaskingsloven fra og med 2018. De forskjellige typene tjenester og produkter tilknyttet virtuell valuta har stor betydning for hvor stor risiko som knytter seg til den rapporteringspliktige. Ettersom disse nylig er definert som rapporteringspliktige, antas det at de i en overgangsfase er forbundet med høyere risiko på grunn av manglende erfaring med regelverket.

Risikoen for hvitvasking og terrorfinansiering kan øke som følge av nye produkter, tjenester og aktører. Dette vil stille økte krav til kundetiltak og oppfølging av kundeforhold for å sikre at foretakene kjenner sine kunder.

Finanstilsynet oppsummerer risikoen for hvitvasking og terrorfinansiering slik:

Type foretak/virksomhet	**Antatt risiko for hvitvasking og terrorfinansiering (før tiltak)**
Banker	Høy
Betalingsforetak	Høy
Virtuell valuta	Høy
Låneformidling	Medium høy
Eiendomsmegling	Medium høy
Verdipapirforetak	Medium høy
AIF-forvaltere	Medium høy
Revisorer og regnskapsførere	Medium lav
Forsikringsforetak	Medium lav
Forsikringsformidlere	Medium lav
E-pengeforetak	Medium lav
Finansieringsforetak	Medium lav
Kredittforetak	Lav
Forvaltningsselskaper for verdipapirfond	Lav
Rapporteringspliktige verdipapirregistre	Lav

3 Banker, kredittforetak og finansieringsforetak

De rapporteringspliktige i denne kategorien er:

a) banker
b) kredittforetak
c) finansieringsforetak
d) filialer av utenlandske finansforetak

Banker, kredittforetak og finansieringsforetak er gjennom sin virksomhet i høy grad utsatt for risiko for hvitvasking og terrorfinansiering. Spesielt banker, som i tillegg til finansiering, tilbyr betalingstjenester og mottar innskudd, er utsatt. Banker som har en global tilstedeværelse, som tilbyr internasjonal betalingsformidling, som tilbyr Private Banking-tjenester, og som har stor eksponering mot utsatte sektorer og bransjer, vurderes å være særlig utsatte for hvitvasking og terrorfinansiering.

Finansieringsforetak er også utsatt for hvitvasking i forbindelse med eksempelvis finansiering av bil og andre objekter, men risikoen er lavere enn for banker, da slike foretak ikke tilbyr betalingsformidling og Private Banking.

For kredittforetak, eksempelvis boligkredittforetak med et enkelt produkttilbud, vurderes risikoen å være lav og begrenset til risiko for hvitvasking via eiendomsmarkedet.
Banker, kredittforetak og finansieringsforetak kan benyttes til hvitvasking og terrorfinansiering på mange forskjellige måter, blant annet:

- Gjennom sin betalingsformidling kan banker motta, oppbevare og kanalisere utbytte fra straffbare handlinger.
- Gjennom sine korrespondentavtaler kan norske banker kanalisere utenlandske aktørers utbytte fra straffbar virksomhet.
- Gjennom sin utlånsvirksomhet kan banker, kredittforetak og finansieringsforetak bidra til å skjule utbytte fra straffbare handlinger. Et eksempel er innvilgede lån som innfris raskt ved salg av finansiert objekt eller ved innbetaling av ekstraordinære avdrag ved bruk av ulovlig midler.
- Gjennom sin virksomhet kan finansforetak bidra til finansiering av terrorisme og spredning av masseødeleggelsesvåpen. Lånebedrageri, herunder forbrukslån og kredittkort, benyttes i større grad for å finansiere fremmedkrigere.

Utviklingen innenfor banker, kredittforetak og finansieringsforetak går både i retning av at risikofylte produkter utfases, men også at nye risikofylte produkter utvikles. Eksempelvis er bruk av sjekk/bankremisser og bruk av kontanter avtagende. Samtidig utvikles nye elektroniske betalingskanaler, som straksbetalingstjenester og mobilbanker, og betalingsformidlingstjenester til og fra utlandet øker. For nye produkter og tjenester kan det være vanskeligere å forutse og avdekke hvordan kriminelle kan benytte disse til hvitvasking og terrorfinansiering. Finansforetakene må også håndtere nye type kunder og forstå risikoen tilknyttet disse, eksempelvis tilbydere av tjenester knyttet til virtuell valuta.

Ulike kjennetegn på hvitvasking eller terrorfinansiering i finansforetak kan være oppdeling av større beløp i hyppige mindre elektroniske overføringer/innskudd til mange mottakere, såkalt "smurfing", eller store elektroniske overføringer/innskudd fra juridiske og fysiske personer som ikke er i samsvar med personens reelle inntektsgivende virksomhet. Foretakene må også være oppmerksomme på muligheten for hvitvasking gjennom eiendomsmarkedet, blant annet ved bruk av manipulerte eiendomsverdier, ved finansiering av utbedringer og oppussinger og i forbindelse med hyppig omsetning av eiendom med ubegrunnet verdiøkning, såkalte "svingdørssalg".

I nasjonal risikovurdering 2018 vises det til at norsk økonomi er preget av store internasjonale bedrifter og tette bånd til utlandet – mange av de største norske bedriftene har også etablert seg i utviklingsland. Dette øker trusselen for alvorlig økonomisk kriminalitet som korrupsjon og skatte- og avgiftsunndragelser. Prispress og konkurranse fra lavkostland bidrar også til at bedrifter kan ta snarveier og eksempelvis begå alvorlig miljøkriminalitet, som ved avfallshåndtering.

Bransjer som opererer internasjonalt, bransjer med vesentlig andel kontantomsetning og arbeidsintensive bransjer vurderes å være spesielt utsatt for hvitvasking eller terror-finansiering. Høy aktivitet og sterk prisstigning i eiendomsmarkedet kan også ha bidratt til å øke risikoen for hvitvasking i eiendomssektoren.

Videre kan merkostnader i finansierte byggeprosjekter, som standardheving og dekning av underestimerte kostnader, dekkes ved ulovlig midler, eller det benyttes fiktive fakturaer.

Det er også en trussel at kriminelle er de reelle eierne i komplekse eierstrukturer som finansieres av finansforetaket.

Truslene forbundet med banker er omfattende og varierer etter produktspekter, geografisk risiko, kundegrupper m.m. Hvitvaskingsrisikoen er høyere for såkalt "private banking" og investeringstjenester grunnet store summer og komplekse eierskapsstrukturer som vanskeliggjør identifisering av reelle rettighetshavere.

Banker er også utsatt for å bli brukt til terrorfinansiering, eksempelvis ved svindel med forbrukslån som benyttes til terrorfinansiering, uten at lånet tilbakebetales. Frivillige organisasjoner kan misbrukes til terrorfinansiering. Ettersom det nå er færre som forsøker å reise til terrorområder, anses trusselen for finansiering av fremmedkrigere redusert fra tidligere år.

Denne gruppen rapporteringspliktige blir også møtt med nye internasjonale tilbydere av finansielle tjenester, herunder av nye tjenester under PSD2, i konkurranse med det tradisjonelle banksystemet. For nye produkter og tjenester kan det være vanskeligere å forutse hvordan kriminelle kan benytte disse til hvitvasking og terrorfinansiering.

Et annet utviklingstrekk er at finansforetak må håndtere nye type kunder og forstå risikoen tilknyttet disse, eksempelvis tilbydere av tjenester knyttet til nye valutamarkeder, eksempelvis kryptovaluta.

Eiendomsmarkedet benyttes for å hvitvaske utbytte, eksempelvis ved at utbedringer og oppussingskostnader betales ved utbytte av kriminell aktivitet, eiendomsverdier manipuleres, profesjonelle aktører tilrettelegger for svingdørsalg mv. Bruk av stråmenn og komplekse eierforhold kan gjøre det vanskelig å avdekke hvitvasking.

4 Forsikringsforetak og forsikringsformidlere

Livsforsikringsforetak, skadeforsikringsforetak, kredittforsikringsforetak og forsikringsformidlere[1] er underlagt hvitvaskingsloven. Pensjonskasser er ikke omfattet.

Generelt er forsikring i begrenset grad anvendelig for hvitvasking, men med noe variasjon avhengig av hvilke typer forsikringsprodukter det gjelder. Skadeforsikring er mindre utsatt enn livsforsikring, og rene risikoforsikringer anses mindre utsatt enn forsikringsprodukter som inneholder elementer av sparing/investering.

Det er mange av de samme typer risiko som gjør seg gjeldende i livsforsikring og skadeforsikring, selv om graden av risiko kan variere. I de fleste tilfeller er graden av risiko størst i livsforsikring. Omtalen i det følgende gjelder både livs- og skadeforsikring med mindre noe annet er angitt særskilt.

[1] Forsikringsformidlere er en samlebetegnelse på forsikringsagenter og forsikringsmeglere. En vesentlig forskjell mellom disse er at forsikringsagenter representerer forsikringsforetak, og forsikringsmegler representerer forsikringstaker.

En del forsikringsavtaler selges gjennom forsikringsformidlere (agenter/meglere). Forsikringsformidlingsforetak er omfattet av hvitvaskingsregelverket, og i utgangspunktet vil det være et ytterligere ledd som har mulighet til å fange opp hvitvaskingsrisiko i tillegg til forsikringsforetaket. Ved bruk av mellommenn antar Finanstilsynet at det likevel vil kunne være en økt risiko for hvitvasking. Risikoen består i at kontrollansvaret kan bli pulverisert ved at forsikringsforetaket i mindre grad gjør egne undersøkelser for å avdekke risikoen for hvitvasking når kunden kommer via en forsikringsformidler. Dette kombinert med at mange forsikringsformidlingsforetak er små foretak med få ansatte, og ikke har de samme ressursene til å følge opp hvitvaskingsregelverket som et forsikringsforetak.

Finanstilsynet fremhever følgende moduser for hvitvasking og terrorfinansiering i forsikring:

- Oppsigelse av forsikringsavtale for å få utbetalt ristorno[2] og feilinnbetaling.
- Inn-/utbetalinger i livsforsikringsavtaler med spare- eller investeringselement i tillegg til forsikringspremien. I livsforsikring med spare-/investeringselement kan en kunde innbetale et større beløp, gjerne i flere omganger over noe tid, i tillegg til at kunden, avhengig av forsikringsvilkårene, har fleksibilitet med hensyn til å kunne si opp avtalen og få utbetalt innestående beløp.
- Forsikring av objekt anskaffet ved ulovlige midler kombinert med svik ved skadeoppgjør, for eksempel tegning av forsikring på en båt som enten er stjålet eller at båten er kjøpt for utbytte av en straffbar handling.

Det er grunn til å anta at potensielle personer som ønsker å foreta hvitvasking, vil gjøre dette med større beløp. Ved "feilinnbetaling" av forsikringspremie kan det bli betydelige beløp som skal tilbakebetales. Dette vil være beløp som kunden har krav på å få tilbake fra forsikringsforetaket.

Det største volumet av avtaler med sparing/investering i norske livsforsikringsforetak er innenfor kollektiv tjenestepensjon. I slike avtaler betales premien av arbeidsgiverforetaket, og alderspensjonen kommer først til utbetaling ved nådd pensjonsalder. Det enkelte medlem i pensjonsordningen har liten påvirkningsmulighet på inn- og utbetalinger, og risikoen for hvitvasking gjennom slike avtaler anses liten. Det kan imidlertid ikke utelukkes at forsikringstakeren (arbeidsgiverforetaket) selv oppretter en kollektiv avtale for å hvitvaske midler.

Forsikringsprodukter som har høyest risiko for hvitvasking, antas å være individuelle livsforsikringsavtaler med stort innslag av spare-/investeringselement og der gjenkjøpsverdien/innestående saldo relativt lett kan realiseres. Dette er typisk investeringsprodukter som har et lite forsikringselement og muligheter for betydelige investeringer.

Hvitvasking av utbytte ved svik gjennom skadeoppgjør anses å være utsatt for hvitvasking.

De fleste norske forsikringsforetak driver hovedsakelig virksomhet i Norge. Unntaket fra dette er sjøforsikringsforetakene med utpreget internasjonal virksomhet.

[2] Forsikringsteknisk uttrykk for tilbakebetaling eller godskriving av for mye innbetalt premie.

Norske livsforsikringsforetak driver i meget begrenset grad livsforsikringsvirksomhet utenfor Norge, og geografisk risiko anses derfor som liten. Finanstilsynet har ingen indikasjoner på at risikoen for hvitvasking varierer geografisk i Norge.

En annen side ved geografisk risiko er forsikringstaker/sikredes opprinnelsesland. Det antas at det er større risiko for at midler fra forsikringsforetaket benyttes til terrorfinansiering der kundens opprinnelsesland er et land som er kjent for å ha baser for terrorvirksomhet.

Totalt sett vurderes risikoen for hvitvasking og terrorfinansiering på forsikringsområdet som medium lav. Det vurderes at individuelle livsforsikringer med spare-/investeringselement har høyest risiko, spesielt der det er mulighet for å innbetale høye beløp og fleksibilitet knyttet til uttak. For små skadeforsikringer i privatmarkedet anses risikoen som lav, typisk innboforsikring, da beløpene som er involvert er lave. Unntak fra dette er verdifulle gjenstander som biler og verdisaksforsikringer der midlene disse gjenstandene er kjøpt for, kan være ulovlige.

5 Betalingsforetak og personer med begrenset tillatelse til å yte betalingstjenester

Et betalingsforetak kan tilby betalingstjenester som er nærmere spesifisert i finansavtaleloven, herunder tilby kunder muligheten å sette inn og ta ut kontanter av en konto, gjennomføring av betalingstransaksjoner, utstedelse av betalingsinstrument, pengeoverføringer mv.

Finansforetaksloven åpner også for at det kan søkes om en begrenset tillatelse til pengeoverføringer. Denne formen for pengeoverføringer utføres ofte av såkalte hawala-foretak.

Grovt sett kan man dele betalingsforetak inn i fire grupper:

1. Store betalingsforetak.

2. Norske betalingsforetak som er etablert for å understøtte andre konsesjonspliktige tjenester/ikke-konsesjonspliktige tjenester, eksempelvis låneformidlings- eller e-pengeforetak eller inkasso.

3. Norske betalingsforetak og utenlandske betalingsforetak som har meldt grensekryssende virksomhet uten etablering eller med bruk av agent, som kun tilbyr betalingstjenesten pengeoverføringer og hvor pengene føres ut av landet. Dette dreier seg stort sett om hawala-foretak.

4. Betalingsforetak som ikke er etablert i Norge som yter øvrige betalingstjenester, eksempelvis gjennom fintech-selskap.

For betalingsforetak med begrenset tillatelse og grensekryssende virksomhet kan pengeoverføringer bli misbrukt av kriminelle fordi dette er en rask og enkel måte å flytte utbytte over landegrenser. Det er videre vanskelig å spore pengene, særlig når de overføres til konfliktområder. Slike pengeoverføringer er en særlig vanlig modus i hvitvaskingssaker. Det er grunn til å anta at betalingsforetakene blir brukt for å hvitvaske penger fra kriminell virksomhet, herunder av personer som har arbeidet svart og ønsker å overføre pengene ut av landet. Denne type tjenester er også attraktive for aktører som ønsker å finansiere terror. Foretak som yter tjenesten pengeoverføringer, og særlig agenter av betalingsforetak, er identifisert som en trussel i innledende stadier hvor ulovlige inntekter i form av kontanter introduseres/plasseres i det finansielle systemet.

For øvrige betalingsforetak er det mange av de samme truslene som gjør seg gjeldende, med unntak av muligheten til grensekryssende overføringer. Selv om det er stor variasjon i tjenestetilbudet, anser Finanstilsynet en rekke av disse å være godt egnet til hvitvasking og terrorfinansiering. Eksempelvis vanskeliggjør "straksbetaling"-elementet i denne typen betalingsforetak nødvendig kontroll og undersøkelser.

I ØKOKRIMs trusselvurdering er det pekt på to viktige utviklingstrekk innen økonomisk kriminalitet: digitalisering og globalisering. Digitale betalingsplattformer brukes om app-er og internettbaserte programmer. Disse kan brukes til å gjennomføre en betalingstransaksjon i stedet for nettbank. Betalingsplattformene kan være tilknyttet tradisjonell bankvirksomhet, men også betalingsforetak. I henhold til ØKOKRIM er de nye betalingsplattformene/ -løsningene brukt ved oppgjør mellom kriminelle.

Selv om nyere betalingstjenester ofte er mer sporbare enn kontanter, viser erfaring at det likevel er vanskeligere å spore når transaksjonen sendes til eller fra nye betalingsløsninger som ikke har Norge som hjemland.

Mange fintech-selskaper og andre betalingsforetak med bakenforliggende bankforbindelse vil ønske å drive virksomhet i flere land, fordi digitaliseringen gjør dette enklere. Det er foreløpig ikke mange aktører som har fått tillatelse på dette grunnlaget, men det antas at dette vil endres med ikrafttredelse av PSD2 i Norge.

Pengeoverføringer må antas å representere den største risikoen for hvitvasking og terror-finansiering, slik foretakene drives i dag. Når pengeoverføringen tilbys over landegrensene, eller til konfliktområder, øker risikoen. Det er utbredt bruk av kontanter ved overføringer gjennom betalingsforetak og agenter. Sett sammen med at betalingsforetakenes og agentenes gjennomføring av kundekontroll ofte er utilstrekkelig, gjør dette at disse er svært anvendelige for hvitvasking av ulovlig ervervede midler.

Enkelte utenlandske betalingsforetak synes å benytte seg av pengetransport for å frakte kontanter ut av landet. Bakgrunnen for dette er at agentene deres har vanskeligheter med å opprette konto i norske banker for videreføring av pengene. Finanstilsynet har fått tilbakemelding om at bankene nå heller ikke ønsker å gjennomføre bulktransaksjoner for norske betalingsforetak. Dette vil medføre økte kostnader for hver enkelt transaksjon og kan lede til en økt bruk av pengetransport for å frakte penger ut av landet. Når det gjelder utenlandske betalingsforetak vil det at kontanter blir fraktet ut av Norge via penge-transportører, innebære at det er liten eller ingen kontroll med pengenes opprinnelse eller hvor de skal, da det ikke blir registrert i valutaregisteret at pengene i realiteten føres ut av landet av et betalingsforetak. Videre blir reell mottaker ikke registrert. Det er selskapet som fysisk fører

pengene ut av landet som blir registrert i registeret. Dette medfører at det er svært høy risiko for at pengene kan ha illegalt opphav. Videre er det risiko for at summen som faktisk føres ut av landet, er større enn den som blir oppgitt til fraktselskapet, da det ikke gjennomføres kontroll av summene som er oppgitt.

Betalingsforetak, og særlig produktet pengeoverføringer, har en iboende høy risiko for å bli brukt til hvitvasking og terrorfinansiering.

6 E-pengeforetak

E-pengeinstrumenter kan i hovedsak deles i følgende kategorier:

1. Forhåndsbetalte kort. Kortet kan være personlig (identifisert kortholder) eller upersonlig (anonym kortholder). Upersonlige kort tillates utstedt etter hvitvaskingsregelverket dersom det er knyttet beløpsgrenser til kortene.

2. Vouchers. Vouchers ligner på forhåndsbetalte kort, men fordi voucheren ofte er en kode lagret på et elektronisk medium, er disse enklere å sende til personer over hele verden.

3. E-lommebok. En e-lommebok er en digital e-pengekonto som det knyttes ett eller flere betalingsinstrument til, eller som det kan utføres betalingstransaksjoner fra uten bruk av betalingsinstrument. Kunden vil som regel kunne sette midler inn på sin e-lommebok til enhver tid.

E-penger kan benyttes i den utstrekning brukerstedet aksepterer det. Flere e-pengeutstedere har inngått avtaler med kortselskaper som Visa og Mastercard for å sikre aksept av brukersteder.

Moduser for hvitvasking og terrorfinansiering ved bruk av e-pengeforetak er blant annet:

- Bruk av anonyme e-penger. Anonyme e-penger som anskaffes med kontanter og uten kundekontroll, er velegnet til å skjule pengenes opprinnelse, samt brukeren av e-pengene. Bruk av anonyme kort er internasjonalt en velkjent metode for hvitvasking og terrorfinansiering.
- Bruk av mellommann.
- Bruk av andres identitet.

I følge Nasjonalt tverretatlig analyse- og etterretningssenters (NTAES) trusselvurdering utgjør norske anonyme forhåndsbetalte kort en moderat trussel innen økonomisk kriminalitet. De benyttes i stor grad til taktiske valg som et verktøy i den kriminelle handlingen for å skjule spor. Et utvalg straffesaker som er gjennomgått, viser at kortene benyttes til å hvitvaske et mindre utbytte, for å skjule spor og overføre anonymt i innland og utland.

Utenlandske anonyme og personlige forhåndsbetalte kort utgjør en betydelig større trussel enn norske forhåndsbetalte kort fordi beløpsgrensene ved bruk er høyere på de utenlandske kortene (alt fra 15 000 kroner i uken, til ubegrensede beløp).

NTAES peker på at tjenesten e-lommebøker ved flere tilfeller er benyttet i forbindelse med økonomisk kriminalitet. E-lommebøker er enkelt tilgjengelig på nett, lette å bruke og kan benyttes i et stort utvalg av norske og utenlandske nettbutikker. Tjenestene tilbys over hele verden. Dette gjør tjenesten egnet til å flytte utbytte av økonomisk kriminalitet ut av landet med begrenset sporbarhet.

Politi- og kontrolletatene har sett at forhåndsbetalte kort i økende grad benyttes ved utøvelse av økonomisk kriminalitet. Bruk av vouchers og e-lommebøker i forbindelse med økonomisk kriminalitet forventes også å være stabil.

Finanstilsynet har i nyere tid opplevd en nedgang i antall norske e-pengeforetak, og det forventes ikke at antallet vil øke igjen i nær fremtid. Utviklingen i Europa generelt synes imidlertid være motsatt.

Anonyme forhåndsbetalte kort og vouchers innebærer høy risiko for hvitvasking og terrorfinansiering. Produktene kan kjøpes anonymt med kontanter, men er begrenset til relativt små beløp per kjøp. Det er ingen kundekontroll for denne type kjøp. Betalingskortet lastes opp med et visst beløp og kan brukes til kjøp ved et stort antall brukersteder i Norge og utlandet. Vouchers kan benyttes for kjøp av varer og tjenester på internett. Undersøkelser knyttet til enkelte produkter viser at det de siste årene er utstedt elektroniske penger for relativt betydelige beløp.

E-lommebøker og ikke-anonyme forhåndsbetalte kort har medium lav risiko for å bli benyttet til hvitvasking og terrorfinansiering. Til tross for den høye risikoen forbundet med anonyme forhåndsbetalte kort som produkt, synes ikke risikoen for hvitvasking og terrorfinansiering i norske e-pengeforetak som sådan å være høy. Totalt sett anses risikoen å være medium lav.

7 Verdipapirområdet

Foretak på verdipapirområdet som er omfattet av hvitvaskingsregelverket:

- verdipapirforetak
- forvaltningsselskaper for verdipapirfond
- rapporteringspliktige verdipapirregistre
- depotmottakere
- forvaltere av alternative investeringsfond

Både omsettelige verdipapirer, fondsandeler og derivater kan benyttes til hvitvasking eller for å gjennomføre transaksjoner i forbindelse med terrorfinansiering. Fysiske verdipapirer (eksempelvis ihendehaverobligasjoner, utenlandske fysiske verdipapir mv.) vil på samme måte som veksler og kontanter kunne anvendes for hvitvasking, men disse aksepteres normalt ikke av norske verdipapirforetak/forvaltningsselskaper. Foretakene må likevel være

oppmerksomme på forhold knyttet til midlenes opprinnelse, og særlig dersom dette er verdipapirer som er overført fra, eller føres hos tredjeparter.

Lavere grad av transparens er felles for alle produkter og tjenester med en høyere risiko for hvitvasking og terrorfinansiering innenfor området. Transaksjoner med færre kontrollinstanser innebærer økt risiko og krever tiltak og dokumentasjon fra foretakene.

Verdipapirer omsettes i stor grad internasjonalt og på flere markeder. Eierskap til verdipapirene kan også være i strukturer som krysser grenser, og kunnskap om reelt eierskap er en kjerneproblemstilling når det gjelder tiltak mot hvitvasking og terrorfinansiering på verdipapirområdet.

Når det gjelder hvitvaskingsrisiko deles det internasjonale markedet gjerne inn i høyrisiko- og lavrisikoland. De typiske "skatteparadisene" med stor grad av sekretesse har en høy risiko. Disse landene har ingen eller svært lave skatter, samt et regelverk med sterke restriksjoner på innsyn, mulighet for å tilsløre selskaps- og stiftelsesstrukturer og manglende offentlige registre. Slike strukturer kan misbrukes til kriminalitet både i form av skatteunndragelse og hvitvasking av midler.

Likvide finansielle instrumenter som handles på regulerte markedsplasser kan være ettertraktet i en tilsløringsfase siden enkelttransaksjoner vil være lite synlige. Slik handel kan gi legitimitet og gir mulighet til å flytte store verdier uten at det vekker oppsikt.

Unoterte aksjer, og til en viss grad lavt prisede og mindre likvide noterte verdipapirer, kan være attraktive for hvitvasking. Særlig gjelder dette der eierskapet i unoterte aksjer er registrert hos utsteder eller hos foretak som ikke er verdipapirregister. Verdipapirene kan også benyttes som andeler i rene skallselskaper med hensikt å drive hvitvasking, innsidehandel, markedsmanipulasjon eller annen verdipapirsvindel. Unoterte aksjer kan også misbrukes i en plasseringsfase, og det samme gjelder til en viss grad lavt prisede og mindre likvide noterte rentepapirer. Det kan avtales transaksjoner basert på fiktive verdier, som kan gjøre utbytte av straffbare handlinger "hvitt" gjennom salg av papirene.

Unoterte derivater har lav transparens og kan konstrueres med formål å overføre midler fra en part til en annen. OTC-kontrakter kan være rene bilaterale kontrakter, og i den grad de "cleares", er dette relativt nye ordninger som ikke har vært under tilsyn tidligere. Omfanget av data og usikkerhet rundt datakvaliteten på "clearede" OTC-derivater kan øke risikoen for at slike produkter blir benyttet til hvitvasking.

Forsikringsprodukter er ikke-finansielle instrumenter etter verdipapirhandelloven, men kan ha likheter med finansielle instrumenter. I noen grad er finansielle instrumenter sentrale elementer av forsikringsproduktet uten at forsikringstager står som eier av disse. Forsikringsprodukter inngår i produkter som verdipapirforetak kan gi råd om. Selv om forsikring er strengt regulert, er det mulig å sette opp eller handle et forsikringsprodukt slik at midler overføres fra en part til en annen som et ledd i hvitvasking eller terrorfinansiering. Et forsikringsprodukt er normalt ikke registrert andre steder enn hos forsikringsselskapet, noe som gir produktene lavere transparens.

I forbindelse med selskapshendelser, eksempelvis oppkjøp, fusjoner mv., kan det være at verdipapirer og derivater inngår som en del av oppgjøret, eksempelvis ved at det utstedes

aksjer eller opsjoner som oppgjør for overtagelse av andre aksjer. Dette kan struktureres for å overføre midler fra en part til en annen og tilsløre midlenes opprinnelse.

Verdipapirkontoer benyttes for oppbevaring av verdipapirer, samt i verdipapiroppgjøret av handel. Disse kontoene kan benyttes til hvitvasking og terrorfinansiering. Ved opprettelse av konto i et verdipapirregister er det derfor viktig at kontoførere gjennomfører betryggende hvitvaskingskontroll.

Overføringer fra konto til konto uten finansielt oppgjør benyttes til korreksjoner og i enkelttilfeller som for eksempel ved arv eller gave. Denne typen transaksjoner er spesielt utsatt for flytting av formue og krever særskilte rutiner hos foretakene.

Bruk av forvalterkontoer (nominee), samlekontoer, skallselskap og strukturer for formuesmasser med begunstiget (trusts) er modus for hvitvasking. Det kan også være mulig å overføre verdipapirer igjennom veldedige stiftelser og andre ideelle organisasjoner i den hensikt å skjule hvitvasking eller terrorfinansiering.

Uregulerte investeringsstrukturer og strukturer underlagt begrenset regulering kan være etablert eller kontrollert for hvitvaskingsformål. Disse strukturene omfatter blant annet AIF-er og ulike syndikerte produkter. Det er en forhøyet risiko for at motpartene til slike strukturer ikke kjenner identiteten til investorene som står bak. Forvaltere for investeringsalternativer med eget andelseierregister, verdipapirfond og AIF-er har i mange tilfeller også færre kontrollmuligheter med hensyn til midlers opprinnelse og kundekontroll enn strukturer som er registrert i et eksternt register.

Overføring av midler er mulig gjennom fiktiv prissetting av verdipapirer. Noterte aksjer og andre verdipapirer som handles direkte på børs har stor grad av transparens i prisingen, men for obligasjoner og unoterte verdipapirer kan prisen manipuleres, særlig der det ikke foreligger noen tradisjonelle prisingsmekanismer eller kontroll med prisingen i handler. Som nevnt kan OTC-derivater struktureres og prises med det formål å overføre verdier fra en part til en annen.

Det er svært få observasjoner av hvitvasking/terrorfinansiering på verdipapirområdet. Det er også svært få rapporter om mistenkelige transaksjoner fra aktørene i verdipapirmarkedet. Begrenset rapportering til ØKOKRIM kan imidlertid også være tegn på underrapportering. Det har vært enkelte narkotika- og svindelsaker som også har omfattet tilsløring/integrering av illegale midler gjennom verdipapirer.

Markedsplassene

Regulerte markedsplasser har krav om medlemskap og etterlevelse av bestemte standarder og er ikke særlig utsatt for hvitvasking. Selv om noen OTC-markeder er organiserte og har automatisert prisstilling, kan det i mindre grad være etablert krav til de som er notert, og det er generelt svakere kontroll med transaksjoner. Det samme gjelder multilaterale handelsfasiliteter (MTF-er) som verdipapirforetak og markedsoperatører som kan ha tillatelse til å drive. Medlemmene på slike handelsfasiliteter kan være uregulerte foretak, selv om det ikke er observert i norske MTF-er per i dag. Enkelte handelsmuligheter har begrenset innsyn og kontroll i handelsøyeblikket, men vil bli regulert i etterkant av handelen (eksempelvis "dark pools").

Uregulerte handelsplattformer og handelsplattformer etablert i land med svakere kontroll, herunder plattformer som handler CFD- og binære opsjoner, er trolig mer utsatt for å bli benyttet til hvitvasking og terrorfinansiering.

Verdipapirforetak

Verdipapirforetak som yter rådgivning kombinert med ordreformidling kan være attraktive for å tilsløre og integrere hvitvaskede midler, særlig på grunn av de store verdiene og kompleksiteten i produkttilbudet.

Finanstilsynet har observert at identifikasjonen av kunder og reelle rettighetshavere, samt innhenting av kundedokumentasjon, er manglende eller mangelfull hos flere av verdipapirforetakene. Det ligger en klar risiko i at foretakene ikke fullt ut kjenner kunden.

Etterlevelsen av verdipapirregelverkets krav om, og foretakets behov for kjennskap til, kunden ved ytelse av investeringstjenester gjør at verdipapirforetak er mindre attraktive for personer som ønsker å tilsløre hvitvasking.

Så langt Finanstilsynet kjenner til, er det svært få observasjoner av hvitvasking fra verdipapirforetak. Det er også få rapporter til ØKOKRIM om mistenkelige transaksjoner fra andre aktører i verdipapirmarkedet. Rapporteringshyppigheten er svært varierende. Dette kan tyde på at bevisstheten og evnen til å avdekke hvitvasking varierer mellom foretakene, eller at foretakenes produkter er lite egnet til hvitvasking.

Forvaltningsselskaper for verdipapirfond og AIF-forvaltere

Verdipapirfond anses i utgangspunktet lite egnet til å plassere ulovlig ervervede midler i. Verdipapirfond er transparente og dermed også lite egnet i tilsløringsfasen, men vil kunne være et mål for endelig integrering av ulovlige midler. Om det benyttes forvalterregistrering, er det lite kontroll med andelseierregisteret. Hvis verdipapirfondene inngår i et forsikrings-produkt som skal omsettes, øker risikoen for hvitvasking og terrorfinansiering i produktene.

Verdipapirfondsandeler skal registreres i et andelseierregister. Norske forvaltningsselskaper benytter VPS eller fører og opprettholder eget register til dette formålet. Andelseier kan forvalterregistreres i registeret, hvilket gir høyere risiko for at midlene tilsløres. Norske forvaltere av fond som markedsføres i utlandet, har begrenset mulighet for å kontrollere opprinnelsen til de investerte midlene ved bruk av forvalterregistrering. Forvaltere fra EØS-området vil imidlertid ha tilsvarende plikter etter hvitvaskingsreglene som det norske forvaltningsselskapet. Tilsvarende vil andre distributører av verdipapirfond, herunder verdipapirforetak, være omfattet av hvitvaskingsreglene.

Alternative investeringsfond er ikke en homogen gruppe, og kan på forskjellig vis være utsatt for tilsløring og integrering av illegale midler. Forvaltere av alternative investeringsfond kan ha begrenset mulighet til å kontrollere opprinnelsen til de midlene som investeres i andelene, og Finanstilsynet observerer at de i noen grad aksepterer tingsinnskudd. Alternative investeringsfond har ofte et begrenset antall kunder med større andel av fondet, og andelseierne har dermed også større påvirkningsmulighet i fondet. Verdsettelsen av alternative investeringsfond kan også være vanskeligere å etterprøve, noe som kan gi mulighet for fiktiv verdsetting og overføring av verdier. Alternative investeringsfond som forvaltes av registrerte forvaltere, har ikke krav om depotmottaker. Disse elementene

innebærer større risiko for hvitvasking og terrorfinansiering i alternative investeringsfond sammenliknet med verdipapirfond.

8 Revisorer og regnskapsførere

Revisorer og regnskapsførere skiller seg fra en del andre rapporteringspliktige ved at det ikke går betalingsstrømmer gjennom revisjons- og regnskapsførerforetak. At et foretak benytter et autorisert regnskapsførerselskap eller det at et foretaks regnskaper er revidert, kan gi inntrykk av at foretakets virksomhet drives lovlig og under betryggende kontroll, herunder at hvitvasking eller terrorfinansiering ikke forekommer. Dette kan gjøre at foretaket unngår mistanke om hvitvasking eller terrorfinansiering, og derfor ikke velges ut for kontrolltiltak som kunne avdekket hvitvasking eller terrorfinansiering.

Forhold på oppdragsgivers side kan føre til økt risiko for at revisor eller regnskapsfører blir benyttet til hvitvasking eller terrorfinansiering. I utførelsen av revisjons- eller regnskaps-føreroppdrag må revisor og regnskapsfører derfor identifisere forhold på oppdragsgiversiden som kan indikere hvitvasking eller terrorfinansiering. Revisorer og regnskapsførere kan også opptre som rådgivere.

Oppdragsgivere kan drive virksomhet i bransjer der hvitvasking eller terrorfinansiering forekommer oftere enn i andre bransjer. Eksempler på særlig utsatte bransjer er entreprenør-virksomhet, restaurantvirksomhet samt spill- og lotterivirksomhet. Eksempler på forhold som *kan* indikere hvitvasking eller terrorfinansiering er:

- transaksjoner som synes å mangle et legitimt formål, er uvanlige i forhold til oppdragsgivers kjente forretningsmessige eller personlige transaksjoner, foretas til eller fra et land eller område uten tilfredsstillende tiltak mot hvitvasking eller terrorfinansiering, eller er uvanlig store eller komplekse
- mottatt faktura med merverdiavgift uten at avsender er registrert i merverdiavgiftsregisteret
- fakturering av fiktive varer eller tjenester
- selskap med lav aktivitet som mottar store pengesummer uten en åpenbar bakenforliggende hendelse
- kapitalinnskudd der pengene kommer fra en uidentifiserbar innskyter
- underslag der ledelse og eiere er involvert
- kompliserte selskapsstrukturer uten at det foreligger en naturlig juridisk eller økonomisk grunn til dette
- ulovlige lån til aksjonærer eller lån fra ansatte til arbeidsgiver

Forhold på revisor og regnskapsførers side kan også medvirke til økt risiko for at revisor eller regnskapsfører blir benyttet til hvitvasking eller terrorfinansiering. Den generelle sårbarheten ved utføringen av revisjonstjenester og regnskapsførertjenester er at revisor eller regnskapsfører:

- gjennom sin oppdragsutførelse og yrkestittel bidrar til å skape tillit til virksomhet som er involvert i hvitvasking eller terrorfinansiering. Dette gjelder selv om revisor eller regnskapsfører ikke har mulighet til å avdekke at hvitvasking eller terrorfinansiering skjer;
- ikke etterlever kravene i hvitvaskingslovgivningen eller lovgivning knyttet direkte til virksomhetsutførelsen på en tilfredsstillende måte, og at dette er grunnen til at det ikke oppdages at oppdragsgiver er involvert i hvitvasking eller terrorfinansiering;
- bevisst medvirker til hvitvasking eller terrorfinansiering gjennom å velge ikke å gripe inn når de ser at oppdragsgiver eller oppdragsgivers forretningsforbindelser er involvert i hvitvasking eller terrorfinansiering;
- bevisst medvirker til hvitvasking eller terrorfinansiering gjennom å tilskynde til eller tilrettelegge for at oppdragsgiver alene eller i samarbeid med andre hvitvasker utbytte fra kriminelle handlinger slik at transaksjonen skjules som en ordinær post i oppdragsgivers regnskap.

Revisors eller regnskapsførers sårbarhet vil videre være avhengig av profesjonaliteten i og størrelsen på revisor- eller regnsapsførerselskapet. Mindre selskaper eller enkeltpersonforetak som driver virksomhet uten å være del av et nettverk, vil kunne være mer sårbare for å bli utnyttet til hvitvasking eller terrorfinansiering enn større selskaper som er del av et nettverk eller på annen måte mer profesjonelt drevet. På den annen side kan større revisjons- eller regnskapsførerselskaper, herunder selskaper som inngår i et internasjonalt nettverk, være mer sårbare for å bli involvert i et multinasjonalt hvitvaskings- eller terrorfinansieringsopplegg.

Risikoen for at den enkelte revisor eller regnskapsfører blir benyttet til hvitvasking eller terrorfinansiering beror på dennes vurdering av trusselbildet og sårbarheter ved egen virksomhet. Videre beror risikoen på revisors eller regnskapsførers profesjonalitet og kompetanse, herunder i utarbeidelser og etterlevelse av gode rutiner og retningslinjer, samt utførelsen av oppdrag i overensstemmelse med hvitvaskingslovgivning. Ved manglende vurderinger og oppmerksomhet på hvitvaskingslovgivningen kan revisor eller regnskapsfører bidra til at underliggende straffbare forhold skjules bak den tilliten som allmenheten har til revisor og regnskapsfører.

Revisorer og regnskapsførere anses å ha medium lav risiko for å bli benyttet til hvitvasking og terrorfinansiering.

9 Eiendomsmeglere og advokater som driver eiendomsmegling

Fast eiendom er kapitalintensiv, og hvitvasking av store beløp kan gjennomføres i én operasjon. Store illegale beløp kan investeres i fast eiendom, og deretter re-investeres og integreres i den legale økonomien med relativt liten risiko for tap ved senere salg eller utleie av eiendommen. Eiendomsmeglingsvirksomheter bistår selgere og kjøpere med eiendomsoverdragelser/-utleie og transaksjoner som oppgjør av kjøpesummer og utbetaling av leieinntekter. Dette er typer tjenester som benyttes av kriminelle for å hvitvaske illegale midler.

I tillegg til den ordinære eiendomsmeglingsvirksomheten kan megler påta seg oppdrag med å anslå verdier på fast eiendom. Slik Finanstilsynet ser det, kan utferdigelse av slike verdivurderinger også være en tjeneste som benyttes av kriminelle for å hvitvaske illegale midler.

På samme måte som andre kriminelle handlinger, blir terrorhandlinger ofte finansiert gjennom en kombinasjon av legale inntekter og utbytte av kriminalitet. Det er dermed en mulighet for at midler utbetalt fra meglers klientkonto kan benyttes til å finansiere terror. Finanstilsynet antar at vurderingen av risiko for terrorfinansiering langt på vei er sammenfallende med de vurderinger som gjøres for hvitvasking.

Potensielle fremgangsmåter for hvitvasking og terrorfinansiering gjennom eiendoms-meglingsvirksomhet utført av eiendomsmeglingsforetak og advokatmeglere er blant annet:

- Kontant betaling av fast eiendom er den mest åpenbare metoden for plassering av illegale midler. Der oppgjør av eiendomshandelen gjennomføres av megler, er kontant betaling etter Finanstilsynets oppfatning ikke en særlig praktisk måte å hvitvaske på. Finanstilsynet er imidlertid kjent med tilfeller hvor oppgjøret bare delvis gjennomføres av eiendomsmeglingsforetaket, samtidig som at partene gjør opp deler av kjøpesummen direkte mellom seg. Dette direkteoppgjøret kan gjennomføres med illegale midler.

- Overføringer av illegale midler til klientkonto fra finansinstitusjon. Eiendoms-meglingsvirksomheter kan også motta overføringer av illegale midler (egenkapital) via det finansielle systemet. Midlene hvitvaskes ved utbetaling til selger.

- Annen bruk av klientkonto. Internasjonale erfaringer viser også at hvitvasking kan skje ved at fiktive lån settes opp mellom to parter for å skape finansielle transaksjoner til/fra klientkontoer, noe som legitimerer overføringer av midler med ulovlig opprinnelse. Finanstilsynet har erfart tilfeller hvor advokaters klientkontoer er benyttet til et stort antall finansielle transaksjoner som er eiendomshandelen uvedkommende. Finanstilsynet har videre erfart at klientkontoer videre kan misbrukes ved at utbetalinger fra klientkontoen foretas til personer eller foretak som ikke er part i den aktuelle eiendomshandelen. Etter Finanstilsynets oppfatning medfører slike utbetalinger en mulighet for at selgers nettoproveny unndras fra beskatning eller kreditorforfølgelse.

- Illegale midler inkorporeres i eiendommen. Eiendommen kan være ervervet med legale midler, og renoveres med illegale midler eller ved hjelp av svart arbeid. Når eiendommen så selges eller leies ut ved hjelp av megler, blir de illegale midlene hvitvasket og integrert i den legale økonomien.

- Manipulasjon av eiendommens verdi. Eiendommens verdi kan fastsettes enten under eller over reell markedsverdi, enten direkte ved at partene avtaler lav eller høy pris i forhold til reell markedsverdi, ved bruk av falske verdivurderinger, eller indirekte ved bruk av falske leiekontrakter eller ved å angi at deler av kjøpesummen utgjøres av inventar, løsøre, driftsutstyr, goodwill eller annet som er vanskelig å fastsette pris for.

- Lånebedrageri. Meglere kan misbrukes til hvitvasking ved lånebedrageri gjennom å motta lånebeløpet på klientkonto og deretter utbetale nettoprovenyet til selger. Selve lånebedrageriet kan gjennomføres ved bruk av falske dokumenter som angir for høy takst, falske leiekontrakter eller lønnsslipper mv. Megler kan også medvirke ved å avgi uriktige bekreftelser om at egenkapitalen er gjort opp.

- Bruk av stråmenn, kompliserte selskapsstrukturer, utenlandske foretak, blanko-skjøter. Utbytte fra kriminelle handlinger kan plasseres i fast eiendom gjennom stråmenn eller lovlige selskaper. Selskapene kan ha kompliserte eierforhold, herunder også utenlandske selskaper hvor det ikke lar seg gjøre å få innsyn i identiteten til de reelle eierne. ØKOKRIM har sett flere eksempler på bruk av blanko-skjøte som verktøy for å hvitvaske utbytte fra straffbare handlinger. Blanko-skjøte er et lovlig instrument som brukes f.eks. der eiendommen skal selges videre, og man ikke ønsker å betale kostnadene ved å etablere rettsvern i første overføring. ØKOKRIM legger til grunn at blanko-skjøte benyttes for å anonymisere og skjule bakmenn.

Internasjonale erfaringer viser at kjøp av fast eiendom er en av de mest benyttede metoder for å hvitvaske utbytte fra kriminalitet. Finanstilsynet er ikke kjent med kilder som omtaler utsatte produkter og tjenester ved eiendomsmegling i utlandet.

Eiendomsmeglingsvirksomheter har en lovbestemt plikt til å oppbevare midler fra sine kunder på klientkontoer. Etter Finanstilsynets oppfatning foreligger det en særlig risiko for hvitvasking i tilknytning til bruk av klientkontoer, enten ved å motta illegale midler, overføre midler i transaksjoner som legitimerer midlene, eller ved utbetaling til andre enn partene i handelen. Virksomheter som ikke har utkontraktert oppgjøret til annet foretak, og som dermed benytter klientkonto i sin virksomhet, har dermed høyere risiko for å bli brukt til hvitvasking enn virksomheter som ikke gjennomfører oppgjør.

Eiendomsmeglingsvirksomheter er forskjellige både i størrelse og tjenestetilbud. Når det gjelder størrelse, vil virksomheter med høy markedsmessig betydning ha en høyere iboende risiko på grunn av antallet transaksjoner. På den andre siden har helt små virksomheter, etter det Finanstilsynet erfarer, generelt svakere rutiner og dårligere etterlevelse av regelverket, og de har høyere iboende risiko for hvitvasking av den grunn. Dette gjelder særlig advokatmeglere, som ikke er underlagt forskrift om risikostyring og internkontroll, og som normalt heller ikke benytter meglersystemer hvor anti-hvitvaskingstiltak er implementert i saksbehandlingsrutinene, og som dermed ikke har det samme grunnleggende rammeverket rundt virksomheten som eiendomsmeglingsforetakene har.

Når det gjelder risikoer forbundet med tjenester det enkelte eiendomsmeglingsforetak yter, kan det skilles mellom produktene utleiemegling, salgsmegling (inklusive oppgjør) samt rene oppgjørsoppdrag. Finanstilsynet vurderer salg av fast eiendom til å være mer attraktivt for hvitvasking enn utleiemegling, på bakgrunn av muligheten for hvitvasking av høyere verdier og kortere tidsperspektiv før midlene er hvitvasket. Der oppdraget omfatter oppgjør, vil det være mulighet for hvitvasking ved gjennomføring av transaksjonen, og risikoen vil være høyere. Ved oppdrag som kun omfatter oppgjør, anses risikoen for hvitvasking å være høyest ettersom megler da antas å ha noe lavere kjennskap til både partene i handelen og eiendommen. Etter det Finanstilsynet erfarer, utgjør oppgjørsoppdrag en stor andel av oppdragene hos advokatmeglerne. Disse har dermed også av denne grunn en høyere risiko enn eiendomsmeglingsforetakene.

Eiendomsmeglingsvirksomhetene opererer i ulike markeder. Det viktigste skillet går mellom næringsmegling og boligmegling. Det antas å være en større risiko ved næringsmegling, på bakgrunn av mulighet til å bruke kompliserte selskapsstrukturer og/eller utenlandske eiere som eiendomsmeglingsvirksomheten ikke kan identifisere. Videre antas det å være vanskeligere å vurdere om prisen på næringseiendom er markedsmessig eller ikke, og det foreligger en større mulighet til å manipulere eiendomsverdien ved bruk av f.eks. falske leiekontrakter. Risikoen vurderes videre å være noe lavere ved ordinær boligmegling, hvor flertallet av kundene er privatpersoner og formålet er egen bruk. Der transaksjonen etter sitt formål inngår i "oppussingsmarkedet", altså ved kjøp av oppussingsobjekt som renoveres og siden selges for en høyere pris, antas imidlertid risikoen å være høy. Finanstilsynet anser også risikoen å være noe høyere ved den delen av boligmeglingen som omfatter boliger under oppføring, hvor selger ofte er juridiske personer og hvor det tidligere var vanlig med re-salg (kjøp og videresalg før ferdigstillelse), som også muliggjør skatteunndragelser.

Etter Finanstilsynets vurdering er eiendomsmeglingsvirksomheter i utgangspunktet medium høy anvendelig for hvitvasking og terrorfinansiering. Det knytter seg særlig risiko til bruk av klientkonto. Virksomheter som driver næringsmegling, anses å ha høyere risiko enn virksomheter som driver ordinær boligmegling. Et unntak fra dette er boliger som har vært gjenstand for oppussing/renovering samt nyboligsegmentet, hvor risikoen anses å være høyere. Virksomheter som har rene oppgjørsoppdrag, anses også å ha høyere risiko.

10 Låneformidling

Låneformidlere er uavhengige mellompersoner som formidler lån mellom långiver og låntaker. Låneformidlingsvirksomhet kan være organisert på ulike måter. Det kan være ulikheter i måten man henvender seg til potensielle kunder, hvilke kunder formidlingen retter seg mot og hvilke type lån som formidles. Lånebasert folkefinansiering omfattes av låneformidlerbegrepet og er derfor rapporteringspliktig etter hvitvaskingsloven. En annen betegnelse på lånebasert folkefinansiering er peer-to-peer lending (P2P). Et felles trekk ved lånebasert folkefinansiering er at det er tre aktører: långivere, låntakere og foretaket som administrerer finansieringen gjennom en elektronisk plattform.

Det er ulike metoder låneformidlingstjenester kan utnyttes til hvitvasking og terror-finansiering. Det kan eksempelvis tenkes at långiver og låntaker kjenner hverandre og lånet

settes opp som en hvitvaskingsoperasjon, hvor låneformidlingstjenesten gir et skinn av legitimitet. Det kan også være tilfeller hvor långiver og låntaker har samme reelle rettighetshavere, slik at lånet ytes og mottas fra reelt sett samme personer. Långiver vil imidlertid også få hvitvasket midler på en effektiv måte, selv om låntaker ikke er kjent med at midlene stammer fra straffbare handlinger.

Dersom låntaker initierer eller er villig til å inngå i et lån med dårlige vilkår, eller låner ut med tap, kan dette være et modus for å hvitvaske midler.

Låneformidling kan også utnyttes til terrorfinansiering ved at lån ytes til personer, grupperinger eller foretak som inngår i planlegging av terrorhandlinger.

På generelt grunnlag knytter det seg risiko til internettbaserte tjenester, hvor det ikke er begrensninger i hvor kundene er etablert. Låneformidlere med slike tjenester må ha tilstrekkelige kontrollmekanismer for å redusere denne risikoen.

Låneformidling gjennom lånebaserte folkefinansieringsplattformer er aktualisert i den senere tid. Det antas at risikoen for hvitvasking og terrorfinansiering gjennom låneformidlings-virksomhet er medium høy. Låneformidlere som har oppgjørsfunksjon og derfor konsesjon som betalingsforetak, antas å være særlig utsatt.

11 Virtuell valuta

Rapporteringspliktige etter hvitvaskingsloven og -forskriften er tilbydere av oppbevaringstjenester og vekslingstjenester av virtuell valuta.

Plattformer og tjenester som tilbyr kunder å handle eller veksle en type virtuell valuta for en offisiell valuta, herunder plattformer som tilrettelegger for handel og vekslinger ved å koble kjøpere og selgere, er omfattet som rapporteringspliktige. Alle vekslinger mellom virtuell valuta og offisielle valutaer fra alle land, er omfattet. Dette gjelder uavhengig av betalings-form, altså om det kjøpes/selges virtuell valuta med kredittkort, kontanter, e-penger etc. Vekslinger mellom forskjellige typer virtuell valuta, eksempelvis fra Bitcoin til Ethereum, er ikke omfattet.

Videre omfattes oppbevaring av private kryptografiske nøkler på vegne av kundene, som brukes til å overføre, lagre eller handle virtuell valuta. Oppbevaringsløsninger som ikke lagrer private kryptografiske nøkler (ofte omtalt som "non-custodial wallets"), omfattes ikke av regelverket.

I utgangspunktet kan vinning fra alle kriminelle handlinger hvitvaskes gjennom veksling til virtuell valuta, samt tilbakeveksling til offisiell valuta. Det er likevel enkelte moduser som trekkes frem som alminnelige per dagens dato.

I nasjonal risikovurdering trekkes investeringsbedragerier frem. Bedrageriene har gjerne utspring i nettsider som kan oppfattes som reelle og seriøse, herunder på nettsider om investeringer i Bitcoin. Bedrageriene kan hvitvaskes ved å veksles til offisiell valuta.

Finanstilsynet er også informert om at alminnelige bedragerier via bankoverføringer veksles til virtuell valuta, eksempelvis gjennom telefonsvindel hvor svindlerne får tilgang til bankinformasjon, eller hvor det utføres hacking.

Virtuell valuta er også utsatt for bruk til hvitvasking og terrorfinansiering gjennom utenlandsbetalinger. Virtuell valuta kan enkelt overføres, oppbevares og veksles i offisiell valuta i utlandet. Den potensielt manglende sporbarheten og verdisvingninger i valutaen, gjør at penger enkelt kan overføres til utlandet via bruk av virtuell valuta. Finanstilsynet antar at dette kan være en svært attraktiv metode for å skjule utbyttet fra kriminelle handlinger, hvitvaske penger, samt finansiere terrorvirksomhet.

I forsøk på å hvitvaske penger ved bruk av virtuell valuta benyttes tidvis såkalte muldyr. Dette er personer som ikke har en åpenbar naturlig sammenheng til den kriminelle virksomheten, men som får betalt for å utføre hvitvaskingsprosessen. Bruken av muldyr kan skje på en rekke forskjellige måter, eksempelvis ved at muldyret mottar overføring av virtuell valuta, som veksles til offisiell valuta og overleveres til oppdragsgiver.

Virtuell valuta er et egnet virkemiddel for å finansiere terror. Forskjellige typer virtuell valuta er akseptert som betalingsmiddel på det mørke nettet, hvor det er mulig å kjøpe varer og tjenester som kan benyttes i terrorhandlinger både nasjonalt og internasjonalt, eksempelvis våpen. Terrorfinansiering foregår imidlertid også ved kjøp av mer alminnelige varer og tjenester, eksempelvis utstyr fra sportsbutikker, transportmidler mv.

Virtuell valuta er et attraktivt virkemiddel for kriminelle. Dette er både fordi virtuell valuta har vært uregulert og fordi det for enkelte valutaer og plattformer er mulig å operere anonymt. Kombinasjonen av potensiell anonymitet og muligheten til å sende penger over landegrensene gjør at det er risiko for bruk av virtuell valuta til både hvitvasking og terrorfinansiering.

Forskjellige virtuelle valutaer har forskjellige funksjonaliteter når det gjelder anonymitet og sporbarhet av transaksjoner på blokkjeden. Monero er et eksempel på en valuta som er anonym og vanskelig å spore. Monero, men også andre typer virtuell valuta, som Ethereum, blir akseptert som betalingsmiddel på det mørke nettet. Disse utgjør derfor en høy risiko for å bli brukt i terrorfinansiering, men også til å kjøpe varer og tjenester som ikke er terrorrelatert for ulovlig ervervede midler.

Andre tjenester som kan utgjøre en høy risiko for hvitvasking og terrorfinansiering, er såkalte miksere eller tromler. Formålet med disse er å mikse identifiserbare kryptomidler med andre, slik at sporbarheten på blokkjeden vanskeliggjøres eller umuliggjøres. Dette kan bidra til å slette spor av kryptovalutaens opprinnelse, hva den har vært benyttet til mv. Mikserne bidrar derfor også til å vanskeliggjøre etterforskning av kriminell aktivitet.

Et annet modus er å kombinere ulike tjenester. NTAES oppgir som modus at den kriminelle veksler kryptovaluta hos utenlandske vekslere, for så å overføre til en utenlandsk konto eller et forhåndsbetalt kort i et fiktivt navn, som kan benyttes i Norge og verden for øvrig. Midlene overføres til egen bankkonto, utenlandske bankkontoer eller forhåndsbetalte kort som kan benyttes i Norge.

Virtuell valuta anses å ha en høy iboende risiko for å bli benyttet til hvitvasking og terrorfinansiering. Det er mange trusler og sårbarheter, som gjør tilbydere av vekslings- og

oppbevaringstjenester anvendelige for hvitvasking og terrorfinansiering. Regelverket er nytt og foreløpig ikke implementert i hele EU, og markedene for virtuell valuta endres raskt.

FINANSTILSYNET
Postboks 1187 Sentrum
0107 Oslo
POST@FINANSTILSYNET.NO
WWW.FINANSTILSYNET.NO