Foto: iStock - BlackJack3D

ØKOKRIM

PST
POLITIETS SIKKERHETSTJENESTE

Nasjonal risikovurdering

Hvitvasking og terrorfinansiering 2022

Innhold

Innledning ... 3
Hovedfunn hvitvasking ... 4
Hovedfunn terrrorfinansiering ... 5

Del 1 – Risikovurdering hvitvasking
1. Metode og datagrunnlag ... 7
2. Trusselbildet for hvitvasking ... 12
   2.1. Norsk økonomi ... 12
   2.2. Næringsstruktur og kriminalitet innen viktige sektorer ... 13
   2.3. Utbyttegenererende kriminalitet og hvitvaskingsmodus ... 16
   2.4. Aktører som bidrar i hvitvaskingsoperasjoner ... 33
3. Overordnede sårbarheter for hvitvasking ... 36
4. Risiko for hvitvasking i rapporteringspliktige sektorer ... 41
   4.1. Banker ... 42
   4.2. Agenter av utenlandske betalingsforetak ... 45
   4.3. Betalingsforetak ... 47
   4.4. E-pengeforetak ... 49
   4.5. Kredittforetak og finansieringsforetak ... 50
   4.6. Tilbydere av vekslings- og oppbevaringstjenester for virtuell valuta ... 51
   4.7. Verdipapirforetak, forvaltningsselskap og forvaltere av alternative investeringsfond ... 52
   4.8. Forsikringsforetak og forsikringsformidlere ... 54
   4.9. Eiendomsmeglere ... 56
   4.10. Autoriserte regnskapsførere ... 58
   4.11. Statsautoriserte revisorer ... 60
   4.12. Advokater ... 62
   4.13. Innenlandske selskaper som tilbyr spilltjenester ... 64

Del 2 – Risikovurdering terrorfinansiering
1. Oppbygging og metode ... 66
2. Bakgrunn – Terrorfinansiering ... 69
3. Trusselnivå ... 70
4. Sårbarheter – Risiko ... 76
5. Kilder – NRA 2022 Terrorfinansiering ... 82

Del 3 – Norges antihvitvaskings- og terrorfinansieringsregime
1. Internasjonalt rammeverk ... 84
2. Nasjonal lovgivning ... 86
3. Regimets aktører og koordinering ... 89

Innledning

For å implementere anbefaling 1 fra Financial Action Task Force (FATF) og artikkel 7 i EUs fjerde hvitvaskingsdirektiv skal Norge utarbeide risikovurderinger av hvitvasking og terrorfinansiering. En oppdatert samlet nasjonal risikovurdering av hvitvasking og terrorfinansiering er et godt utgangspunkt for forståelse og erkjennelse av risikoene vi møter i Norge, og for å møte disse risikoene på en effektiv og virkningsfull måte. Dette arbeidet er også viktig for å sørge for at Norge etterlever sine internasjonale forpliktelser på området. Nasjonalt er dette arbeidet forankret ved regjeringsbeslutning, og det er bestemt at risikovurderingen skal oppdateres hvert andre år.

Norge har de beste forutsetningene til å forebygge, avdekke og sanksjonere forbrytelser forbundet med hvitvasking og terrorfinansiering. Gjennom sterk tilslutning til internasjonalt regelverk, en stabil og gjennomsiktig økonomi, uavhengige institusjoner, lav korrupsjon og en høy grad av finansiell inkludering er alle elementer for et effektivt system til stede. Likevel viser så vel evalueringer, trusselvurderinger og andre kilder at det er reelle og alvorlige trusler i Norge, og at det er rom for ytterligere forbedringer av Norges systemer.

NRA 2022 skal også være grunnlaget for risikodempende tiltak på alle nivåer både i privat og offentlig sektor. Den bør brukes i den risikobaserte tilnærmingen til bekjempelse og forebygging av hvitvasking, for eksempel ved utvikling av regelverk og veiledning, prioritering av ressursbruk, utvelgelse av tilsynssubjekter eller åpning av straffesaker, samt til videre analyser. NRA kan benyttes som basis for å videreutvikle mer detaljerte risikoanalyser for egen sektor.

Risikovurderingen må ses i sammenheng med regjeringens *Strategi for bekjempelse av hvitvasking, finansiering av terror og finansiering av spredning av masseødeleggelsesvåpen*. Formålet med strategidokumentet er å sikre koordineringen av den samlede nasjonale innsatsen mot hvitvasking, finansiering av terror og finansiering av spredning av masseødeleggelsesvåpen ved å gjennomføre nye tiltak. Målet er at tiltakene i strategien skal gi de berørte etatene de nødvendige føringene og metodene for dette arbeidet.

NRA 2022 er utarbeidet på oppdrag fra Justis- og beredskapsdepartementet. Økokrim har utarbeidet risikovurderingen for hvitvasking, mens Politiets Sikkerhetstjeneste (PST) har utarbeidet risikovurderingen for terrorfinansiering. Ved utarbeidelsen er det innhentet informasjon og vurderinger fra en rekke aktører i politi- og påtalemyndigheten, kontrolletater, tilsyn og privat sektor.

Denne nasjonale risikovurderingen for bekjempelse av hvitvasking og terrorfinansiering (NRA 2022) er Norges femte samlede risikovurdering av trusler, sårbarheter og risikoer for hvitvasking og terrorfinansiering.

Hovedfunn hvitvasking

Trussel
Trusselbildet preges særlig av den økte digitaliseringen vi ser både i økonomien og i samfunnet generelt. Kriminalitet utført ved hjelp av digitale verktøy ventes å øke og generere større utbytte fremover. Samtidig har digitalisering og teknologisk utvikling økt handlingsrommet til kriminelle aktører både hva gjelder primærkriminalitet og hvitvasking. Nye digitale tjenester fører også til økt bruk av grensekryssende tjenester.

Digitalisering i kombinasjon med sosial manipulering ser ut til å være en spesielt stor trussel i dagens kriminalitetsbilde.

Det registreres en økning i bruk av pengemuldyr i hvitvaskingsprosesser. Det er spesielt alvorlig at unge og andre sårbare personer utnyttes.

Sårbarheter
Bruken av tredjepartsaktører i betalingstransaksjoner øker. En overordnet sårbarhet er utfordringer med deling av informasjon på tvers av rapporteringspliktige sektorer. Det fremstår også tidvis å være uklart for de rapporteringspliktige hvem som faktisk har ansvar for å detektere og rapportere mistenkelige forhold - banken som står for infrastrukturen hvor transaksjonen foregår eller betalingsforetaket som har kundeforholdet.

En annen overordnet sårbarhet er at mange rapporteringspliktige kjøper anti-hvitvaskingsprodukter- og tjenester som hyllevare. Disse er sjeldent tilpasset den aktuelle virksomheten og således lite optimale.

Mye av den alvorlige økonomiske kriminaliteten kamufleres ved at lovbryterne gjennomfører transaksjoner og organiserer eierskap på en ikke-transparent måte. Banker har generelt utfordringer med å kartlegge reelle rettighetshavere, noe som ytterligere kompliseres hvis kundene er utenlandske juridiske personer, det benyttes skallselskap, skatteparadis og klientkontoer i transaksjonskjeden.

Risiko
Banker, betalingsforetak og agenter for utenlandske betalingsforetak vurderes å ha høy risiko for å bli benyttet til hvitvasking av utbytte fra kriminalitet.

Betalingsforetak, advokater og regnskapsførere vurderes å ha høyere risiko enn i forrige NRA. Dette skyldes primært bedre informasjonsgrunnlag.

Bruk av kryptovalutavekslere og miksere trekkes frem som en hvitvaskingsmetode som vurderes å høy risiko og særlig bli benyttet knyttet til digital kriminalitet. Risikoen knyttet til norske tilbydere av vekslings- og oppbevaringstjenester for virtuell valuta vurderes imidlertid ikke å være så høy fordi kriminelle i liten grad benytter seg av de norske tilbyderne. Kriminelle med tilknytning til Norge benytter seg hovedsakelig av utenlandske vekslingstjenester.

Hovedfunn terrorfinansiering

Trusselnivået i Norge er MODERAT. Trusselnivået omfatter samtlige ekstremistfelter.

Radikalisering, både til islamsk ekstremisme og høyreekstremisme skjer særlig på ulike digitale nettverk. Internasjonalt ser man også at mye av finansieringen til disse miljøene skjer også her.

Kontakten mellom norske ekstremister og terrorgrupper i utlandet er en vedvarende bekymring, og vil kunne fortsette å bidra til terrorrelatert aktivitet.

Løslatelse av terrordømte i Norge og andre europeiske land vil fortsette å påvirke terrortrusselen negativt.

I den krevende sikkerhetspolitiske situasjonen Norge og Europa står i vil en nedprioritering i kontraterrorarbeidet fra vestlige sikkerhets- og etterretningstjenester bidra til at ekstremister får et større handlingsrom både på fysiske og digitale arenaer.

Flere av sårbarhetene og risikoene for hvitvasking som blir presentert i NRA 2022 gjelder også for terrorfinansiering. Dette gjelder i stor grad fordekte transaksjoner, der enten avsender og/eller mottaker er fordekt eller anonymisert og sporbarheten i transaksjonen minimal. Dette gjelder spesielt transaksjoner som foretas via følgende:

- Uregistrerte betalingsforetak og betalingsforetak som ikke etterlever hvitvaskingslovens krav eller rapporterer til Valutaregisteret.
- Virtuell valuta, hvor aktørene etterlater seg elektroniske spor som det kreves oppdatert kunnskap og analyseverktøy for å avdekke.
- Frivillig sektor, hvor enkelte aktører i liten grad registrerer seg og dermed unngår kontroll og rapportering.
- Pengeinnsamling via sosiale medier til krypterte aktører.

Del 1

Risikovurdering hvitvasking

1. Metode og datagrunnlag

1.1. Metodikk

Internasjonale regelverk som Norge er tilsluttet stiller visse krav til prosessen og analysen for å vurdere risiko for hvitvasking og terrorfinansiering. NRA 2022 er utarbeidet i tråd med Norges internasjonale forpliktelser på dette området og i henhold til de kravene og anbefalingene som stilles gjennom EUs fjerde og femte hvitvaskingsdirektiv, samt gjennom FATF-rekommandasjon nr. 1. Kravene og anbefalingene er operasjonalisert i FATF Guidance, National Money Laundering and Terrorist Financing Risk Assessment (februar 2013).

Økokrim har også utarbeidet risikovurderingen av hvitvasking i henhold til rammer og prinsipper beskrevet i Politiets etterretningsdoktrine.

Det prioriterte etterretningsbehovet er: «Hva er risikoen relatert til hvitvasking i Norge og til at midler som er utbytte fra kriminalitet i Norge hvitvaskes i utlandet?»

1.2. Definisjoner

Hvitvasking defineres i straffeloven § 337. For hvitvasking straffes den som

a) yter bistand til å sikre utbyttet av en straffbar handling for en annen ved for eksempel å innkreve, oppbevare, skjule, transportere, sende, overføre, konvertere, avhende, pantsette eller investere det, eller
b) gjennom konvertering eller overføring av formuesgoder eller på annen måte skjuler eller tilslører hvor utbyttet av en straffbar handling han selv har begått, befinner seg, stammer fra, hvem som har rådigheten over det, dets bevegelser, eller rettigheter som er knyttet til det.

Likestilt med utbyttet er gjenstand, fordring eller tjeneste som trer i stedet for det.

Trusler defineres som en person, et objekt, grupper av personer eller aktiviteter som potensielt kan skade staten, samfunnet og økonomien. I snever forstand kan man si at trusler utnytter sårbarheter ved hjelp av bestemte moduser. Dette inkluderer kriminelle og deres fasilitatorer som utfører hvitvaskingsaktiviteter. Den utvidede definisjonen av trusler ser på omfanget av utbyttet som genereres fra kriminelle handlinger i ett land (intern trussel) og innførsel fra utlandet (ekstern trussel), samt moduser og trender som kjennetegner trusselaktørene.

Sårbarheter er innretninger og mangler ved eksempelvis vårt kontrollsystem og vår kriminalitetsbekjempelse, som kan bli utnyttet av trusselaktører, og derigjennom bidra til kriminalitet. I risikovurderingen av sektorer forstås sårbarheter som karakteristika ved sektorer, finansielle produkter eller bestemte typer tjenester som er attraktive i en hvitvaskingssammenheng. Svakheter og hull i det overordnede anti-hvitvaskings-systemet på nasjonalt nivå kan også

utgjøre en sårbarhet for sektorer. Dette kan omfatte alt fra innebygde sårbarheter i infrastrukturen i bekjempelsen av hvitvasking, til mangelfull MT-rapportering og dårlig ID-kontroll hos de rapporteringspliktige. Videre kan det være svakheter ved lovverket og fraværende reguleringer som forhindrer forebygging av hvitvasking.

Konsekvenser refererer til skaden hvitvasking kan påføre, og inkluderer effekten av primærkriminaliteten på finanssystemer og -institusjoner, økonomien og samfunnet. Størrelsen på verdiene som hvitvaskes er en vesentlig del av skaden.

Risikoen for at en sektor er særlig utsatt for hvitvasking er avhengig av trusselen mot sektoren, sektorens sårbarhet for trusselen og konsekvensene av hvitvaskingen i sektoren.

1.3. Tverretatlighet

Tverretatlighet i oppdraget med å utarbeide en nasjonal risikovurdering er sikret gjennom å innhente informasjon fra aktører i regimet både i offentlig og privat sektor. De som har bidratt med informasjon i 2022 er: Finanstilsynet, Tilsynsrådet for advokatvirksomhet, Lotteritilsynet, Skatteetaten, Tolletaten, EFE, Norsk tipping, Økonomiforbundet, Regnskap Norge, Eiendom Norge, Eiendomsmegler 1, Finansieringsselskapenes forening, OPS AT. Vi retter en stor takk til disse for deres bidrag.

1.4. Datagrunnlag

Trusselvurderingen av utbyttegenererende kriminalitet og hvitvaskingsmodus er primært utarbeidet på bakgrunn av politiets samlede etterretningsproduksjon på området.

Til resten av risikovurderingen består datagrunnlaget av utarbeidede rapporter og analyser fra både politiet, tilsyns- og kontrollorganer samt private aktører, samt internasjonale trussel og risikovurdering som EUs supranasjonale risikovurdering.

Sårbarheter knyttet til rapporteringspliktige er i stor grad basert på informasjon fra tilsynsmyndighetene. I tillegg gir informasjonen som ble hentet inn aktørenes vurderinger av trusler, sårbarheter de ser fra sitt ståsted og eksempler de måtte ha på hvitvasking.

1.5. Vurdering av trussel

Nivået på trusselen fra ulike typer utbyttegenererende kriminalitet vurderes basert på en standardisert matrise. Trusselskalaen gir uttrykk for hvilke typer kriminalitet som vil generere mest utbytte og derav også behov for hvitvasking av midler.

Matrisevurdering av trussel

Nasjonal standard	Beskrivelse	NATO standard
Meget sannsynlig	Det er meget god grunn til å forvente …	Highly likely (〉90 %)
Sannsynlig	Det er grunn til å forvente …	Likely (60–90 %)
Mulig	Det er like sannsynlig som usannsynlig …	Even chance (40–60 %)
Lite sannsynlig	Det er liten grunn til å forvente …	Unlikely (10–40 %)
Svært lite sannsynlig	Det er svært liten grunn til å forvente …	Highly unlikely 〈10 %

Vurderingen av fremtidig utvikling av truslene vil alltid inneholde en grad av usikkerhet. For å håndtere dette på en standardisert og strukturert måte er det benyttet sannsynlighetsord (se tabell). Sannsynlighetsord angis i kursiv i teksten.

Nasjonal standard for sannsynlighetsord (2018)

Nivå	Trusselbegrep	Kort forklaring
5	Svært høy trussel	Det er svært høy trussel. Det er flere internasjonale organiserte kriminelle grupperinger som begår svært profittgenerende kriminalitet i Norge. Utbyttet medvirker til å bygge nettverkenes kapabiliteter.
4	Høy trussel	Flere nettverk og aktører har intensjon og kapabilitet til å gjentagende gjennomføre svært profittgenerende kriminalitet i Norge. Det genereres et stort utbytte som hvitvaskes. Dette kan gjenspeiles i antall anmeldelser, etterretningsinformasjon og MT-meldinger.
3	Moderat trussel	En eller flere aktører og/eller nettverk har intensjon og kapasitet til å gjennomføre profittgenerende kriminalitet i Norge. Utbyttet som genereres og hvitvaskes er moderat. Dette kan gjenspeiles i antall anmeldelser, etterretningsinformasjon og MT-meldinger.
2	Lav trussel	Enkelte aktører har vilje og evne til å gjennomføre utbyttegenererende kriminalitet, men utbyttet som genereres er lavt.
1	Ingen kjent trussel	Trusler som politiet ikke har informasjon til å vurdere. Det er ikke registrert hverken anmeldelser eller etterretningsinformasjon.

1.6. Risikomodell for å vurdere hvitvasking

Risikovurderingen av hvitvasking gjøres ved hjelp av en modell utviklet av Økokrim.[1] Modellen tar utgangspunkt i veilederen til FATF og følger deres retningslinjer.[2] Modellen benytter indikatorer for trussel, sårbarhet og konsekvenser for å vurdere den totale risikoen i sektoren.

Indikatorer for trussel:
- Omfang/antall trusselaktører
- Aktørens kapasitet når det gjelder å benytte sektoren
- Utbytte relatert til trusselaktørene
- Utsatthet for internasjonale penge-strømmer

Indikatorer for sårbarhet ved vurdering av hvitvaskingsrisiko i sektorer:
- Iboende egenskaper ved sektoren og eksponering for risiko
- Juridisk rammeverk/reguleringer

Forståelse av ansvaret for hvitvaskingsar-beid og fokus på compliance og rapporte-ring i sektoren, inkludert systemer
- Kontroll med sektoren

Indikatorer for vurdering av konsekvenser:
- Direkte konsekvenser
- Langsiktige konsekvenser

Risikomatrise			
Gul 4	Oransje 8	Rød 12	Rød 16
Grønn 3	Gul 6	Oransje 9	Rød 12
Grønn 2	Grønn 3	Gul 6	Oransje 8
Grønn 1	Grønn 2	Grønn 3	Gul 4

Farge	Risikonivå
Rød	Høy
Oransje	Betydelig
Gul	Moderat
Grønn	Lav

Indikatorene vurderes fra 1 til 4 (lav, moderat, betydelig og høy). Nivået på trussel, sårbarhet og konsekvenser fastsettes ved å beregne et gjennomsnitt av indikatorene innenfor hver kategori.

For å beregne risiko beregnes først «justert trusselnivå», hvor den opprinnelige trusselen justeres for sårbarhetsnivået, som er en indikator på hvor bra anti-hvitvaskingssystemet er til å forhindre at utbyttet blir hvitvasket. Justeringen gjøres ved å justere ned trusselnivået etter følgende nøkkel, basert på score relatert til sårbarhetsnivå: høy (0 %), betydelig (25 %), moderat (50 %) og lav (75 %).

Risikonivået finnes ved å multiplisere det justerte trusselnivået med konsekvensnivået.

1 Økokrim, «Modell risikovurdering hvitvasking i sektorer», 2020.
2 Financial Action Task Force (FATF), «National Money Laundering and Terrorist Financing Risk Assessment», 2013.

1.7. Forkortelser benyttet i rapporten

BNP – Bruttonasjonalprodukt
EBA – European Banking Authority
EFE – Enheten for Finansiell Etterretning
FATF – Financial Action Task Force
FinTech (finansteknologi) – Et paraplybegrep på innovative teknologier som skal forbedre eller erstatte dagens produkt- og tjenestetilbud innen bank- og finansnæringen.
FIU – Financial Intelligence Unit
IMF – International Monetary Fund
NFT – Non-fungible token
NRA – Nasjonal Risikovurdering: Hvitvasking og terrorfinansiering
NTAES – Nasjonalt tverretatlig analyse- og etterretningssenter
SNRA – Supra-National Risk Assessment

2. Trusselbildet for hvitvasking

2.1. Norsk økonomi

Norge har en åpen økonomi som baserer seg på handel og deltagelse i den internasjonale økonomien.[3] Norsk økonomi er preget av store internasjonale bedrifter, hvor flere ekspanderer virksomheten til utviklingsland og land med strukturelle korrupsjonsproblemer. Dette øker trusselen for alvorlig økonomisk kriminalitet som korrupsjon og skatte- og avgiftsunndragelser.

De økonomiske konsekvensene av pandemien var mindre omfattende i 2021 enn i 2020. Aktiviteten har steget ytterligere etter at smitteverntiltakene ble fjernet vinter 2022 og arbeidsledigheten er på det laveste nivået siden før finanskrisen i 2008.[4] Mange bedrifter opplever et stramt arbeidsmarked hvor det er vanskelig å få tak i arbeidskraft. Økonomien preges av en sterk prisvekst på 7,5 prosent fra oktober 2021 til oktober 2022.[5] Dette er den sterkeste prisveksten som er målt siden juni 1988.

Den høye prisveksten påvirker husholdningenes kjøpekraft negativt og Norges bank har kommet med det som anses som drastiske rentehevinger. Det forventes en videre rask økning i renten for å få ned inflasjonen. Siden finanskrisen har verdens største sentralbanker gradvis satt ned rentene, og da pandemien traff ble flere sentralbankrenter satt ned til null eller negativ. Dette ble gjort samtidig med økt pengetrykking og omfattende finanspolitiske stimulanser, noe som har bidratt til å presse prisene opp. Utviklingen i økonomien tilsier en innstramming i finanspolitikken de neste årene, men strømstøtte og tiltak i forbindelse med krigen i Ukraina bidrar til en fortsatt høy bruk av oljepenger i 2022.[6] Støtteordninger bidrar til å opprettholde husholdningenes kjøpekraft i en periode hvor Norges Bank er avhengig av å tøyle inflasjonen. På sikt kan dette føre til kraftige innstramminger i finanspolitikken og ytterligere rentehevinger utover dagens forventede nivå.

Andelen husholdninger med høy gjeldsbelastning økte markant i perioden 2004 til 2020, og husholdningenes gjeldsbelastning ligger nå på et historisk høyt nivå.[7] Kun en liten andel av husholdningers gjeld har fastrente. Et høyere rentenivå ventes derfor å slå raskt ut i større renteutgifter for husholdningene med et fall i realinntekt.

3 Finansdepartementet, «Perspektivmeldingen 2021», 2021.
4 SSB, «Høy inflasjon og økte renter vil bremse veksten i norsk økonomi», 2022.
5 SSB, «Konsumprisindeksen», 10.11.2022.
6 Norges Bank, «Pengepolitisk rapport med vurdering av finansiell stabilitet nr. 2», 2022.
7 Finanstilsynet, «Finansielt Utsyn – juni 2022», 2022.

Dette vil ha en negativ effekt på realøkonomien gjennom et lavere konsum i husholdningene.

Det lave rentenivået har også medført en økning i boligprisene i Norge, en økning som også er betydelig mer enn disponibel inntekt per innbygger.[8] Renteøkningene er ventet å slå ut i boligmarkedet med en avtakende og moderat prisvekst de neste årene.

Mye tyder på at man kan stå overfor et scenario hvor økonomien vil gå inn i en stagflasjons- eller resesjonsperiode, hvor det enten blir fortsatt høy inflasjon samtidig som veksten er svak eller resesjon hvor det vil være negativ økonomisk vekst. Utviklingen i den internasjonale økonomien vil utvilsomt påvirke norsk økonomi og finansielle stabilitet. Økonomien vil videre preges av krigen i Ukraina, globale forsyningskjedeproblemer, svak etterspørsel og nedstengte havner i Kina, i tillegg til en global levekostnadskrise.[9]

Den russiske invasjonen av Ukraina har også medført flere sanksjoner og restriktive tiltak mot russiske og hviterussiske statsborgere, foretak og interesser. Dette får konsekvenser for norsk økonomi og næringsinteresser, i tillegg til å øke risikoen for at aktører fra disse landene forsøker å overføre verdier via Norge.

Den norske økonomien er bedre rustet til å takle nedgangstider sammenlignet med andre land. Selv med den forventede nedgangen i økonomisk vekst vil Norge fortsatt være et land med høy levestandard og relativt høy grad av økonomisk og politisk stabilitet. Dette vil gjøre at Norge fortsatt vil være et attraktivt land å plassere verdier i for utenlandske aktører, inkludert midler av ulovlig opprinnelse. Det forholdsvis høye lønnsnivået i Norge gjør det også attraktivt for arbeidsinnvandring samt bedrageri av privatpersoner.

2.2. Næringsstruktur og kriminalitet innen viktige sektorer

2.2.1. Olje- og gassektoren

Olje- og gassvirksomheten er den største næringen i Norge både målt i verdiskaping, inntekter til statskassen, investeringer og eksportverdi.[10] Russlands invasjon av Ukraina har økt olje- og energiprisene, ført til reduserte gassleveranser til Europa og skapt et press i markedet etter fossilt brennstoff. Olje- og gassindustrien kjennetegnes av store aktører og streng regulering. Oppdagelsesrisikoen for økonomisk kriminalitet vil være større i en gjennomregulert bransje. Det er likevel sider ved bransjen som kan utnyttes for å oppnå fordeler og økonomisk vinning på ulovlig vis.

Petroleumstilsynet har etter en opptrappet innsats mot arbeidslivskriminalitet begynt å føre tilsyn med selskapenes bruk av innleid arbeidskraft.[11] Dette avdekket både ulovlig innleie, mangel på rutiner eller system, og generelt manglende bevissthet rundt reglene om innleie. Olje- og gassektoren er også kapitalintensiv og preget av pengeflyt på tvers av landegrenser

8 Finanstilsynet, «Finansielt Utsyn – juni 2022», 2022.
9 SSB, «Økonomiske analyser 2/2022: Konjunkturutvikling i norsk og internasjonal økonomi», 2022.
10 NHO, «Tall og fakta om internasjonal handel og samarbeid», 2022.
11 Petroleumstilsynet, «Behov for mer kunnskap og oppmerksomhet om innleie», 2022.

og høye verdier på kontraktene som inngås. Equinor sine avtaler om lisenstildelinger i Angola har blant annet fått sterk kritikk.[12] I forbindelse med det amerikanske finanstilsynets forslag om regelendring på feltet ble Equinors avtale i Angola trukket frem som eksempel på hvordan avtaler, pengeflyt, manipulasjon og misbruk i oljesektoren skjer i forbindelse med enkeltkontrakter.[13] Det ble fremhevet hvordan slike avtaler kan være med på å skjule mistenkelige transaksjoner og tillate korrupsjon.

Det høye nivået på teknologien i norsk olje- og gassindustri gjør det til et aktuelt investeringsområde for utenlandske investorer og statlige aktører. Lekkasjen Pandora Papers avslørte blant annet hvordan et norsk advokatfirma hadde fungert som strømenn for en russisk oligark.[14] Oligarken, med forbindelser til Kreml, hadde oppnådd en betydelig eierandel i et norsk oljeselskap hvor eierskapet var skjult gjennom en kompleks eierstruktur. Dette viser hvordan opprettelsen av slike strukturer ofte er avhengig av tjenester fra andre sektorer i norsk næringsliv.

2.2.2. Fornybar energi og det grønne skiftet

Den fornybare energisektoren er et raskt voksende marked og overgangen til det grønne skiftet vil bidra til betydelig verdiskaping, samtidig som omstillingen vil kreve store investeringer.[15] International Energy Agency anslår at det vil kreves mer enn en dobling av årlige investeringer i klimavennlig energiproduksjon- og effektivisering for å være på en netto-null-utslippsbane globalt innen 2050.[16] For å fremskynde det grønne skiftet vil staten bidra ved å tilby offentlige støtte- og insentivordninger. Slike ordninger kan utnyttes av kriminelle aktører.[17] Kombinasjonen av omstilling i høyt tempo, kapitalintensive investeringer og anbudskonkurranser kan skape et mulighetsrom og øke risikoen for korrupsjon.[18]

Energikrisen, som følge av Russlands invasjon av Ukraina, har lagt et ytterligere press på utbygging av fornybare energikilder for å sikre energisikkerhet. Utbyggingen av fornybar energi vil igjen legge et press på allerede knappe arealressurser.[19] For å utnytte den fornybare energien er det avhengig av utbygging av relativt store arealer for plassering av for eksempel vindmølleparker, havvindparker og solcellepanel. Dette innebærer ofte områder med store naturverdier og det økende presset på utbygging av fornybar energi kan øke risikoen for miljøkriminalitet knyttet til ulovlige naturinngrep og arealendringer.

2.2.3. Fiskeri- og havbruksnæringen

Eksport av sjømat har opplevd en enorm vekst de seneste årene og i 2021 ble det satt eksportrekord både i volum og verdi, med henholdsvis 3,1 millioner tonn og 120,8 milliarder

12 E24, «Equinors tvilsomme pengebruk», 2020.
13 Natural Resource Governance Group, «Comment on SEC proposed rule 13q-1 to implement Section 1504 of the Dodd-Frank Act, File Number S7-24-19», 2020.
14 E24, «Norske advokater var strømenn for mektige russere», 2021.
15 Regjeringen, «Det grønne skiftet», 2021.
16 International Energy Agency, «Net zero by 2050», 2021.
17 Økokrim, «Trusselvurdering», 2022.
18 OECD, «Fighting corruption and promoting integrity in the renewable energy sector», 2021.
19 Tekna, «Fornybar energi har et arealproblem», 2022.

kroner.[20] Havbruksnæringen utgjør Norges nest største eksportnæring etter olje og gass, og er en viktig næring i vekst.[21] Fiskerinæringen er globalisert og flere sider ved næringen gjør den utsatt for et bredt spekter av økonomisk motivert kriminalitet.[22] Produksjon- og verdikjeden i fiskerinæringen er kompleks, grensekryssende og lite oversiktlig med både små aktører og globaliserte konsern som kontrollerer flere ledd.

Den økende eksportverdien på norsk sjømat kan gjøre næringen spesielt attraktiv for aktører med både vilje og evne til å utøve kriminalitet i forlengelse av næringsdriften.[23,24] Overfiske andre steder bidrar også til å presse opp priser og gjør norske fiskeressurser attraktive for utenlandske aktører.

Det internasjonale aspektet og de uoversiktlige verdikjedene på tvers av jurisdiksjoner gjør også næringen sårbar for andre typer kriminalitet, som for eksempel hvitvasking av utbytte fra ulovlig fiske. Det er også eksempler på at det begås arbeidslivskriminalitet i næringen, blant annet ved utnyttelse av sårbare arbeidstagere fra utlandet.[25] Kriminalitet i fiskerinæringen kan være svært konkurransevridende.

2.2.4. Eiendomsutvikling, bygg og anlegg

Eiendomsutvikling og bygg- og anleggsbransjen er preget av store prosjekter og hard konkurranse, der pris ofte er utslagsgivende for hvem som vinner oppdrag. Sektoren er også utsatt for korrupsjonsrisiko i forbindelse med offentlige anbudsprosesser og manipulasjon av eiendomspriser. Priskonkurranse om å vinne kontrakter og anbud gjør også den tilknyttede bygge- og anleggsbransjen sårbar for arbeidslivskriminalitet.

Den nesten uavbrutte prisstigningen de siste ti årene og velfungerende økonomiske rammer rundt markedet gjør det til et attraktivt sted å plassere både norsk og utenlandsk kapital. I flere tilfeller vil det også generere inntekt via utleie eller prisavkastning på investeringen.[26] Det gjør at store beløp som har opphav fra kriminalitet kan investeres i fast eiendom, og deretter re-investeres og integreres i den legale økonomien.

Transparency Internationals rapport om hvitvaskingsrisiko i eiendomsmarkedet fant klare indikatorer på at det kan finnes aktører som har interesse av å skjule og hvitvaske ulovlig opptjente verdier blant eierne i attraktive eiendomsområder i Oslo. De viktigste indikatorene knyttet seg særlig til et betydelig innslag av eierskap i skatteparadis, et visst innslag av fysiske og juridiske personer som var registrert i land med moderat til høyt korrupsjonsnivå og forekomst av skjult eierskap og stråmenn som gjør identifisering av reelle rettighetshavere vanskelig.

20 Norges sjømatråd, «Sjømateksporten passerte 120 millioner kroner i fjor», 2022.
21 Regjeringen, «Norsk havbruksnæring», 2021.
22 Regjeringen, «Fiskerikriminalitet», 2018.
23 United Nations Office for Drugs and Crime, «Fisheries crime», uå.
24 NTAES, «Havbruk og fiskeri – verdikjeder, ansvar, lovbrudd», 2021.
25 Økokrim, «Trusselvurdering», 2022.
26 European parliament, «Briefing: Understanding money laundering through the real estate sector», 2019.

2.2.5. Servicesektoren og varehandel

Servicesektor og varehandel består av et stort spenn av næringer, og omfatter blant annet varehandel, hotell og restaurant til rengjøring og personlig tjenesteyting.[27] Foreløpige tall fra SSB viser at bygge- og anleggsvirksomhet, varehandel, transport og lagring, og overnattings- og serveringsvirksomhet sysselsatte 870 000 mennesker i 2021 og omsatte for 3 270 milliarder kroner.[28]

Mange av disse bransjene er arbeidsintensive, har lave formalkrav, og er bransjer hvor arbeidslivskriminalitet tidvis er svært utbredt. Det benyttes ofte utenlandske arbeidskraft som er midlertidig ansatt.

Økokrim mottar mest informasjon om a-krim innen bygg og anlegg, varetransport, bilpleiebransjen og bilverksted og servering. Samtidig er flere av bransjene som er utsatt for a-krim sesongbaserte.[29]

2.3. Utbyttegenererende kriminalitet og hvitvaskingsmodus

Antall registrerte anmeldelser i Norge i 2021 er 12 prosent lavere enn gjennomsnittet i perioden 2016 til 2020. Nedgangen er størst innen anmeldte narkotikalovbrudd og vinningskriminalitet.

Koronapandemien har trolig medvirket til de siste to års nedgang i anmeldte vinningslovbrudd, både på grunn av reduserte ankomster av mobile vinningskriminelle og på grunn av mindre bruk av offentlige rom og dermed færre tyverier fra person fra offentlig sted. Når det gjelder narkotikakriminalitet er nedgangen i stor grad et resultat av riksadvokatens og politiets nedprioritering av bruk og besittelse av narkotika, selv om også alminnelige og grove narkotikaovertredelser er noe redusert.

1 av 15 anmeldte lovbrudd i 2021 var et bedrageri, og til sammen ble det anmeldt nesten 18 900 bedrageri. Dette er en nedgang på 5,6 prosent sammenlignet med den foregående femårsperioden.[30] Flere banker rapporterer imidlertid om en økning i bedragerisaker på 66 prosent i 2021 sammenlignet med året før. Det kan derfor være grunn til å tro at antall bedrageri har økt de senere år, til tross for at antallet anmeldelser har gått ned.

Også finansiell kriminalitet og kriminalitet i og mot virksomheter anmeldes sjeldent og antas å ha store mørketall.

27 FAFO, «Arbeidstakere og organisasjonsgrader i servicesektoren», 2018.
28 SSB, «12817: Foreløpige tall for antall foretak, sysselsatte og omsetning, etter næring (SN2007), statistikkvariabel og år», hentet: 11.11.2022.
29 Økokrim, «Status - Arbeidslivskriminalitet», 2022.
30 Politidirektoratet, «STRASAK-rapporten 2021», 2022.

Mye av den mest alvorlige og utbyttegenererende kriminaliteten i Norge begås av norske eller utenlandske kriminelle nettverk.[31] I Norge er det flere kriminelle nettverk med høy gjennomføringsevne til å begå alvorlig kriminalitet over tid.[32] Nettverkene benytter i noen grad profesjonelle tilretteleggere både for å skjule primærforbrytelsen og for å hvitvaske utbytte fra de straffbare handlingene.

I Norge finnes det ikke god statistikk eller estimater på hvor mye utbytte som genereres fra ulike typer kriminalitet. Det er derfor i stedet lagt til grunn en vurdering av hvilke kriminalitetstyper som genererer illegal profitt (primærkriminalitet), basert på Økokrim og Politiets åpne trusselvurderinger, samt annen informasjon politiet besitter.

I tilknytning til disse kriminalitetstruslene presenteres hvitvaskingsmodus som vurderes å ha særlig høy risiko for å bli benyttet knyttet til hvitvasking av utbytte fra denne typen kriminalitet. Modusene kan imidlertid også bli benyttet ved hvitvasking av utbytte fra andre typer kriminalitet.

2.3.1. Digital kriminalitet

Digitalisering og teknologisk utvikling har økt handlingsrommet til kriminelle aktører med den følge at kriminaliteten blir mer kompleks, ikke er begrenset til fysisk rom og landegrenser og kan ramme flere på kortere tid. Sosial manipulering er ofte en sentral del av digital kriminalitet, både ved bedrageri, datainnbrudd og skadevare - tre ganske så ulike kriminalitetstyper som krever ulik form for forebygging eller respons fra politi og banker. Mye av utbytte fra de kriminelle handlingene ender i utlandet og forledelseselementet som ligger i sosial manipulering gjør at ofrene ikke alltid forstår hva de er utsatt for, før pengene er forsvunnet.[33]

Trusselen for at det genereres utbytte fra digital kriminalitet som hvitvaskes vurderes å være HØY.

Digitale bedrageri er økende og kriminaliteten genererer samlet sett stort utbytte. Bedrageriforsøkene forventes å bli mer troverdige etter hvert som ny teknologi tilgjengeliggjøres. Det er også en jevn økning i antall hendelser med løsepengevirus og mulighet for høy profitt for gjerningsaktørene, selv om norsk politi fraråder foretak og organisasjoner å betale løsepenger. Det er derfor *sannsynlig* at utbytte fra digital kriminalitet vil øke de kommende årene.

Digitale bedrageri

I følge Finanstilsynet ble det innrapportert om lag en halv milliard kroner i tap som følge av svindel i 2021.[34,35] I Sverige estimeres utbytte fra bedrageri å utgjøre over to milliarder sven-

31 Med kriminelle nettverk menes miljøer, gjenger, grupperinger eller sett av individer som samarbeider om den kriminelle aktiviteten.
32 Kripos, «Politiets trusselvurdering», 2022.
33 Økokrim, «Temarapport: Bedragerier», 2021.
34 Finanstilsynet, «Risiko og sårbarhetsanalyse - 2022», 2022.
35 Banker, kredittinstitusjoner, e-pengeforetak, betalingsforetak og filialer av slike foretak med hovedsete i annen EØS-stat skal rapportere svindelstatistikk til Finanstilsynet en gang i året.

ske kroner årlig, tilsvarende utbyttet fra narkotikaomsetning på gateplan.[36] Bedrageri regnes nå for å være den viktigste driveren til hvitvasking i USA ved at det genereres milliarder av dollar i utbytte årlig.[37]

I flere land anses investeringsbedrageri som den raskest voksende kriminalitetsutfordringen. I Norge har omfanget av investeringsbedrageri økt de senere år og det forventes at særlig investeringsbedrageri med kryptovaluta og falske handelsplattformer vil fortsette å øke. Politiet får daglig henvendelser fra personer som har investert, eller fått tilbud om å investere, i verdiløse eller tilnærmet verdiløse prosjekter. Privatpersoner utsettes fremdeles også for kjærlighetsbedrageri.

Enkelttilfeller av digitale bedrageri mot næringslivet kan medføre store tapsbeløp. Det er tilfeller hvor bedrifter frarøves over hundre millioner kroner i en hendelse. Direktørbedrageri og fakturabedrageri er de mest utbredte fremgangsmåtene i bedrageri mot foretak, og de kriminelle benytter sofistikerte og målrettede metoder. Koronapandemien har fungert som en driver i denne utviklingen, blant annet fordi mange foretak ble tvunget til rask digitalisering av virksomheten, med mange ansatte som arbeidet på hjemmekontor.

Løsepengevirus og datainnbrudd
Løsepengevirus rettet mot foretak og organisasjoner er en type skadevare som brukes til å kryptere filer hos et mål, og deretter kreve penger for å dekryptere dem eller true med å spre informasjonen. Ifølge Kripos er det en jevn økning i antall hendelser og mulighet for høy profitt for gjerningsaktørene, selv om norsk politi fraråder foretak og organisasjon å betale løsepengene. De kriminelle aktørene opererer i flere tilfeller fra Øst-Europa, og ønsker i hovedsak å få betalt løsepenger i kryptovaluta. Pengene hvitvaskes deretter gjennom flere ledd av vekslertjenester.

Datainnbrudd utgjør også en trussel mot norske virksomheter. Det er særlig dersom formålet med innbruddet er tyveri av data at det genereres økonomisk gevinst for gjerningspersonene.[38] Alt fra bedrifters innloggingsinformasjon til privatpersoners kredittkortdetaljer kan stjeles og videreselges på det mørke nettet. I følge Chainalysis utgjør inntekt fra denne type stjålet informasjon 14 prosent av inntektene fra markedsplassene på det mørke nettet i 2021.[39]

Direkteoverførte seksuelle overgrep
Enkelte nordmenn foretar transaksjoner som mistenkes å være betaling for direkteoverførte seksuelle overgrep begått i utlandet. Antallet norske statsborgere som overfører penger til kjente tilretteleggere er langt høyere enn antall personer som anmeldes for slike overgrep. Dette indikerer at omfanget er høyere enn anmeldelsestallene tilsier. Overførslene går til mennesker i utlandet som lever i fattigdom. De norske aktørene overfører relativt små beløp per overgrep. For mottakerne i utlandet kan imidlertid utbyttet fra salg av seksuelle overgrep ha en relativt større verdi.

36 Dette inkluderer ikke det man i Sverige kaller velferdsbedrageri.
37 US Department of Treasury, «National Money Laundering Risk Assessment», 2022.
38 Trusselen for at det genereres utbytte fra digital kriminalitet som hvitvaskes vurderes å være HØY.
39 Chainalysis, «Crypto Crime Report 2022», 2022.

2.3.1.1. Hvitvaskingsmodus som særlig kan knyttes til digital kriminalitet

Ved bedrageri blir utbyttet ofte hvitvasket tilnærmet i samme operasjon som primærkriminaliteten finner sted. Fornærmede overfører et beløp i tradisjonell valuta til en annen konto eller kjøper kryptovaluta og bidrar uvitende til første fase av hvitvaskingen - å skjule midlenes opprinnelse. Ved løsepengevirus og datainnbrudd hvor formålet er tyveri av penger eller verdifull informasjon, utbetales utbyttet gjerne ved en senere anledning enn når primærkriminaliteten finner sted.

Bruk av kryptovalutavekslere og miksere

Virtuell valuta er et digitalt uttrykk for en verdi som er utstedt av en privat aktør, ikke av en sentralbank eller annen offentlig myndighet. Kryptovaluta er kryptert virtuell valuta.

De fleste kryptovalutaer har full åpenhet om transaksjoner, adresser (tilsvarende bankkontoer) og innestående beløp på de ulike adressene. Hvem som er reell eier av adressene er imidlertid ukjent. Det er også en iboende sårbarhet at kryptovaluta er et digitalt og grensekryssende produkt, hvor vekslinger går raskt. Spesielt manglende beløpsgrenser, global dekning, miksetjenester, useriøse vekslingstjenester og desentralisering gjør kryptovaluta egnet for kriminelle. Kombinasjonen av dette og hopping mellom blokkjeder er noe som brukes bevisst og i økende grad av mer avanserte aktører.[40,41]

I sammenheng med kriminalitet observerer politiet at det særlig er i relasjon til bedrageri inkludert pyramidespill, narkotika og løsepengevirus at kryptovaluta dukker opp som en hvitvaskingsmodus.

Utenlandske kryptovalutavekslere

Aktører som benytter kryptovaluta i hvitvaskingsøyemed har flere fremgangsmåter. Den enkleste er å kjøpe kryptovaluta for utbytte fra kriminaliteten. Bruk av utenlandske vekslingstjenester som ikke etterlever hvitvaskingsregelverk eller er samarbeidsvillige med politiet, vanskeliggjør sporing av transaksjoner og mottakere.

> Politiet er kjent med at en utenlandsk vekslingstjeneste har mottatt kryptovaluta, blant annet utbytte fra bedrageri mot nordmenn, verdt flere milliarder kroner

Det er et relativt lite antall utenlandske vekslingstjenester som mottar mesteparten av det kjente utbyttet, både globalt og fra Norge, som hvitvaskes via kryptovaluta. Disse bruker ofte infrastrukturen og likviditeten til en større vekslingstjeneste, men har selv ansvaret for å kontrollere opplysninger om kunder og opphavet til pengene. Dette er ofte svært mangelfullt utført. Det er også utfordrende at mange av de store internasjonale kryptovekslingstjenestene holder til i jurisdiksjoner som er kjent for manglende åpenhet og tilsynsvirksomhet.[42] Kryptovekslingstjenester som opererer fra vestlige land følger som regel opp anti-hvitvaskingsarbeidet på en god måte.

40 Kripos, Politiets trusselvurdering», 2022.
41 Elliptic, «Elliptic cross-chain report 2022: The state of cross-chain crime», 2022.
42 Europol, «Cryptocurrencies: Tracing the evolution of criminal finances», 2021.

I bedragerisaker er det ikke uvanlig at fornærmede manipuleres til å selv veksle ordinær valuta til kryptovaluta, for så å sende kryptovalutaen til den kriminelles kryptovalutakonto.[43] Det er også eksempler på at kriminelle som har tatt kontroll over nettbanken til en fornærmet overfører penger til seg selv via en kryptovalutaveksler ved å utgi seg for å være fornærmede. Bedragerne benytter gjerne en kryptovalutakonto hos en av de større kryptovalutavekslerne som oppsamlingskonto for overførslene fra de fornærmede. Det benyttes også pengemuldyr som er manipulert av bedragere til å motta penger fra bedrageriofre for så å veksle pengene til kryptovaluta. Formålet er å unngå stans av transaksjoner. Økokrim har også observert tilfeller hvor forfalsket ID har blitt benyttet til å opprette kundeforhold hos utenlandske vekslere.

I relasjon til narkotikakriminalitet er det eksempler på at aktører samler opp større kontantmengder før kontantene veksles til kryptovaluta og overføres til utlandet. Nordmenn involvert i narkotikavirksomhet kan knyttes til betydelig beløp hos store utenlandske kryptovalutavekslere. Aktører innen organisert kriminalitet benytter også kryptovaluta som oppgjør seg imellom.

Miksetjenester

Miksetjenester blir stadig mer brukt av kriminelle internasjonalt og er en mer avansert form for hvitvasking. En miksetjeneste blander egen kryptovaluta med andre personers kryptovaluta og benyttes for å skjule hvor pengene kommer fra og vanskeliggjøre sporing. Per tredje kvartal 2022 har ingen større miksetjenester iverksatt effektive hvitvaskingstiltak.

I følge analyseselskapet Chainalysis mottok miksetjenester i andre kvartal 2022 over seks hundre millioner dollar (USD) i kryptovaluta fra kryptovalutaadresser tilhørende kjente kriminelle. Dette utgjorde ca. 23 prosent av den totale mengden kryptovaluta som ble mottatt av miksetjenester i denne perioden. Særlig nordkoreanske og russiske cyberkriminelle var blant de meste aktive brukerne.[44]

Politiet er kjent med at miksetjenester også er benyttet av norske aktører for å hvitvaske utbytte fra kriminalitet.

Hvitvasking via kjøp og omsetning av digital kunst - NFT

NFT står for Non-fungible token og er et unikt kryptografisk eierskapsbevis. En offentlig tilgjengelig blokkjede brukes for å lagre og beskytte eierskapet gjennom en unik kode. NFT benyttes blant annet som eierskapsbevis for at en eier et aktuelt bilde, videoklipp, billett eller gjenstand i et spill. NFT kjøpes og selges på digitale markedsplasser ved bruk av ulike kryptovalutaer og omsetningen økte fra 106 millioner amerikanske dollar i 2020 til 44,2 milliarder dollar i 2021.[45]

43 Finanstilsynet, «Risikovurdering – Hvitvasking og terrorfinansiering», 2019.
44 Økokrim, «Notat: Miksetjenester», 2022.
45 Chainalysis, «Crime and NFTs: Chainalysis Detects Significant Wash Trading and Some NFT Money Laundering In this Emerging Asset Class», 2022.

Globalt var det i 2021 og første halvdel av 2022 en stor økning i kjøp og salg av NFTer.[46] Siden har det derimot vært et stort fall i omsetningen.[47] Bruksområdet for NFTer kan derimot bli betraktelig større enn i dag. Eksempelvis kan artister bevise eierskap til musikk eller video, noe som vil gjøre det mulig for kunstnere, artister og andre å selge sine produkter og tjenester direkte til fans.

Handel med såkalt kryptokunst, unike digitale kunstverk som inneholder en digital kode som bevis på eierskap (NFT), kan benyttes til hvitvasking av midler fra kriminalitet. Selv om det er mulig å spore kjøper og selger av kryptokunst er det ingen krav om at selger/kjøper legitimerer seg. Manglende identifisering av kjøper og selger gjør det i praksis mulig å kjøpe digital kryptokunst av seg selv, og det dermed er også godt egnet for hvitvasking av straffbart utbytte.

Bruk av neobanker

Neobanker tilbyr banklignende tjenester via en app eller en nettside.[48] Neobanker har ikke fysiske filialer, og har gjerne også utspring fra FinTech-bransjen med fokus på brukervennlighet og bruk av teknologi til å forenkle prosesser. De tilbyr som regel bankkonto og betalingskort, men kan også tilby tilleggstjenester som enkel veksling mellom ulike valutaer eller investering i kryptovaluta. Eksempler på neobanker er Revolut, N26, Paysera, Stripe og Wise.

Neobanker har som regel konsesjon som bank eller e-pengeforetak. Norske foretak av denne typen skal ha konsesjon og vil da være under tilsyn av Finanstilsynet. Utenlandske foretak som ønsker å rette seg mot det norske markedet må ha meldt om grensekryssende virksomhet. Disse foretakene skal ha konsesjon fra, og da være underlagt tilsyn i sine hjemland.

Neobanker benyttes av kriminelle som oppgjørskanal for blant annet kjøp og salg av illegale varer på det mørke nettet, narkotikahandel, til hvitvasking og terrorfinansiering. For eksempel har betalingskort tilknyttet en utenlandsk neobank blitt brukt til å ta ut store mengder kontanter og til å kjøpe dyre varer i Norge. Personer som betaler for overgrepsmateriale og direkte-overførte seksuelle overgrep på nett benytter ofte internettbaserte betalingstjenester. I bedragerisaker benyttes ofte neobanker for raskt å føre pengene ut av Norge. Dette gjøres gjerne av pengemuldyr. I flere arbeidslivskriminalitetsaker ser man også at ulike neobanktjenester benyttes.

Hovedutfordringen med neobanker er at det nå er enklere å opprette et kundeforhold i en utenlandsk bank. Neobanker muliggjør også raske overføringer av penger kontantfritt.[49] Det er også usikkert hvorvidt enkelte av neobanktjenestene utfører tilstrekkelig kundekontroll, og eventuelle avdekkede mistenkelig transaksjoner blir uansett rapportert til FIUen i foretakets hjemland selv om transaksjonen er mellom to nordmenn. Disse egenskapene gjør det enklere for kriminelle aktører å skjule grensekryssende transaksjoner, reelt eierskap, inntekt og formue.

46 Business Insider, «NFT sales hit $293 million over the past week» , 2021.
47 Dune analytics, «@thomas_m / NFT market overview», hentet: 01.11.2022.
48 Black Wallet project, «Black Wallet Guidebook for Law Enforcement Agencies», 2021.
49 FATF, «Guidance on Digital Identity», 2020.

Utenlandske spillselskaper

Det har vokst frem et stort uregulert marked av utenlandske pengespill som kasino, poker, oddsspill og bingo på internett. Lotteritilsynet estimerer at det uregulerte pengespillmarkedet utgjorde mellom 1,8 og 2,2 milliarder kroner i 2021. Til sammenligning var det norske pengespillmarkedet på 10,6 milliarder kroner i 2019.[50] Utenlandske pengespill har ikke de samme taps- og innsatsbegrensningene som norske spillselskap, og vil dermed være mer attraktive å benytte til hvitvaskingsformål.

Norske banker og andre betalingstjenester i Norge har ikke lov til å formidle innsats og utbetaling i pengespill som tilbys av pengespillselskaper uten tillatelse i Norge.[51] Det benyttes neobanker til å omgå dette forbudet.

Ofte brukte modus er at man overfører utbytte fra straffbare handlinger via en betalingsformidlingstjeneste til en utenlandsk spillekonto. Utbyttet kan brukes til å spille, men kan også oppbevares på spillekonto en kort periode før man tar ut pengene igjen, gjerne til bankkonto i en annen bank slik at det blir vanskeligere for rapporteringspliktige å se sammenhengen. Man kan også overføre innskudd på spillekonto til en annen spillekonto hos den samme spill tilbyderen som oppgjør imellom to personer. Uavhengig av om utbyttet genererer gevinst eller har vært urørt, vil flytting og endring av form på utbyttet være hvitvaskingshandlinger.

Det er rapportert om flere tilfeller hvor norske personer som kan knyttes til alvorlig profittmotivert kriminalitet overfører store summer til utenlandsk spillekonto. I flere tilfeller er de involverte omhandlet med narkotikakriminalitet og bedrageri. Beløpene varierer fra noen titalls tusen- til flere millioner kroner. Fremgangsmåten kan for eksempel være at flere personer spiller ved det samme digitale pokerbordet med kontakt via telefon underveis. De sørger deretter for at den som skal ha betalt vinner pokerspillet, og vedkommende kan deretter legitimere inntekten som gevinst fra spill.[52]

Forhåndsbetalte kort

Ved kjøp av gave- og forhåndsbetalte kort vanskeliggjøres sporing og det er enklere å flytte pengene over landegrenser.[53] Mange fornærmede i bedragerisaker kjøper gavekort som de deretter sender bedragere, typisk ved kjærlighetsbedrageri. Andre ganger blir pengemuldyr lurt til å kjøpe gavekortene på vegne av bedragere. En indikator på at kjøp av gavekort gjøres for å hvitvaske penger er at det kjøpes flere gavekort for store totalbeløp samtidig.

Gavekort fra Apple er svært populære. Dette skyldes trolig at disse er likvide og man trenger kun å benytte koden på disse for å handle. Bedragere kan derfor bruke koden til å handle Apple produkter hvor som helst

En person har alene har kjøpt gavekort for nesten seks millioner kroner over en fem-års periode.

50 Lotteri- og stiftelsestilsynet, «Risikovurdering – Hvitvasking og terrorfinansiering, oktober 2021», 2021.
51 Lotteri- og stiftelsestilsynet, «Pengespill på nett», 2020.
52 Polisen, «Penningtvätt på spelmarknaden» 2021.
53 Økokrim, «Infoskriv - Modus hvor offer fra kjærlighetsbedrageri kjøper dyre varer og gavekort for å omgå bankenes kontroll med internasjonale transaksjoner», 2021.

i verden, og få disse levert til ønsket adresse. Flere utenlandske borgere bosatt i Norge har forsøkt å kjøpe gavekort fra Apple for betydelige beløp ved å forhåndsbestille gavekortene fra matbutikker ulike steder i Norge.

Paygoo-kort er et annet forhåndsbetalt kort som ofte kjøpes med utbytte fra spesielt bedrageri. Det er også observert tilfeller hvor fornærmede kjøper gavekort til Playstation Store. Her er det på samme måte som for Apple gavekort kun behov for å sende en kode (QR-kode), ingen fysisk forsendelse. Kriminelle aktører benytter også nettbaserte tilbydere av virtuelle gavekort til hvitvasking av utbytte.

Visa og MasterCard debetkort som fylles opp ved å bruke kryptovaluta som innskudd benyttes både til skatteunndragelse og hvitvasking. Bitplastic, Coinbase Card og Crypto.com er konkrete eksempler på dette. Skatteetaten antar at disse vil bli brukt i økende omfang fremover. Det eksisterer også uregistrerte kryptovalutavekslere som aksepterer gavekort som betaling.

2.3.2. Kriminalitet i og via foretak

En rekke ulike typer kriminalitet begås i og via foretak. Både ved arbeidslivskriminalitet og ved fiskerikriminalitet er det i hovedsak gjennom næringsdriften at det genereres utbytte fra en ellers lovlig vare eller tjeneste som omsettes. Mange lovlige varer transporteres både nasjonalt og over landegrenser og er også svært godt egnet til hvitvasking.

Trusselen for at kriminalitet i og via foretak genererer utbytte som hvitvaskes vurderes å være HØY.

Kriminalitet i og via foretak er stabil hva gjelder omfang, men genererer like fullt stort utbytte og foretak kan også benyttes til hvitvasking. Økonomisk nedgangstid kan føre til økt konkurskriminalitet og at flere begår arbeidslivskriminalitet. Domfellelse og etterforskning av korrupsjonssaker i Norge det siste året viser at det trolig genereres millionbeløp i utbytte ved korrupsjon. Det er derfor *sannsynlig* at utbytte fra kriminalitet i og via foretak vil holde seg stabilt på et forholdsvis høyt nivå de kommende årene.

Arbeidslivskriminalitet

Utbytte fra arbeidslivskriminalitet kommer fra skatte- og avgiftskriminalitet, samt besparelser ved å unndra seg arbeidsgiveransvar, manglende HMS-tiltak og lønnstyveri fra sårbare arbeidstakere. Særlig har kriminaliteten vært utbredt i arbeidsintensive bransjer med lave kvalifikasjonskrav og hvor det er utstrakt bruk av underleverandører.[54,55]

Under koronapandemien økte internetthandelen og etterspørselen etter hjemlevering av varer. Varetransportbransjen er lite regulert og det er lave oppstartskostnader. Det er avdekket utstrakt bruk av underleverandører, bevisst bruk av enkeltpersonforetak for å unndra seg arbeidsgiveransvar, svart avlønning og annen skatte- og avgiftsunndragelse. Etter koronapan-

54 NRK, «Posten ber om hjelp fra regjeringen med å bli kvitt sosial dumping», 2022.
55 NTAES, «Leverandører til det offentlige», 2022.

demien har man også sett en økning i bruk av ulovlig arbeidskraft i bygg- og anleggsbransjen, samt i andre bransjer med stor andel utenlandske arbeidstakere.

Fiskerikriminalitet
Norsk sjømat er Norges nest største eksportvare etter olje og gass og de enorme økonomiske verdiene tiltrekker seg aktører som profitterer på blant annet ulovlig fiske, systematisk under- og feilrapportering av fangst og svart omsetning.[56] Den svarte omsetningen skjer både fra mindre fartøy og hos større aktører i næringen. Aktørene er primært norske, men også utenlandske kriminelle nettverk er omhandlet med denne typen kriminalitet. Aktørene som både er horisontalt og vertikalt integrert i verdikjeden utgjør størst trussel. I noen tilfeller samarbeider ulike fartøy, mottak og selgere om den kriminelle aktiviteten, og det er ofte tette tillitsbånd mellom aktørene.

Det er også indikasjoner på at enkelte turistfiskeforetak legger til rette for at turister tar med seg mer fisk ut av landet enn de har lov til. I enkelte tilfeller fremstår turistfisket som godt organisert, med ulike arbeidslag og varebiler med permanent monterte frysebokser som frakter fisken ut av landet på nattestid.

Korrupsjon
I følge Europol er nærmere 60 prosent av de kriminelle grupperingene i EU innblandet i korrupsjon.[57] I Norge avdekkes det sjelden korrupsjonssaker, men det antas at korrupsjonsfaren i kommunal sektor er særlig til stede der privat og offentlig sektor møtes, som i offentlige anbudskonkurranser eller i tildeling av tillatelser. Sommeren 2022 ble også en tidligere kommuneansatt og en bedriftseier dømt til flere års fengsel for grov korrupsjon og til å betale erstatning på 21 millioner kroner til kommunen som var utsatt for momsbedrageri ved fiktiv fakturering.[58]

Profesjonelle tilretteleggere innen bank og finans benyttes særlig til å gi lån på uriktig grunnlag mot vederlag på grunnlag av fiktive a-meldinger og forfalskede lønnsslipper og boligutleiekontrakter.[59] Våren 2022 ble flere bankansatte i to banker siktet for grov korrupsjon og grovt bedrageri for å ha tilrettelagt for uriktig innvilgelse av lån mot vederlag. I det ene tilfellet dreier det seg om lån for til sammen 150 millioner kroner.[60,61]

Konkurskriminalitet
Konkurskriminalitet favner om en rekke type lovbrudd begått i forkant av at det åpnes konkurs i en bedrift og skyldes ofte mangel på likviditet i virksomheten. Kriminaliteten kan være overtredelser av regnskapsloven, skatt- og avgiftsloven og bedrageri av kreditorer. Lovovertredelser kan direkte skade virksomheter og indirekte ramme kreditorfellesskapet ved utroskap, underslag og urettmessige utdelinger i strid med aksjelovgivningen.

56 Økokrim, «Trusselvurdering», 2022.
57 Europol, «Serious and organised crime threat assessment (SOCTA)», 2020.
58 NRK, «Dom i svindelsaken i Tana: Må i fengsel samt betale tilbake 21 millioner kroner – NRK Troms og Finnmark», 2022.
59 Økokrim, «Temarapport - Profesjonelle aktører», 2021.
60 TV2, «Flere bankansatte arrestert for grov korrupsjon: - Alle løslatt», 2022.
61 Finanswatch, «Korrupsjonssiktet tidligere DNB-ansatt er også siktet for forhold knyttet til en annen bank», 2022.

I 2021 ble det åpnet 4926 konkurser.[62] Ifølge Konkursrådet avdekkes det mistanke om straffbare forhold i ca. halvparten av konkurs- eller tvangsavviklingsboene i Norge.[63] Økokrim etterforsket tre konkurssaker som endte i rettskraftig dom i 2021.[64]

Bedrageri av det offentlige

Under Korona-pandemien innførte regjeringen flere støtteordninger og økonomiske tiltak for næringsliv og kultur. Ett av disse var lønnstøtteordningen som gjaldt foretak som hadde fall i omsetning grunnet smitteverntiltak. Både enkeltaktører og sentrale aktører i kriminelle nettverk begikk bedrageri av lønnstøtteordningen. Politiet har etterforsket flere enn 50 saker vedrørende utnytting av ordningen.

Skatte- og avgiftskriminalitet begås både av enkeltpersoner og selskaper og er utbredt på tvers av bransjene i arbeidslivet fordi slike kriminelle handlinger gir høy profitt og oppdagelsesrisikoen er lav. En metode for å unndra beskatning i Norge er å skjule verdier i såkalte skatteparadis.[65]

Grensekryssende merverdiavgiftssvindel

Momskaruseller[66], der varer blir fakturert gjennom flere ledd i forskjellige land og i et høyt tempo, er et kjent fenomen innen EU og anses der som en trussel mot merverdiavgiftssystemet og hele velferdsstaten på grunn av de enorme beløpene som unndras.

Utsatt avregning ble innført i 2017 som en forenkling for de næringsdrivende. Frem til da var risikoen for grensekryssende merverdiavgiftssvindel i Norge knyttet til visse typer tjenester, som for eksempel klimakvoter som skattemyndighetene avdekket svindel med allerede i 2010.

Europol trekker frem risiko-sektorer som edle metaller, mobiltelefoner og annet elektronisk utstyr med høy verdi, grønne sertifikater og energisektoren.[67] Skattemyndighetene har advart energibransjen i Norge og Europa om forsøk på svindel med grønne sertifikater.[68]

Grenseryssende merverdiavgiftssvindel genererer enorme strømmer av finansielle transaksjoner, både innenlands og utenlands. Stadig skiftende betalingsløsninger, kompleksiteten og globaliseringen gjør det vanskeligere for skattemyndighetene å spore pengestrømmer fra denne svindelen og få tilbake unndratt merverdiavgift. Det er også avdekket hvitvasking i flere saker.

62 Brønnøysundregisteret, Konkurrsstatistikk 2018-2022.
63 Kapital, «Konkursrådet kritisk til politiets behandling av konkurskriminalitet», 2021.
64 Oslo tingretts dom 06.05.21 Saksnr. 21-038329ENE-TOSL/05, Eidsivating lagmannsretts dom, 07.04.21 Saksnr. 20-096455AST-ELAG/, Møre og Romsdal tingrett 04.05.21, Saksnr. 21-016773MED-TMOR/TVOL.
65 Økokrim, «Trusselvurdering», 2022.
66 Missing Trader Intra-Community (MTIC) Fraud.
67 Europol, «MTIC (Missing Trader Intra Community) fraud», ukjent.
68 Skatteetaten, «Skatteetaten advarer: Risiko for MVA-svindel med grønne sertifikater», 2019.

2.3.2.1. Hvitvaskingsmodus som særlig kan knyttes til kriminalitet i foretak

Ved kriminalitet i foretak benyttes ofte foretaket og foretakets virksomhet også til selve hvitvaskingen av utbytte.

Selskapsstrukturer benyttes til hvitvasking

Selskapsstrukturer egner seg godt for å hvitvaske utbytte fra kriminalitet da de har gjennomgående høyere kapitalflyt enn privatpersoner, gis høyere kreditt og har en kundemasse som sikrer en tilsynelatende legal fasade.[69] Mer enn 80 prosent av de kriminelle nettverkene undersøkt av Europol benytter legale selskapsstrukturer i kriminalitetsutøvelsen. Rundt halvparten av de kriminelle nettverkene oppretter egne legale selskapsstrukturer eller infiltrerer eksisterende selskaper.[70]

Bransjer med høyt omløp av kontanter øker risikoen for hvitvasking, da kontanter som stammer fra kriminalitet blant annet kan benyttes til svart avlønning. I arbeidsintensive bransjer med stor utbredelse av arbeidslivskriminalitet benyttes ofte også underleverandører som et verktøy i selve hvitvaskingsprosessen, for eksempel ved fiktiv fakturering. Skatteetaten observerer at inntekt fra arbeidsgivere eller bemanningsbyrå som ikke er oppgitt for beskatning og som kanaliseres via utlandet, har økt. Det mistenkes også at enkelte butikker hvitvasker kontantutbytte fra kriminalitet ved kontantkjøp av varer fra grossister som deretter selges i butikken.

Det foregår også samarbeid mellom kriminelle nettverk som driver med organisert narkotikakriminalitet og nettverk som driver med økonomisk kriminalitet eller arbeidslivskriminalitet. Foretak i næringslivet benyttes som tilsynelatende legal fasade og benyttes til hvitvasking samt trygde- og lånebedrageri. Under pandemien benyttet også kriminelle nettverk og aktører innen narkotikahandel legale foretak til å begå bedrageri av offentlige støtteordninger ved å opprette fiktive a-meldinger.[71]

Virksomheter benyttes også ved grensekryssende banktransaksjoner ved at bedriftskonto stilles til disposisjon som transittkonto. Det foreligger også informasjon om utenlandske aktører innen fiskerinæringen som benytter norske foretak til å hvitvaske og overføre penger til utlandet.

Handelsbasert hvitvasking

Britiske National Crime Agency anser grensekryssende handel som en av de mer komplekse metodene for hvitvasking.[72] Handelsbasert hvitvasking foregår ved å underslå eller overrapportere pris, kvantitet eller kvalitet ved import eller eksport.[73] Det er altså en form for over- eller underfakturering av varers reelle verdi og oppgitt verdi

> En fremgangsmåte ved handelsbasert hvitvasking kan være å oppgi for lav kilopris ved tolldeklarasjon av sjømat.

69 BRÅ, «Kriminell infiltration av företag», 2016.
70 Europol, «Serious and organised crime threat assessment (SOCTA)», 2021.
71 Børsen, «Mistenkt bedrageri med corona-millioner», 2020.
72 National Crime Agency, «National Strategic Assessment of Serious and Organised Crime», 2018.
73 FATF, «Trade-based money laundering», 2006.

(fakturabeløp). Attraktive varer som benyttes til handelsbasert hvitvasking er varer som er vanskelig å vurdere verdien av, som eksempelvis gullvarer, smykker, kunst og samlegjenstander, men også fisk og byggevarer er benyttet. Varene fremstår legitime og selve pengeutbyttet må ikke krysse landegrensene.

Handelsbasert hvitvasking forutsetter ofte et samarbeid mellom eksportør og importør. Ved at eksportøren overfakturerer varene, kan importøren overføre ett større beløp enn hva som er markedsverdien på produktene. Det motsatte, altså underfakturering, gjør at importøren sitter igjen med produkter til en høyere markedsverdi enn hva man betalte. Det samme kan gjøres ved at mengden varer som eksporteres/importeres er høyere eller lavere enn hva man fakturers for, og dermed blir det overskytende beløpet hvitvasket.[74]

Eksportvirksomheter kan også benyttes for å kjøpe lovlige varer med utbytte fra kriminalitet.[75] Det er eksempler på at utbytte fra bedrageri mot nordmenn benyttes til å kjøpe tørrfisk og fiskehoder, som deretter eksporteres til afrikanske land. Utbytte fra bedrageri er også benyttet til å kjøpe bruktbiler i Norge som eksporteres til afrikanske land.

Hvitvasking via eiendomsmarkedet

Eiendomsmarkedet er kapitalintensivt, noe som muliggjør hvitvasking av store beløp i enkelttransaksjoner.[76] I mange tilfeller er de involverte omhandlet med narkotikakriminalitet, svart arbeid og bedrageri.

Kriminelle aktører investerer i privatboliger og næringsbygg, både i Norge og i utlandet.[77] Det benyttes ofte stråpersoner og stråselskaper for å tilsløres midlenes opphav og reell eier. I tillegg kan profesjonelle aktører som eiendomsmeglere og advokater medvirke med fiktive verdivurderinger og tilrettelegge for såkalt svingdørsalg[78], hvor samme eiendom omsettes hyppig og gjerne med unormal prissetting.

En fremgangsmåte for å hvitvaske midler i eiendomsmarkedet er å betale for utbedringer og oppussing som ofte utføres svart med utbytte fra kriminalitet. Endringen i avhendingsloven som trådte i kraft 1. januar 2022, stiller strengere krav til dokumentasjon til utbedringer av eiendom, men dette kan omgås.

Eiendomsbransjen rapporterer at kjøp, oppussing og raske videresalg av borettslagsleiligheter er et økende problem. Rask verdistigning og omsetning utenfor det åpne markedet kort tid etter kjøp, kan være en hvitvaskingsoperasjon dersom det er avtalt pris mellom kjøper og selger, eller eiendomsverdier er manipulert. Dette strider mot brukereierprinsippet i borettslagsloven, men det er lite effektive sanksjonsmuligheter for å hindre slike oppkjøp.

74 CITI, «Trade-Based Money Laundering», 2016.
75 FATF, «Trade-based money laundering: Trends and development», 2020.
76 Finanstilsynet, «Risikovurdering – Hvitvasking og terrorfinansiering», 2019.
77 NTAES, «Situasjonsbeskrivelse – Arbeidslivskriminalitet 2019», 2020.
78 Hyppig salg av samme eiendom med unormal prissetting.

Eiendom registrert i selskaper kan også bytte eier hyppig uten at dette registreres. Manipulasjon av eiendomsverdi er utfordrende å avdekke. Det samme er omsetning av kontrakter på kjøp i fremtidige byggeprosjekter.

Det foreligger også informasjon om at kriminelle samarbeider om hvitvasking i eiendomsmarkedet ved at huseier leier ut boligen til langt over markedspris slik at leietaker hvitvasker midler gjennom leieforholdet. Dokumentasjon på høye leieinntekter kan i tillegg generere en kunstig høy salgssum av eiendommen.[79]

Skatteetaten erfarer at utenlandske selskap eier bolig i Norge der reell eier av selskapet er skattepliktig til Norge. Ifølge Transparency International eies over 500 eiendommer på Aker Brygge, Tjuvholmen, Sørenga og Bjørvika i Oslo av selskap registrert i såkalte skatteparadis. I gjennomsnitt eies 13 prosent av eiendommene i Oslo av juridiske personer (foretak), mens i de nevnte bydelene er dette og 33 prosent. En betydelig andel av disse foretakene kan knyttes til Kypros.[80]

Indikasjoner på hvitvasking via eiendom kan være at innbetaling til megler kommer fra andre enn kjøper og at utbetaling skjer til andre enn selger. Bransjen erfarer også at det gis bud av en privatperson med forbehold om at de skal utpeke en kjøper/hjemmelshaver. Skjult eierskap, bruk av sekretessejurisdiksjoner, kompliserte selskapsstrukturer og indirekte transaksjoner via stråmenn er andre fremgangsmåter som benyttes ved hvitvasking i eiendomsmarkedet.

2.3.3. Handel med ulovlige varer og mennesker

Omsetning av ulovlige varer og tjenester genererer et betydelig utbytte. Spesielt ved narkotikainnførsler og handel med truede arter føres utbyttet fra kriminaliteten ut av Norge, både i form av kontanter og som grensekryssende transaksjoner.

Trusselen for at det genereres utbytte som hvitvaskes fra handel med ulovlige varer og mennesker vurderes å være HØY.

Handel med ulovlige varer og mennesker utføres i stor grad av organiserte kriminelle nettverk som opererer over landegrenser. Det registrerte utbyttet fra narkotikakriminalitet er høyt og det faktiske utbytte som genereres er med sikkerhet enda høyere. Internasjonale markeder fører til stor omsetning av ulovlige varer som avfall og truede arter. Det er derfor *sannsynlig* at utbytte fra handel med ulovlige varer vil fortsette å være på et høyt nivå de kommende årene.

Narkotikakriminalitet

Kriminelle nettverk i Norge er involvert i innførsel og omsetning av narkotika. Selv om det totale antallet anmeldelser og beslag knyttet til narkotikakriminalitet er redusert de seneste årene, ble det i 2021 i Norge beslaglagt narkotika og legemidler til en verdi av om lag én milliard kroner.[81] Det faktiske utbyttet som genereres fra innførsel og omsetning som ikke avdekkes av politiet er med sikkerhet betydelig større.

79 Finansavisen, «Eiendomsbransjen har vært for naive», 06.05.2022.
80 Transparency International Norge, «Hvem eier Oslo? Hvitvaskingsrisiko i eiendomsmarkedet», 2021.
81 Beslagene i 2021 i antall kilo for noen tyngre stoffer har vært høyere enn tidligere.

Hasj er den type narkotika det beslaglegges mest av, etterfulgt av amfetamin og marihuana. Antall kokainbeslag økte i Norge i 2021 og trenden forventes å øke da dette stoffet regnes for å være det nest mest vanlige narkotiske stoffet i Europa.[82]

Opprinnelseslandet til de narkotiske stoffene samt fraktruter kan gi en indikator på hvor betalingen for narkotikapartiene tar veien i retur. Dette er særlig aktuelt i de tilfeller hvor organisator i utlandet tar risikoen og pengene betales når stoffet er distribuert og videresolgt. Det er grunn til å tro at det er svært mye kontanter i omløp ved bruk av denne metoden. Beslag fra Tolletaten indikerer at norske kroner blir fraktet ut av Norge, både til Sverige, Nederland og Tyrkia. Større narkotikaparti kan også betales før de sendes fra opprinnelsesland. Det er uklart om oppgjør da skjer i kontanter eller via andre betalingsmetoder. Den siste metoden er en kombinasjon av de to ovenfor og fremstår som en foretrukket løsning for å spre risiko blant aktørene involvert i innførsel og transport. Denne modusen vil også blant annet innbefatte uttransportering av kontanter fra Norge.

Utbytte fra narkotikakriminalitet i Norge hvitvaskes ofte ved generelt forbruk, kjøp av verdigjenstander og gjennom tilsynelatende legal virksomhet i Norge eller ved at det kanaliseres til utlandet.

Handel med truede arter

Globalt er handelen med truede arter en milliardindustri og kategoriseres som «alvorlig organisert kriminalitet» av FN.[83] I hovedsak går handelen fra land i sør til pengesterke kjøpere i nord. Norge er derfor først og fremst et marked for kjøp av slike produkter, men har også sin plass i omsetningskjeden som leverandør av rovfugler og -egg som tas ut, og som transittland. Informasjonen om koblinger til organisert kriminalitet ved handelen i Norge er begrenset, men vi vet at norske arter er ettertraktet blant samlere nasjonalt og internasjonalt. Vi ser også eksempler på at næringsdrivende og privatpersoner importerer truede arter eller produkter av disse for videresalg. Hvor mye som genereres i utbytte fra slik type handel med knytning til Norge er derimot ukjent.

Ulovlig eksport av avfall

EE-avfall inneholder verdifulle komponenter med høy omsetningsverdi. FN har tidligere estimert at det årlig på verdensbasis dumpes eller omsetter ulovlig EE-avfall til en verdi av 19 milliarder dollar (USD). Returselskapene i Norge har i prosjektet «EE-avfall på avveie» dokumentert at tyverier av EE-avfall fra elektrokjedens returpunkter er meget utbredt. I Stor-Oslo er aktørene primært personer fra Øst-Europa, samt aktører med opprinnelse fra Vest-Afrika som driver eksportnæring. Den ulovlige eksporten skjer hovedsakelig til Nigeria, Romania og Litauen.[84] Mye av denne kriminaliteten virker godt organisert og enkelte av aktørene kan også knyttes til annen, alvorlig kriminalitet, som grovt bedrageri, hvitvasking og narkotikakriminalitet. I tillegg til det ulovlige utbyttet kriminaliteten generer, er ulovlig eksport av EE-avfall grensekryssende miljøkriminalitet som har alvorlige konsekvenser for både mennesker og natur i de landene avfallet eksporteres til.

82 Kripos, «Narkotika- og dopingstatistikk», 2021. Verdien er beregnet basert på veiledende markedspriser per gram for de ulike narkotiske stoffene.
83 United Nations, «General Assembly resolution 69/314 - Tackling Illicit Trafficking in Wildlife», 2015.
84 RENAS, «EE-avfall på avveie», 2022.

Menneskehandel
Det ble i 2021 anmeldt totalt 29 forhold som gjelder menneskehandel hvorav én gjaldt prostitusjon eller andre seksuelle ytelser, og ti omhandlet tvangsarbeid. Det er det laveste antallet anmeldelser på flere år. Samme år var det tre domfellelser for menneskehandel, hvorav en endte med frifinnelse.[85]

Utbyttet som genereres fra menneskehandel kan være betydelig, både ved prostitusjon og tvangsarbeid, men sakene er ofte vanskelige å avdekke og utfordrende bevismessig. I en rettskraftig dom fra 2021 ble en fornærmet tilkjent erstatning for manglende lønn på rundt 850 000 kroner, hvilket gir en indikasjon på størrelsen av utbyttet gjerningspersonen har hatt av utnyttelsesforholdet.[86]

2.3.3.1. Hvitvaskingsmodus som særlig kan knyttes til omsetning og smugling av ulovlige varer

Felles for omsetningen av både lovlige og ulovlige varer er at oppgjøret gjennomføres i en annen transaksjon enn varetransaksjonen. Innenfor kriminelle grupper foregår en utstrakt bruk av kontanter.[87] I tillegg ser vi at ulovlige varer i større grad nå betales for med kryptovaluta.[88]

I tillegg til risikomodusene som trekkes frem under er bruk av veldedige organisasjoner gunstig for tilsløring av utbytte i kontanter, da opphavet til midlene kamufleres som pengeinnsamling, i tillegg til at knytninger mellom kriminell virksomhet og mottager tilsløres.

Kjøp av verdigjenstander
En velkjent fremgangsmåte i Norge for å hvitvaske kontanter er ved kjøp av ulike verdigjenstander som kunst, kostbare klokker, merkeklær og kjøretøy. Kjøpet tilslører opphavet til utbyttet. Ved videresalg av gjenstandene fremstår oppgjøret som legal inntekt. Gjenstandene er lett omsettelige og kan benyttes som oppgjørsmiddel ved en senere anledning. Gjenstander som er utfordrende å verdi-vurdere gir også kriminelle et mulighetsrom for å kjøpe og selge til under- eller overpris.

Kjøp av kostbare klokker er en mye benyttet hvitvaskingsmetode for aktører som har profittert på både narkotikakriminalitet, bedrageri og arbeidslivskriminalitet. Klokkene kjøpes med kontanter, stjålne bankkort eller med gavekort. Enkelte kriminelle aktører skal angivelig ha klokkesamlinger verdt flere millioner kroner. Flere av dem selger også kostbare klokker på markedsplasser på internett.

Kunst er en annen kostbar gjenstand som kjøpes for å hvitvaske utbytte fra kriminalitet. Den usikre markedsverdien på kunst gjør det vanskelig å avdekke om gjenstanden er kjøpt for over/underpris.[89] I tillegg er det lite kontroll og manglende oversikt over eierskap og

85 KOM, «Rapport fra Koordineringsenheten for ofre for menneskehandel 2021», 2022.
86 Hålogaland lagmannsrett dom av 17.11.2020 (LH-2020-114183). Rettskraftig ved Høyesteretts beslutning av 19.02.2021 (HR-2021-354-U).
87 NOU 2020: 10, «Straffelovens utredning nr. 2 – Inndragning av utbytte fra gjengkriminalitet», 2020.
88 Chainalysis, «Crypto Crime Report 2022», 2022.
89 Økokrim, «Miljøkrim», desember 2021.

transaksjoner innen kunsthandel.[90] Salget kan også realiseres gjennom lovlige kanaler som kunsthandlere. De er ikke rapporteringspliktige, så oppdagelsesrisikoen er lav. I noen tilfeller benyttes malerier også som sikkerhet for lån blant kriminelle.

Tollagre for oppbevaring av ufortollede varer fra utlandet benyttes i økende grad av investorer og kunstsamlere som permanente oppbevaringsplasser for kunstgjenstander.[91] Lite myndighetskontroll og hemmelige kundelister muliggjør fordekt omsetning av kunst og dermed hvitvasking via slike lagre.[92,93]

Bingospill
Høy kontantomsetning, en gevinstprosent på rundt 80 prosent og skattefri gevinst gjør bingospill attraktiv for hvitvasking. Bingoenes spillekort er ikke registrert på person hvilket vanskeliggjør verifisering av identitet på spiller og omfanget det spilles for. Ved å sette inn kontanter på sin spillekonto, for deretter å overføre dette til bankkonto fremstår transaksjonen som en gevinstutbetaling. Ved fremvisning av spill-kvittering vil gevinster fremstå som legalt tilegnede midler.

Omsetning av spill-kvitteringer er også en kjent metode for hvitvasking av utbytte fra straffbare handlinger.

Spill i bingohaller foregår i skjermede omgivelsene og hallene har lange åpningstider. I kombinasjon med sentrumsnære lokasjoner er bingohaller et egnet sted for kriminelle å møtes uforstyrret for å spille eller kjøpe spill-kvitteringer med formål om hvitvasking.

Hawala og ulovlig utførsel av kontanter
Hawala er et uformelt system for betaling og pengeoverføringer over landegrenser. Betalingssystemet er en populær måte å overføre penger til hjemlandet for diasporamiljøer i Norge, men de legale pengestrømmene kan også bidra til å tilsløre overførsler som er utbytte fra kriminalitet. Felles for flere av betalingsformidlerne er at de kombinerer legal pengeformidling for diasporamiljøer i Norge med uregistrert betalingsformidling og hvitvasking.

> Det er grunn til å tro at penger som oppgjør for narkotikaparti fraktes fysisk til Tyrkia.

Store summer overføres årlig fra Norge til utlandet ved bruk av Hawala, både via utførsel av kontanter og som bankoverføring. I den grad overføringer er hvitvaskingshandlinger, sendes pengene ut av landet uten knytning til riktig identitet for å omgå krav om at avsender skal kunne identifiseres i Valutaregisteret.[94] Det er heller ikke uvanlig å overføre utbyttet til et land midlertidig for deretter å videreføre pengene til andre land.

90 European Commission, «Supra-National Risk Assessment (SNRA)», 2022.
91 UNESCO, «Free Ports and risks of illicit trafficking of cultural property - ICPRCP/16/20.COM/12», 2016.
92 Dagens Næringsliv, «Toll, Skattekrim og Kemneren aksjonerte mot kunstlager» , 2019.
93 Dagens Næringsliv, «Kunstlagerets konfidensielle «show room"», 2019.
94 Finanstilsynet, «Merknader – endelig rapport: Iftin Express Michael Duale», 28.04.2017.

Det er identifisert flere tilfeller av at foretak som bedriver ulovlig Hawala-virksomhet er registrert som foretak innen en helt annen bransje hvor det er naturlig med grensekryssende pengeoverføringer. Overføringer fra slike foretak kamufleres ofte med mangelfulle og/eller fiktive fakturaer.

Innstramming av hvitvaskingsregelverket og tilbaketrekking av konsesjonen til flere betalingsforetak som bedrev ulovlig hawala-virksomhet, medførte at flere av foretakene startet med betydelig utførsel av kontanter i 2019. Nå ser vi en stor nedgang i deklarert fysisk utførsel av kontanter. Det er grunn til å tro at nedgangen skyldes at Hawala-aktører i stedet for å deklarere den fysiske utførselen, smugler kontanter ut av landet.

Tolletaten forventer at 7-8 milliarder kroner i kontanter vil bli smuglet ut av Norge i 2023, mesteparten av dette vil være i norsk valuta. Tidligere har de vurdert at opp mot en tredjedel av det som smugles ut er penger som stammer fra kriminalitet.[95]

2.3.4. Utbytte fra kriminalitet i utlandet

Det hvitvaskes også utbytte i Norge som kommer fra primærkriminalitet begått i utlandet. Også norske kriminelle aktører bosatt i utlandet vil ha behov for å flytte ulovlige fortjenester til Norge

Trusselen for at utbytte fra kriminalitet i utlandet hvitvaskes i og gjennom Norge vurderes å være MODERAT.

Det er informasjonshull når det gjelder omfang av utbytte fra utlandet som hvitvaskes i og gjennom Norge. I dokumentlekkasjen FinCEN files ble det likevel avdekket at norske bankkonti benyttes til å sluse penger fra kriminalitet gjennom Norge. Tatt i betraktning legitimiteten det gir at midler kommer fra Norge vurderes det som *sannsynlig* at slik hvitvasking vil benyttes i de kommende årene.

2.3.4.1. Hvitvaskingsmodus som benyttes for å hvitvaske utbytte fra utlandet

En fremgangsmåte for utenlandske aktører å legitimere pengestrømmer på er å bruke norske finansinstitusjoner til å gjennomføre transaksjoner. Norge er ansett som et lavrisiko-land og overføringer via norske foretak eller banker gir penger et skinn av legitimitet.

Utenlandske kriminelle aktører benytter Norge som transittland

I Norge er det flere titalls tusen norske bankkontoer som innehas av utenlandske selskaper. Utbytte fra kriminelle handlinger sluses gjerne gjennom bedriftskontoer til norske selskap fordi det er enklere å fordekke og legitimere opphavet av større beløp gjennom bedriftskontoer enn ved bruk av privat konto. Norske bankkontoer som innehas av utenlandske selskaper kan derfor både utgjøre en hvitvaskingstrussel og gjøre Norge til et gjennomstrømmingsland. At Norge i noen grad benyttes som transittland, indikerer også rapporteringen fra de rapporteringspliktige.

95 Deklareringer over 25 000 kroner fra både virksomheter og privatpersoner.

Også privatkontoer benyttes som gjennomstrømningskonti, spesielt ved bedrageri. I dokumentlekkasjen FinCEN files fremkommer det at totalt en milliard norske kroner ble sluset gjennom ulike norske kontoer. Å benytte advokaters klientkonto ved transaksjoner gir høy legitimitet. Transaksjoner og opplysninger om hvem midlene tilhører, er også til dels beskyttet av advokatenes taushetsplikt og hindrer utenforstående innsyn. Advokaters klientkonto er derfor særlig egnet for å skjule og tilsløre midlers opprinnelse og eierskap.

2.4. Aktører som bidrar i hvitvaskingsoperasjoner

2.4.1. Profesjonelle hvitvaskere

I følge Europol har crime-as-a-service fått økt utbredelse blant kriminelle nettverk.[96] Tilbydere av hvitvaskingstjenester har ofte en kritisk rolle i forbindelse med gjennomføringen av flere typer kriminalitet og tar en mindre prosentandel av totalbeløpet som skal hvitvaskes som betaling.

Enkelte profesjonelle hvitvaskere hvitvasker for ulike organiserte kriminelle miljøer, andre hvitvaskere tilbyr hvitvaskingstjenester utelukkende til ett kriminelt miljø. Felles for flere av de profesjonelle hvitvaskerne er at de distanserer seg fra primærkriminalitet og vold som kan tiltrekke seg politiets søkelys.

Selve hvitvaskingen kan foregå gjennom kompliserte selskapsstrukturer, kryptovaluta, investeringer i eiendom eller bruk av skatteparadis. For å gjennomføre hvitvaskingen samarbeider hvitvaskingsaktørene ofte med profesjonelle aktører, som revisorer og advokater. Aktørene har gjerne også tilgang på flere stråpersoner, identiteter og pengemuldyr samt stråselskaper som benyttes som tilslørende ledd i transaksjoner.

Hvitvaskerne kan selv ha opparbeidet seg erfaring innen økonomisk kriminalitet ved at de har drevet næringsvirksomhet og begått kriminalitet som bedrageri, utroskap og underslag. Aktørene kan nå ha roller i foretak som aktivt benyttes i hvitvaskingsoperasjoner. I tillegg kan «sovende» selskaper benyttes til å overføre utbytte til og fra utlandet.

Hawala-agenter kan også fungere som profesjonelle hvitvaskere og har kapasitet til å føre ut store mengder kontanter. Profesjonelle hvitvaskere kan også være behjelpelig med å konvertere utbytte til kostbare gjenstander.

De profesjonelle hvitvaskerne opererer også i det grå og svarte pengemarkedet og tilbyr også ofte lån til svært høye renter til andre kriminelle aktører.

96 Europol, «Serious and organised crime threat assessment (SOCTA)», 2021.

2.4.2. Profesjonelle tilretteleggere

Profesjonelle tilretteleggere omhandler personer som i kraft av sitt yrke og fagkunnskap benyttes til å blant annet tilrettelegge for hvitvasking av utbytte fra kriminalitet. Det er uvisst i hvilket omfang kriminelle benytter profesjonelle tilretteleggere til hvitvasking.

Lekkasjer viser at profesjonelle mellommenn spiller en sentral rolle ved opprettelse av komplekse strukturer som tilslører eierskap.[97] Skatteetaten ser eksempler på at utenlandske profesjonelle rådgivere har gitt investeringsråd til nordmenn om hvordan de skal unngå beskatning.[98]

> En eiendoms-megler er dømt for å gi tre ulike eiendomshandler legitimitet når vedkommende solgte eiendom på vegne av en kriminell aktør.

Politiet har informasjon som indikerer at enkelte advokater stiller klientkonto til disposisjon for hvitvasking. Å benytte advokaters klientkonto ved transaksjoner gir høy legitimitet. Transaksjoner og opplysninger om hvem midlene tilhører, er også til dels beskyttet av advokatenes taushetsplikt og hindrer utenforstående innsyn. Advokaters klientkonto er derfor særlig egnet for å skjule og tilsløre midlers opprinnelse og eierskap.

Informasjon tilsier at et mindre antall virksomheter innen regnskap bistår kriminelle i arbeidet med å kamuflere mislighold i regnskap, oppretter fiktive dokumenter og at de bidrar med kunnskap om sårbarheter slik at dokumentasjon tåler ettersyn av kontrollmyndigheter og hvitvaskingsoperasjonen ikke avdekkes. Det er også mange regnskapsførere uten konsesjon som bistår kriminelle på samme måte.

Oppgjørsadvokater og eiendomsmeglere kan også gi legitimitet ved kriminelles eiendomshandler. I følge FATF er advokater som tilbyr eiendomsmeglingsoppdrag mer risikoutsatt enn eiendomsmeglere. Grunnen er at advokatmeglere i større grad har rene oppgjørsoppdrag med lavere kjennskap til partene i handelen og eiendommen som omsettes.

2.4.3. Pengemuldyr

Pengemuldyr bistår kriminelle ved at de mottar penger på egne konti som er ulovlig ervervet, for deretter å flytte disse videre. Ofte overføres pengene fra muldyrenes bankkonti til norske og utenlandske bankkonti som disponeres av kriminelle aktører, men det er også flere eksempler på at pengemuldyr kjøper gavekort eller dyre klokker. I noen tilfeller overføres pengene til ulike kryptovalutabørser for kjøp av kryptovaluta. Det er også eksempler hvor muldyrsidentiteter benyttes for å opprette konto hos utenlandske betalingstjenester hvor pengene deretter overføres. Overføringer til betalingstjenestene vanskeliggjør sporingen av utbyttet i enda større grad.

97 De Groen & Willem Pieter, «Role of advisors and intermediaries in the schemes revealed in the Panama Papers, European Parliament Economic and Monetary Affairs, Study for the PANA-Committee», 2017.
98 Skatteetaten, «Analysenytt 02/2018», 2018.

Bruk av pengemuldyr i hvitvaskingsoperasjoner er en økende utfordring i mange land inkludert Norge.[99,100] EFE registrerte en økning på hele 740 prosent i antall rapporteringer om mistenkelige transaksjoner fra rapporteringspliktige vedrørende bedragerier og pengemuldyraktivitet mellom 2017-2021.[101] Økningen kan ses i sammenheng med økningen av digital kriminalitet, men også utbytte fra narkotikakriminalitet hvitvaskes på denne måten.[102] Pengemuldyrene får lovnader om høy og rask profitt, og motytelser i form av penger eller formuesgoder.

Det er en økende trend at unge personer rekrutteres til å utføre transaksjoner i bytte mot penger eller dyre formuesgoder. Få av dem forstår alvoret i handlingen og tenker at dette er lettjente penger. De blir kontaktet på internett, e-post eller gjennom sosiale medier av kriminelle aktører, enkelte ganger av jevnaldrende som driver med hacking og phishing-angrep. Den senere tiden har det i Norge foregått blant annet verving av pengemuldyr via Facebook fordekt som en deltidsjobb. Det er også eksempler på ungdommer som forledes til å bidra i et «gambling opplegg» hvor de tjener penger på ulike velkomstbonuser som tilbys av ulike nettspillaktører. Pengemuldyret får instrukser om å opprette konto hos en neobank i eget navn, og pengene de så mottar på konto er fra de nevnte velkomstbonusene.

En annen type pengemuldyr er enslige personer, i mange tilfeller eldre, som forledes til å utføre transaksjoner.[103] Fremgangsmåten fremstår i noen tilfeller å være den samme som ved kjærlighetsbedragerier. Også personer med presset økonomi er særlig sårbare for å bli utnyttet som pengemuldyr.

Det finnes kriminelle nettverk som har tilgang på andres identiteter som gjør det mulig for dem å opprette og disponere bankkonti i deres navn. Mange kriminelle aktører i Norge samarbeider om muldyrsvirksomhet og overfører penger mellom hverandres konti. Kriminelle aktører som sitter fengslet benyttes som pengemuldyr ved at de lar andre kriminelle disponere deres konti mens de er inkapasitert.

99 NCA, «National Strategic Assessment of SOC», 2021.
100 Cifas, «Fraudscape 2021 – Key Findins», 2021.
101 Økokrim v/EFE, «Årsrapport 2021», 2022.
102 Europol, «Money muling», 2021.
103 Europol, «228 arrests and over 3800 money mules identified in global action against money laundering», 2019.

3. Overordnede sårbarheter for hvitvasking

I arbeidet med denne risikovurderingen har vi identifisert noen overordnede sårbarheter ved anti-hvitvaskingsregimet og sårbarheter som går på tvers av modus og rapporteringspliktige sektorer. De trekker vi frem her.

3.1. Asymmetri i ressursfordeling i regimet

Ansvars- og arbeidsbyrden for rapporteringspliktige og tilsynsorganer har økt. Mange av de største rapporteringspliktige aktørene har etablert store avdelinger som arbeider med anti-hvitvaskingsarbeid. I 2021 økte antallet MT-rapporter med 30 prosent sammenlignet med 2020. Tilsvarende økning forventes i 2022. I tillegg øker antallet rapporteringspliktige aktører. Privat sektor har påpekt at det er utfordrende at etatene som skal motta og agere på rapportene ikke er oppbemannet i samme takt.

3.2. Utfordringer med nasjonalt kunnskapsgrunnlag

Informasjonsbehovet knyttet til hvitvasking er fortsatt stort. Det utarbeides interne trussel- og risikoanalyser på ulike nivåer, men de deles i liten grad. EFE mottar eksempelvis tilsynsrapporter fra Finanstilsynet, men det er ingen systematikk i at tilsynsmyndighetene deler strategiske produkter de utarbeider med EFE.

Det er også en sårbarhet at det ikke i tilstrekkelig grad utarbeides statistikk over utbytte i straffesaker. Det er vanskelig å få en god oversikt over utbytte som genereres innenfor de enkelte kriminalitetsområder og hvilke metoder som benyttes til hvitvasking.

Mangelen på kunnskap er en utfordring både i myndighetenes utforming av tiltak og i de rapporteringspliktiges arbeid med å identifisere mistenkelige transaksjoner.

3.3. Deling av informasjon

Det er en sårbarhet at det er vanskelig for rapporteringspliktige å dele informasjon på tvers av rapporteringspliktige sektorer, jf. Hvitvaskingsloven §28. Dette kan medføre utfordringer når tredjepartsaktører som har konsesjon som for eksempel betalingsforetak eller e-pengeforetak benytter infrastrukturen til en aktør som har konsesjon som bank. Videre fremstår det som at det tidvis er uklarhet rundt hvem som er rapporteringspliktig - banken som står for infrastrukturen hvor transaksjonen foregår eller betalingsforetaket som har kundeforholdet.

Det deles også lite informasjon om aktører som kan knyttes til hvitvasking, modus og sårbarheter mellom tilsyn og politiet og omvendt.

Bransjen på sin side etterlyser eksempler på relevante mistenkelige transaksjoner, da offentlige produkter har begrenset nytte i deres arbeid.

3.4. Stor markedsandel for utenlandske aktører

Mange av tjenestetilbyderne i flere av de rapporteringspliktige sektorene som benyttes av norske aktører er ikke rapporteringspliktige til norske myndigheter, men det landet de er registrert i. Det er også en sårbarhet at det er internasjonale aktører innen betalingsformidling og formidling av virtuelle verdier som det i praksis ikke blir ført tilsyn med.

3.5. Manglende transparens om reelle rettighetshavere

Mye av den alvorlige økonomiske kriminaliteten kamufleres ved at lovbryterne gjennomfører transaksjoner og organiserer eierskap på en ikke-transparent måte.[104,105] Et sentralt element i hvitvaskingsregelverket er gjennomføring av kundekontroll ved etablering av kundeforhold. Gjennomføringen av denne kundekontrollen fremstår varierende. Når kunden er et selskap skal identiteten til reelle rettighetshavere også bekreftes, noe som kan være utfordrende for foretak med kompleks eierstruktur, herunder oppkjøpsfond som eier store nasjonale og internasjonale virksomheter. Hvordan bankene foretar denne kontrollen varierer.[106]

I tråd med EUs fjerde hvitvaskingsdirektiv er det planlagt å ferdigstille et nasjonalt register over reelle rettighetshavere. Lovgivningen er vedtatt, men registeret er ikke ferdig per oktober 2022. Foretak skal selv rapportere inn informasjon, og registeret skal bli et hjelpemiddel for rapporteringspliktige i arbeidet med å identifisere reelle rettighetshavere.[107] Regelverket knyttet til reelle rettighetshavere oppfattes imidlertid fremdeles som komplisert, særlig når det gjelder faktisk innflytelse og ikke bare eierandel. Basert på erfaringer fra arbeidsgiver- og arbeidstakerregisteret forventes det at etterlevelsen blir begrenset. Det er også overlatt til rapporteringspliktige å vurdere og verifisere informasjonen, noe som sår tvil om kvalitetssikringen av registeret.

3.6. Nye aktører

Digitalisering og det store antallet nye aktører som springer ut av FinTech industrien, slik som neobanktjenester og vekslingsplattformer for virtuell valuta, fører til nye sårbarheter. Selskaper som befinner seg i en nyetableringsfase har ofte generelt mindre ressurser og kompetanse innen finansregulatorisk juss, samt at de i sin risikovurdering legger for stor vekt på at midlene er kontrollert av foregående rapporteringspliktige i betalingskjeden.

104 Tax Justice Network - Norge, «Skjulte eiere», 2014.
105 FATF, «Concealment of Beneficial Ownership», 2018.
106 Økokrim, «Trusselvurdering 2015–2016», 2016.
107 Regjeringen, «Proposisjon til Stortinget 117 S (2019-2020), Tilleggsbevilgninger og omprioriteringer i statsbudsjettet 2020», 2020.

3.7. Økt bruk av teknologiske systemer

Det forventes at bruken av digitale tjenester vil øke i en digital økonomi.[108] FinTech har sine fordeler, men skaper også nye sårbarheter for hvitvasking.[109] FinTech kan legge til rette for blant annet raske, grensekryssende og anonyme transaksjoner i finansiell sektor. Dersom innovasjon av nye produkter og tjenester ikke i tilstrekkelig grad tar hensyn til krav om kundetiltak og transaksjonsovervåkning, utgjør dette en sårbarhet for hvitvasking. Påliteligheten til elektroniske systemer kan også undergraves av for eksempel datatap som følge av uautorisert tilgang. Kriminelle aktører kan også misbruke digitale systemer ved eksempelvis å bruke falske identiteter.[110] Fiktive a-meldinger og manipulering av inntektsdata har muliggjort både bedrageri og hvitvasking.

3.8. Økt bruk av hyllevare

Stadig flere aktører velger å benytte seg av konsulenttjenester eller «hyllevare» fra ulike advokat- og konsulentfirmaer for å innfri fastsatte krav til registrering. Slik hyllevare kan mangle tilpassede løsninger basert på lokal risiko.

3.9. Svakheter i tilsynsvirksomhet

Tilsynet som føres med de rapporteringspliktiges arbeid på hvitvaskingsområdet skal sikre at kriminelle ikke kan misbruke finansielle tjenester for å sikre utbytte. Det er tre offentlige aktører som fører tilsyn med rapporteringspliktige i Norge – Finanstilsynet, Tilsynsrådet for advokatvirksomhet og Lotteritilsynet.

Jevnt over fremstår tilsynsorganene å være presset fra flere kanter og ikke besitte tilstrekkelige ressurser til å ha en tilsynsaktivitet i tråd med krav og forutsetninger fra for eksempel FATF, EBA og IMF.

FATFs anbefaling om bruk av overtredelsesgebyr ved avdekking av alvorlige mangler i etterlevelsen av hvitvaskingsloven ble ikke vurdert som fullstendig gjennomført ved FATFs oppfølgingsevaluering i 2019.[111] Samme år ble det opprettet en egen seksjon hos Finanstilsynet for anti-hvitvasking og betalingsforetak, som har utstedt overtredelsesgebyr for brudd på hvitvaskingsloven til flere rapporteringspliktige aktører.

Den nye seksjonen har medført økt tilsynsvirksomhet på hvitvaskingsområdet, samt en rekke nye veiledningsdokumenter. En utfordring er derimot at det er behov for mer praktisk og bransjespesifikk veiledning.

108 European Commission, «Supra-National Risk Assessment (SNRA)», 2019.
109 Finanstilsynet, «Fintech og regulatorisk sandkasse», 2020.
110 FATF, «Guidance on Digital Identity», 2020.
111 FATF, «5th Year Follow-Up Assessment Report of Norway», 2019.

Finanstilsynet har også ikke samme mulighet til å kontrollere vandelsattester for agenter, og har sett tilfeller av at kriminelle er forsøkt, eller er blitt, registrert.

Arbeidet til Tilsynsrådet for advokatvirksomhet er fortsatt preget av uklarheter rundt hvitvaskingsloven og rekkevidden av advokaters taushetsplikt. Uklarhetene omfatter rekkevidden av lovens transaksjonsbegrep og rekkevidden av særskilte unntak fra advokatenes rapporteringsplikt. Finansdepartementet har i en uttalelse tidligere lagt til grunn at advokatenes rapporteringsplikt representerer et klart unntak fra advokatens lovbestemte taushetsplikt. Problemstillinger knyttet til forholdet mellom hvitvaskingslovens regler og rekkevidden av advokaters taushetsplikt kan få fornyet aktualitet i forbindelse med innføring av ny lov for advokater *(Prop. 214 L (2020–2021) Lov om advokater og andre som yter rettslig bistand (advokatloven)*).

Tilsynsrådet har besluttet å midlertidig utsette bruken av overtredelsesgebyr etter hvitvaskingsloven § 49 i påvente av Finansdepartementets vurdering av et forslag om å endre bestemmelsens virkeområde. Tilsynsrådet har bedt om at hvitvaskingsloven endres slik at overtredelsesgebyret kan ilegges advokatforetaket som sådan, og ikke bare den enkelte advokat. Utsettelsen er omtalt i Tilsynsrådets årsrapport for 2020.

Hvitvaskingslovens anvendelsesområde ble utvidet til også å omfatte tilbydere av spilltjenester, som medførte at Lotteritilsynet siden 2018 har utvidet sitt tilsynsmandat. De rapporteringspliktige Lotteritilsynet fører tilsyn med har varierende forståelse av hvitvaskingsregelverket og kunnskapsnivå om hvordan deres virksomhet kan bli utnyttet til hvitvasking varierer. Det er mange aktører som trenger veiledning og oppfølging.

3.10. Varierende kvalitet på MT-rapporter

Kvaliteten på informasjon som mottas fra rapporteringspliktige påvirker potensialet for EFEs produkter og den videre oppfølgingen overfor politi eller kontrollmyndigheter. Det er en sårbarhet at det, på tross av en bedring i mange rapporter, fortsatt er varierende kvalitet og generelt svak kvalitet på MT-rapportene fra noen av de rapporteringspliktige. Sårbarheten i MT-rapporteringen ligger fremdeles vel så mye i hva som ikke rapporteres til EFE, som i innholdet i det som faktisk rapporteres.

EFE opplever at informasjons- og veiledningsbehovet fra de rapporteringspliktige er stort og av varierende art. Hovedsakelig dreier det seg om rapporteringspliktige som har behov for veiledning i forbindelse med usikkerhet med hensyn til innholdet av undersøkelses- og rapporteringsplikten.

3.11. For lite informasjon fra MT-rapporter formidles til, og brukes av, politiet

Et grunnleggende element i den samlede innsatsen mot hvitvasking er at finansiell etterretning blir analysert, og at resultatet av disse analysene blir videreformidlet til politiet, som benytter den i politiets øvrige etterretningsproduksjon, etterforskning og inndragning.

På grunn av blant annet ressurssituasjonen, se pkt. 3.1., er det kun noe av informasjonen fra MT-rapporter som formidles videre til politiet. Dette gjør at politiet ikke får utnyttet potensialet i denne informasjonen til å avdekke kriminalitet.

Det registrerte antallet hvitvaskingssaker har vært lavt over tid. I mange tilfeller må komplekse saker avgrenses i etterforskningssporet av hensyn til effektivitet og ressursforhold. Dette kan medføre at etterforskningen ofte velger å fokusere på primærforbrytelsen, og ikke utvides til å involvere hvitvaskingsaktørene. En annen årsak til det lave antallet hvitvaskingssaker kan imidlertid være mangel på kunnskap om finansiell etterforskning og om hvordan ulovlige pengestrømmer og hvitvasking foregår i Norge.

3.12. Grensekryssende etterforskning er ressurskrevende

Hvitvasking er ofte grensekryssende kriminalitet. Effektiv bekjempelse av slik kriminalitet fordrer samarbeid med andre lands myndigheter.

Det har blitt lettere å innhente informasjon etter inngåelse av bistandsavtaler med de fleste land[112] og norske myndigheter har over tid utviklet og engasjert seg aktivt i internasjonalt rettslig og politioperativt samarbeid. Ved etterforskning av grensekryssende hvitvasking erfares det imidlertid at myndighetene i noen land yter lite eller ingen bistand, eller at samarbeidet er omstendelig, med tidkrevende prosesser. Kriminelle som plasserer utbytte fra straffbare handlinger, eller tilslører midlers opprinnelse, søker gjerne nettopp til land preget av strengt hemmelighold og lite samarbeidsvillige myndigheter. Etterforskning av grensekryssende kriminalitet er derfor ressurskrevende og en utfordring for politiet.

112 Norge har inngått skatteavtaler med cirka 100 land. De fleste bilaterale skatteavtalene tar utgangspunkt i føringer fra OECD eller FN.

4. Risiko for hvitvasking i rapporteringspliktige sektorer

Banker, betalingsforetak og agenter for utenlandske betalingsforetak vurderest å ha høyest risiko for å bli benyttet til hvitvasking av utbytte fra kriminalitet.

Betalingsforetak, advokater og regnskapsførere har blitt vurdert å ha høyere risiko enn i forrige NRA. Dette skyldes primært bedre informasjonsgrunnlag. Blant advokater har eksempelvis Tilsynsrådet avdekket alvorlige mangler. Blant betalingsforetakene finner man aktører som flytter store kontantbeløp til høyrisikoland samt mange nye aktører innen FinTech-industrien som har lite kunnskap og erfaring om anti-hvitvasking.

Kreditt- og finansieringsforetak og tilbydere av vekslings- og oppbevaringstjeneste for virtuell valuta nedjusteres på sin side fra BETYDELIG til MODERAT. Førstnevnte kan forklares med at det observeres få tilfeller av hvitvasking via denne sektoren. Når det gjelder vekslingstjenester har disse blitt mer modne siden forrige NRA og industrien domineres av et par store aktører.

Vurdering av risiko for hvitvasking knyttet til rapporteringspliktige sektorer

Rapporteringspliktig sektor	Risiko
Banker (kap. 4.1)	Høy
Betalingsforetak (kap. 4.3)	Høy
Agenter for utenlandske betalingsforetak (kap. 4.2)	Høy
E-pengeforetak (kap. 4.4)	Betydelig
Eiendomsmeglere (kap. 4.9)	Betydelig
Advokater (kap. 4.12)	Betydelig
Regnskapsførere (kap. 4.10)	Betydelig
Verdipapirforetak (kap. 4.7)	Moderat
Revisorer (kap. 4.11)	Moderat
Kreditt og finansieringsforetak (kap. 4.5)	Moderat
Veksling og oppbevaring av virtuelle valuta (kap. 4.6)	Moderat
Forsikringsforetak (kap. 4.8)	Moderat
Innenlandske spillselskap (kap. 4.13)	Lav

4.1. Banker

I 2021 var det 116 banker og 34 filialer av utenlandske banker som hadde tillatelse til å drive banktjenester i Norge. De sendte 11 045 MT-meldinger av totalt 16 513 i 2021.[113]

Norske banker varierer i størrelse, hvilke tjenester og produkter de tilbyr og hvor eksponert de er for hvitvaskingsrisiko. Banker tar imot innskudd og andre tilbakebetalingspliktige midler fra allmennheten, yter kreditt og stiller garantier for egen regning.

Trusler
Bankene er innslagspunktet for det meste av utbytte fra kriminalitet som innplasseres i finanssystemet. Mange andre rapporteringspliktige benytter også banker for å gjennomføre betalinger i sin virksomhet. Både plassering og flytting av midler i banker utgjør en trussel for hvitvasking.

Det er en trussel at norske kontoer benyttes som uttakskontoer og gjennomstrømmingskontoer av både norske og utenlandske aktører. Bruk av pengemuldyr som tilslørende ledd i banktransaksjoner benyttes oftere ved overføring av utbytte både innenlands og utenlands. EFE registrerte en økning på 740 prosent i antall rapporteringer om mistenkelige transaksjoner fra rapporteringspliktige vedrørende pengemuldyraktivitet mellom 2017-2021.

Bransjen rapporterer at nye teknologiske løsninger og flere betalingsaktører gir kriminelle aktører økt mulighet til å hvitvaske. Samtidig er kontanter fremdeles en trussel.

EFE ser en utvikling hvor samme objekt blir innrapportert av flere og mindre banker. Dette kan indikere at kriminelle forsøker å unngå deteksjon ved å ha flere kundeforhold, og gjerne i mindre banker hvor anti-hvitvaskingsarbeidet er antatt å være svakere. Foretak som knyttes til Hawala virksomhet synes også å aktivt opprette bankforbindelser hos mindre lokalbanker, selv om de selv har tilhold i de store byene.

Private banking er en samlebetegnelse for konsepter hvor banken tilbyr pakkeløsninger av spesialtilpassede banktjenester for velstående kunder, slik som brukskonto, lån og investerings- og skatterådgivning. EU vurderer at kombinasjonen av sofistikerte produkter og rådgivningstjenester øker risikoen for misbruk.

Tjenester rettet mot bedriftsmarkedet medfører imidlertid generelt større trussel enn tjenester i personmarkedet, fordi både transaksjoner og forhold knyttet til reell rettighetshaver kan medføre kompleksitet.[114] Gjennom tilsynsvirksomheten ser Finanstilsynet at banker har utfordringer knyttet til kartlegging av reelle rettighetshavere. Det er også en underrapportering av mistenkelige forhold innen bedriftsmarkedet.

113 Økokrim, «Statistikk MT-rapporter», hentet: 28.10.2022.
114 European Commission, «Supra-National Risk Assessment (SNRA)», 2022.

Etter Russlands invasjon av Ukraina har sanksjonsunngåelse vært en av hovedutfordringene for bankene. Bankene ser også en økning i aktører fra land som grenser til Russland som foretar transaksjoner for russiske selskaper og at russiske selskaper oppretter forhold i nærliggende land og gjennomfører transaksjoner derfra.

Sårbarheter

Finanstilsynet opplever at banker generelt har utfordringer med å kartlegge reelle rettighetshavere, noe som ytterligere kompliseres hvis kundene er utenlandske juridiske personer.

Finanstilsynet vurderer også at mangler ved bankenes IT-systemer påvirker etterlevelsen på hvitvaskingsområdet. Mange av systemene som brukes er ikke integrert med hverandre, og informasjon om kunder som bør være oversiktlig og tilgjengelig for relevante ansatte er lagret på ulike steder, og svekker forutsetningene for å se helheten i et kundeforhold og slik sett informere utforming av kundetiltak, risikoklassifisering og undersøkelser og rapportering av mistenkelige forhold. Denne sårbarheten finnes særlig i de større bankene med flere ulike forretningsområder.

En person opprettet kundeforhold i flere banker kort tid etter fylte 18 år. Det ble foretatt innbetalinger fra en rekke ulike privatpersoner, midlene gikk ut igjen etter kort tid, blant annet i form av hyppige og store kontantuttak. Mange av innbetalingene var merket «faktura nr. xx". Vedkommende sine foreldre viste seg å være godt omhandlet for skatteunndragelse og svart arbeid.

Det er også avdekket at flere banker har vesentlig forbedringspotensial for konkretisering og tilpasning av risikovurderinger til lokale forhold.[115]

I følge Finanstilsynet er tjenestetilbud til særlig velstående kunder, såkalt «private banking» og eksempelvis investeringstjenester, sårbare for hvitvasking. Dette fordi det ofte innebærer store beløp. Bransjen har manglende risikoforståelse og det ligger en potensiell sårbarhet i bankenes evne til å vurdere kunders bruk av flere høyrisikoprodukter og -tjenester i sammenheng, eksempelvis der ulike forretningsområder i banken har ansvaret for kundetiltakene for forskjellige produkter. Innen private banking kan det også være utfordrende å fastslå midlenes opprinnelse.

Det er ifølge Finanstilsynet en generell underrapportering av mistenkelige forhold innen bedriftsmarkedet. Dette har trolig sammenheng med at mange bankers risikoklassifisering har mangler som leder til at for få bedrifter blir underlagt forsterkede kundetiltak, og at forsterkede kundetiltak ofte ikke gjennomføres tilstrekkelig eller i det hele tatt, selv for kunder klassifisert med høy risiko.

Produkter og tjenester med internasjonalt tilsnitt er særlig sårbare for hvitvasking, herunder såkalte «trade finance»-produkter og internasjonal betalingsformidling. Tjenestenes sårbarhet må sees i sammenheng med geografisk risiko, produktenes egenskaper og kundegruppe-

115 Finanstilsynet, «Rapport etter dokumentbasert anti-hvitvaskingstilsyn», 2022.

ne som benytter denne type produkter. Tjenester som straks-betaling og «kontant i butikk» anses også som potensielt sårbare for hvitvasking.

Banksektoren selv erfarer at utfordringer knyttet til PSD2 (betalingstjenestedirektivet), fragmenterte kundeforhold som resultat av økt bruk av tredjeparter og kryptovaluta vil være sårbarheter i årene som kommer. Det er også sårbarheter knyttet til nye tekniske løsninger, som for eksempel samtykkebasert lånesøknad.

Risiko
Totalt vurderes risikoen for at banker utnyttes til hvitvasking for å være HØY. De mest vanlige produktene innen personmarkedet og bedriftsmarkedet antas å være mest utsatt for hvitvasking på grunn av antallet kunder med tilgang til tjenesten og at de er enkle å bruke. Enkeltinnskudd av kontanter anses fremdeles å ha høy risiko for hvitvasking, men volumet av transaksjoner er ikke lenger så store.

Mer avanserte bankprodukter i bedriftsmarkedet kan anvendes i tilsløringsfasen hvis kriminelle først får tilgang til dem gjennom for eksempel stråmenn eller selskapsstrukturer. I bedriftsmarkedet er trade finance-produkter til utenlandske virksomheter et produkt med høy risiko. Det skyldes dels mangelfull identifisering av reelle rettighetshavere, grunnet ikke-transparente eierskapsstrukturer og betydelige summer.

Private banking tjenester har flere iboende sårbarheter. Det at man ikke ser produkter og tjenester i sammenheng samt at det i Norge ofte er lavere terskel for å få tilgang til slike tjenester gjør at risikoen forbundet med dette er høy.

4.2. Agenter av utenlandske betalingsforetak

Per 1. januar 2022 var det åtte utenlandske betalingsforetak som har meldt om agentnettverk i Norge, hvor Western Union og Ria er de to største. Det er videre 299 unike agentforhold registrert i Finanstilsynets virksomhetsregister. Agentene er som regel mindre foretak, særlig kiosker, dagligvarebutikker og reisebyrå. Agenter for utenlandske betalingsforetak opererer i Norge på grunnlag av betalingsforetakets konsesjon i sitt hjemland. Agentene i Norge er imidlertid underlagt store deler av det norske hvitvaskingsregelverket.[116]

Utenlandske betalingsforetak og agenter av disse sendte 2 384 MT-meldinger av totalt 16 513 i 2021.[117]

Trusler
Agenter av utenlandske betalingsforetak benyttes ofte for å overføre utbytte av kriminalitet til høyrisikoland. Erfaringer fra straffesaker tilsier at det særlig er utbytte fra kontantgenererende kriminalitet som narkotikaomsetning, hallikvirksomhet og svart arbeid som formidles.

Agenter benyttes også i stor grad i forbindelse med bedrageri hvor pengemuldyr, som gjerne er rekruttert via sosiale medier, typisk vil motta utbytte på egen bankkonto, tar ut dette i kontanter og formidler midler videre til en mottaker i utlandet på instruksjon.

Det har også vært tilfeller av misbruk av kunders identitet for å gjennomføre overføringer, enten som følge av utro tjenere i foretaket, eller ved at foretaket grovt uaktsomt eller forsettlig har tilrettelagt for overføringer ved misbruk av identiteter. I andre tilfeller har det forekommet overføringer av beløp for fiktive personer.

Sårbarheter
Finanstilsynet har ved tilsyn funnet at agenter av utenlandske betalingsforetak har mangelfull etterlevelse av hvitvaskingsregelverket. Foretakenes rutiner er tidvis utdaterte og/eller innholdsmessig svake, og de har ikke gjennomført foretaksspesifikke risikovurderinger. Agentnettverkene baserer seg i stor grad på bruken av transaksjonsovervåkingssystemer for å oppdage mistenkelige transaksjoner. Erfaring viser at treff i systemene sjelden kombineres med manuelle kundetiltak. Agenter av utenlandske betalingsforetak er i all hovedsak mindre foretak, hvor økonomiske insentiver til å gjennomføre mistenkelige transaksjoner og kontrollplikter står i motstrid. Tilsyn viser også at agentene i liten grad er kjent med kravene til gjennomføring av kundetiltak etter hvitvaskingsloven.

Agentene er ofte konsentrert geografisk og en agent kan også være agent for flere nettverk samtidig. Det er derfor enkelt å bruke ulike agenter for å gjøre overføringer av utbytte mindre iøynefallende for nettverket. Det oppstår også en kombinasjonsrisiko fordi kriminelle kan bruke flere nettverk til overføring av utbytte til samme mottaker. Terskelen for å bli registrert som agent er også lavere enn terskelen for å få konsesjon som betalingsforetak. Finanstilsynet

116 Jf. hvitvaskingsforskriften § 1-2.
117 Økokrim, «Statistikk MT-rapporter», hentet: 28.10.2022.

har ikke hjemmel til å kontrollere vandelsattester for agenter, og tilsynet har sett tilfeller av at kriminelle er forsøkt, eller er blitt, registrert som agent.

Agenter av utenlandske foretak har ofte en høy kontantandel i sin omsetning og flere benytter seg av pengetransporter for å frakte kontanter til utlandet.

Risiko
Risikoen knyttet til hvitvasking for agenter av utenlandske betalingsforetak anses som HØY, da en vesentlig andel av transaksjonene betales med kontanter hvor midlenes opprinnelse er ukjent. Midlene sendes i stor grad til sluttdestinasjoner som anses som høyrisikoland.

Sektoren har store sårbarheter knyttet til kundekontroll. Når et foretak er agent for flere betalingsforetak, øker risikoen for sammenblanding av midler, som vil bidra til å gjøre identifisering av midler mer utfordrende.

4.3. Betalingsforetak

Per 1. januar 2022 var det 33 foretak med konsesjon som betalingsforetak, hvor syv hadde begrenset tillatelse. De sendte 171 MT-meldinger av totalt 16 513 i 2021.[118] Per 3. november 2022 var det i tillegg 183 betalingsforetak med grensekryssende virksomhet fra utland til Norge.[119]

Betalingsforetak er en sammensatt gruppe rapporteringspliktige, med svært ulike forretningsmodeller og varierende risiko for hvitvasking. Flere nye betalingsforetak er etablert for å understøtte andre tjenester som for eksempel låneformidling (crowdfunding), betalingstransaksjoner, pengeoverføringer eller å gi forbrukere oversikt over konto og låneforhold. Disse omtales ofte som FinTech-foretak eller neobanker og søker å tilby mer innovative betalingsløsninger.

Tradisjonelle betalingsforetak tilbyr pengeoverføringer til land med svak eller ingen bankinfrastruktur, som gjerne også er å anse som høyrisikoland. Mens denne type betalingsforetak utgjorde en stor andel av betalingsforetakene fram til utgangen av 2018, ser vi nå at denne type aktører utgjør en betydelig mindre andel av betalingsforetak med norsk konsesjon.

Trusler

Truslene knyttet til betalingsforetak varierer ut fra foretakets forretningsmodell. De tradisjonelle betalingsforetakene opererer i stor grad kontantbasert, mens FinTech-foretakene opererer via en app eller nettside. Felles for disse er at truslene primært er knyttet til den grensekryssende virksomheten og betalingsforetak kan i mange tilfeller knyttes til overføring av utbytte fra bedrageri, narkotikavirksomhet og arbeidslivskriminalitet.

Begrenset tillatelse som betalingsforetak innebærer at man ikke kan overføre mer enn fem millioner kroner i snitt per måned. En aktør med slik konsesjon overførte derimot over 150 millioner kroner til utlandet i løpet av 12 måneder.

Enkelte betalingsforetak som kun innehar begrenset tillatelse til pengeoverføring, har også oversteget totalbeløpet de kan overføre. Rapportering til blant annet valutaregisteret og Økokrim, samt etterlevelse av hvitvaskingsregelverket, har tidvis vært svært mangelfull. Eksempelvis fikk en kunde uten registrert arbeidsforhold gjennomført over 400 transaksjoner på til sammen en kvart million kroner over en ett års periode.

Hovedutfordringene med neobanker er hastigheten på internasjonale overføringer[120] og at det er enklere å opprette kundeforhold i en utenlandsk bank. Betalingsforetak som tilbyr tjenester som kobles opp mot andre tekniske løsninger, eller mot andre finansforetak, kan også medføre at ikke all informasjon knyttet til en transaksjon blir synlig for de rapporteringspliktige, men i stedet fragmentert. Denne trusselen antas å øke dersom betalingsforetaket er etablert

118 Økokrim, «Statistikk MT-rapporter», hentet: 28.10.2022.
119 Finanstilsynet, «Virksomhetsregisteret», hentet: 03.11.2022.
120 FATF, «Guidance on Digital Identity», 2020.

i et annet EØS-land og eksempelvis har et annet utenlandsk finansforetak som motpart for transaksjonen.

Sårbarheter
Finanstilsynet vurderer at tradisjonelle betalingsforetak har en rekke sårbarheter som øker risikoen for hvitvasking. Blant disse er høy kontantandel, mangelfull opplæring i pliktene etter hvitvaskingsloven av ansatte og agenter, at foretakene kjenner kundene i begrenset grad, og at foretakene i stor grad består av mindre enheter hvor økonomiske insentiver til å gjennomføre mistenkelige transaksjoner og kontrollplikter står i tydelig motstrid.

Etter at banksystemet har lagt begrensninger på bulktransaksjoner har enkelte betalingsforetak begynt å transportere pengene fysisk til sine samarbeidspartnere. Transporten av pengene blir ofte gjennomført på en uforsvarlig måte, for eksempel ved at en kurer medbringer store beløp på offentlige transportmidler.

Tilsyn i FinTech-foretak har avdekket svakheter i opplæringen. Den generelle opplæringen var for overordnet, mens den særskilte opplæringen av nøkkelpersoner ikke var tilstrekkelig formalisert eller dokumentert.

Risiko
Risikoen for hvitvasking gjennom betalingsforetak vurderes totalt som HØY.

Risikoen for hvitvasking gjennom neobanking og FinTech aktører vurderes som betydelig og potensielt økende ettersom tjenestene blir mer utbredt. På den annen side vil en profesjonalisering og mulig konsolidering av bransjen over tid medføre redusert risiko for hvitvasking.

Det har vært en reduksjon i antallet foretak med konsesjon som betalingsforetak som håndterer store kontantbeløp. Risikoen anses allikevel som høy grunnet store kontantbeløp, overføringer til høyrisikoland samt at etterlevelsen av hvitvaskingsregelverket tidvis er mangelfull.

4.4. E-pengeforetak

Per 1. januar 2022 var det fem foretak med konsesjon som e-pengeforetak i Norge. De sendte 14 MT-meldinger av totalt 16 513 i 2021.[121] Per 3. november 2022 var det i tillegg 122 e-pengeforetak med grensekryssende virksomhet fra utlandet til Norge.[122]

Med elektroniske penger («e-penger») menes en elektronisk lagret pengeverdi, som eksempelvis forhåndsbetalte kort, vouchers og e-lommebok. Forhåndsbetalte kort kan være personlige (identifisert kortholder) eller upersonlige (anonym kortholder). Vouchers minner om forhåndsbetalte kort, men er som regel en kode lagret på et elektronisk medium som har global rekkevidde. En e-lommebok er i all hovedsak en digital e-pengekonto, som består av ett eller flere betalingsinstrumenter, som eksempelvis Apple Pay og Paypal. Flere e-pengeforetak har avtaler med kortselskaper som Visa og Mastercard for å sikre aksept av brukersteder. E-pengeforetak kan også ha distributører som innløser og distribuerer e-penger på vegne av foretaket.

Trusler
Truslene relatert til neobanker er særlig knyttet til hvor enkelt det er å opprette kundeforhold i en utenlandsk bank og gjennomføre raske grensekryssende transaksjoner.[123]

Forhåndsbetalte kort kan kjøpes anonymt med kontanter, men er begrenset til relativt små beløp per kjøp. Det er per i dag ingen norske e-pengeforetak som utsteder upersonlige forhåndsbetalte kort, men slike kort utstedt av utenlandske foretak selges hos norske distributører. Mange kriminelle miljøer benytter seg imidlertid av forhåndsbetalte kort fra utenlandske foretak for å hvitvaske utbytte, spesielt fra bedrageri.

Norske anonyme e-penger som tilegnes med kontanter og uten kundekontroll er begrenset til små beløp. Utenlandske anonyme og forhåndsbetalte kort har en vesentlig høyere beløpsgrense, noe som vil være attraktivt dersom brukeren ønsker å være anonym og skjule pengenes opphav. Mange kriminelle miljøer benytter seg derfor av forhåndsbetalte kort fra utenlandske foretak for å hvitvaske utbytte, spesielt fra bedrageri.

Sårbarheter
Det er gjort unntak fra krav om kundetiltak ved etablering av kundeforhold og bruk av e-penger under visse vilkår i hvitvaskingsforskriften. Dette kan potensielt misbrukes.

Internasjonalt synes det å være en økning i antallet nyetablerte utstedere av e-penger blant en rekke nyetablerte FinTech-selskap som har tatt eller ønsker å ta i bruk e-pengeinstrumenter i sin virksomhet. Dette kombinert med svakheter i opplæring hos flere slike selskap og at disse har lite kunnskap og erfaring om anti-hvitvasking utgjør en sårbarhet.

Risiko
Risikoen for hvitvasking via e-pengeforetak vurderes som BETYDELIG. Dette relateres spesielt til neobanker og upersonlige forhåndsbetalte kort utstedt av utenlandske foretak som selges hos norske distributører.

121 Økokrim, «Statistikk MT-rapporter», hentet: 28.10.2022.
122 Finanstilsynet, «Virksomhetsregisteret», hentet: 03.11.2022.
123 FATF, «Guidance on Digital Identity», 2020.

4.5. Kredittforetak og finansieringsforetak

Per 1. januar 2022 var det 31 foretak med konsesjon som kredittforetak og 28 som finansieringsforetak i Norge. De sendte 252 MT-meldinger av totalt 16 513 i 2021.[124]

Kredittforetak og finansieringsforetak rommer ulike forretningsmodeller og har ulike sårbarheter og risikoer knyttet til hvitvasking.

Kredittforetakene kjennetegnes ved at de kan finansiere sin virksomhet ved å motta andre tilbakebetalingspliktige midler enn innskudd og yte kreditt og stille garantier for egen regning. 23 av de totalt 31 selskapene med kredittforetakskonsesjon er såkalte boligkredittforetak. De er tilknyttet banker, som da har flyttet hele eller deler av sin boliglånsvirksomhet til egne selskaper. Finansforetak driver på sin side blant annet med leasing, factoring, valutavirksomhet og annen finansvirksomhet.

Trusler
Kreditt- og finansieringsforetak kan brukes til å hvitvaske midler gjennom nedbetaling av lån med bruk av utbytte fra straffbare forhold. Dette kan være boliglån, boligkreditt, kredittkortgjeld eller nedbetaling av leasingavtale på bil eller anleggsmaskiner. Indikatorer på hvitvasking via nedbetaling på kredittkort kan være innbetalinger som overstiger innvilget kredittramme eller at innbetalingene gjøres av andre enn kortinnehaver.[125]

For finansieringsforetak er det en trussel knyttet til valutavirksomhet. Finanstilsynet antar at mistenkelige kjøp av utenlandsk valuta i all hovedsak vil være utbytte fra kontantgenererende kriminalitet som narkotikaomsetning, hallikvirksomhet, skatteunndragelser og arbeidslivskriminalitet.

Sårbarheter
Kredittkort er særlig sårbart for å misbrukes til hvitvasking siden det kan benyttes på tvers av landegrenser.

Det foreligger en sårbarhet i at flere boligkredittselskap er datterselskap i et større konsern og at anti-hvitvaskingsarbeidet er utkontraktert. For finansieringsforetak innebærer valutaomsetning ofte at foretakene har kunder som de i liten grad kjenner. Dette forutsetter at foretakene har effektive innledende kundetiltak.

Risiko
Risikoen for hvitvasking knyttet til kredittforetak og finansieringsforetak vurderes som MODERAT. Det er imidlertid store variasjoner i risiko blant finansieringsforetakene siden produktene er av ulik art. Manglende kontroll med at selskapet som har kjøpt varen i realiteten er selskapet som betaler for varen, øker risikoen for hvitvasking. Fire av finansieringsforetakene driver valutavirksomhet hvor risikoen for hvitvasking er høy.

124 Økokrim, «Statistikk MT-rapporter», hentet: 28.10.2022.
125 Finansieringsselskapenes forening, «Innspill til Nasjonal risikovurdering av hvitvasking og terrorfinansiering (NRA) 2022», 2022.

4.6. Tilbydere av vekslings- og oppbevaringstjenester for virtuell valuta

Per 1. januar 2022 var ni foretak registrert som tilbyder av vekslings- og oppbevaringstjeneste for virtuell valuta i Norge. De sendte 135 MT-meldinger av totalt 16 513 i 2021.[126]

Veksling- og oppbevaringstjenester for virtuell valuta har vært underlagt registreringsplikt hos Finanstilsynet siden ny hvitvaskingslov trådte i kraft 15. oktober 2018.[127] Tall fra Skatteetaten viser at stadig flere nordmenn oppgir at de eier kryptovaluta.

Trusler
Den kriminelle bruken av norske vekslingsplattformer for virtuell valuta er i stor grad relatert til betaling for ulovlige varer og tjenester, samt hvitvasking av utbytte fra bedrageri og narkotikaomsetning. Bruken er imidlertid ikke så stort sammenlignet med bruken av utenlandske vekslingsplattformer.

> Politiet fant en person i besittelse av store mengder overgrepsmateriale etter at vedkommende hadde overført Bitcoin til en kryptovalutaadresse som tidligere hadde blitt knyttet til overgrepsmateriale.

Metodene for å hvitvaske via norske vekslingsplattformer er i stor grad like metodene for å hvitvaske via de utenlandske. En modus innebærer at kriminelle mottar en bankoverføring med ulovlig ervervede midler og deretter veksler dette til kryptovaluta, før dette sendes til en kryptovalutaadresse eller utenlandsk kryptovalutatjeneste.

Ved bedrageri blir ofte fornærmede manipulert til å selv gjennomføre vekslingen og sende kryptovaluten fra en norsk vekslingsplattform til en kryptovalutaadresse de kriminelle kontrollerer. Kriminelle kan også ta kontroll over nettbanken til fornærmede og overføre penger derfra til seg selv via veksleren ved å utgi seg for å være fornærmede. Fellesnevneren er at det er vanskelig for veksleren å vite midlenes opphav, og om den som ønsker å veksle er manipulert av kriminelle.

Sårbarheter
Finanstilsynet erfarer at det er sprikende kompetanse hos aktørene som ønsker å tilby veksling- og oppbevaringstjenester for virtuell valuta i Norge. Aktørene er i stor grad teknologidrevet, med hovedvekt av ekspertise innenfor teknologi og utvikling av it-tjenester. Imidlertid har de ofte mindre erfaring med hvitvaskingsregelverket og etterlevelsesarbeid.

Risiko
Norske aktører har en liten andel av det globale markedet for veksling til virtuell valuta. De fleste, inkludert kriminelle, benytter utenlandske aktører som ikke er rapporteringspliktige i Norge. Norske tilbydere av vekslings- og oppbevaringstjenester av virtuell valuta vurderes derfor å ha en MODERAT risiko for hvitvasking.

126 Økokrim, «Statistikk MT-rapporter», hentet: 28.10.2022.
127 Jf. forskrift 14. september 2018 nr. 1324 § 1 – 3.

4.7. Verdipapirforetak, forvaltningsselskap og forvaltere av alternative investeringsfond

Per 1. januar 2022 var det 359 foretak med konsesjon som AIF[128]-forvalter, verdipapirforetak eller forvaltningsselskap for verdipapirfond i Norge. Sektoren sendte 16 MT-meldinger av totalt 16 513 i 2021.[129]

Disse opptrer gjerne som mellommenn i verdipapirmarkedet og tilbyr investeringstjenester knyttet til finansielle instrumenter etter tillatelse fra Finanstilsynet. Foretakene har en svært sentral rolle i annenhåndshandelen med finansielle instrumenter og ved tilrettelegging av emisjoner i førstehåndsmarkedet (corporate-virksomhet). De tilbyr også investeringsrådgivning, analysevirksomhet og garantistillelse for fulltegning av emisjoner, og driver også aktiv forvaltning av investorers portefølje på individuell basis og etter investors fullmakt.

Trusler

Det kan genereres ulovlige midler gjennom verdipapirmarkedet, eksempelvis gjennom markedsmisbruk, innsidehandel eller bedrageri.[130] Midlene hvitvaskes da gjerne også via verdipapirmarkedet.

Verdipapir kan også benyttes til å hvitvaske midler ved at aksjer handles med utbytte fra en straffbar handling. Verdipapirene selges senere, og beløpet overføres til en bankkonto.

Et norsk verdipapirforetak avdekket at dokumentasjonen de ble gitt i forbindelse med en ønsket investering på over 100 millioner kroner, ikke viste reell rettighetshaver, men i stedet en stråperson.

Reell rettighetshaver var en forretningsmann med kjente knytninger til det russiske regime.

Eierskap til aksjer kan også overføres som betaling for ulovlige tjenester. Meglerhus kan bli bedt om å overføre et gitt antall aksjer i et selskap til en ny eier med instruksjon om at oppgjør har funnet sted. Når ny eier selger aksjene, er de hvitvasket. Det kan også være at det omsettes andeler i rene skallselskaper med hensikt om hvitvasking, innsidehandel, markedsmanipulasjon eller annen verdipapirsvindel.

Unoterte aksjer, herunder mange alternative investeringsfond og til en viss grad lavt prisede og mindre likvide noterte verdipapirer, kan være mer attraktive for hvitvasking. Særlig der eierskapet i unoterte aksjer er registrert hos utsteder eller hos foretak som ikke er verdipapirsentral.

Det kan også være mulig å overføre verdipapirer gjennom veldedige stiftelser og andre ideelle organisasjoner i den hensikt å skjule hvitvasking.

128 Alternative investeringsfond.
129 Økokrim, «Statistikk MT-rapporter», hentet: 28.10.2022.
130 FATF, «Guidance for a risk-based approach for the securities sector», 2018.

Sårbarheter

Finanstilsynets tilsyn har avdekket svakheter ved foretakenes etterlevelse av hvitvaskingsregelverket, herunder svakheter ved skriftlige kontroll- og kommunikasjonsrutiner, risikovurderinger, gjennomføring og dokumentasjon av kundekontroll, rutiner for og bevissthet om undersøkelse og rapportering av mistenkelige transaksjoner, samt opplæring.

Finanstilsynet påpeker at risikovurderingene ikke oppdateres ofte nok til at de kan være det tiltenkte verktøyet for de rapporteringspliktige. Likeledes er det avdekket at rutineverket ikke alltid er utarbeidet på bakgrunn av foretakets risikovurderinger slik loven stiller krav om. Det forekommer fortsatt kjøp av pakkeløsninger av risikovurderinger og/eller rutineverk som ikke er utarbeidet på bakgrunn av det aktuelle foretakets virksomhet.

For verdipapirforetak som er en del av et større konsern, eksempelvis en bank, har Finanstilsynet også observert at kundetiltakene kan være basert på opprettelse av kundeforhold i en annen del av konsernet, eksempelvis ved opprettelse av bankkonto, uten at kundetiltakene er tilstrekkelig oppdatert for å reflektere det endrede risikobildet forbundet med at kunden også har en verdipapirkonto.

Risiko

Risikoen for hvitvasking vurderes som MODERAT for AIF-forvaltere, verdipapirforetak eller forvaltningsselskap for verdipapirfond i Norge. Uregulerte markedsplasser er imidlertid eksponert for høyere hvitvaskingsrisiko enn regulerte, særlig der eierskapet i unoterte aksjer er registrert hos utsteder eller hos foretak som ikke er en verdipapirsentral.

4.8. Forsikringsforetak og forsikringsformidlere

Per 1. januar 2022 var det 173 foretak med konsesjon som forsikringsforetak eller forsikringsformidlingsforetak i Norge.[131] Antallet MT-rapporter fra forsikring har økt de siste årene, fra 68 i 2016 til 320 i 2021.[132] Finanstilsynet antar at økningen skyldes økt oppmerksomhet og bedre etterlevelse fra foretakene, snarere enn endringer i kriminalitetsbildet og truslene.

Forsikringsforetak er som regel livsforsikringsforetak, skadeforsikringsforetak eller kredittforsikringsforetak.[133] Forsikringsformidlere, hhv. forsikringsagenter og forsikringsmeglere, er aktører som enten selger forsikringer på vegne av forsikringsselskapene, eller som skal forhandle forsikringsavtaler på vegne av kundene.

Trusler
For å hvitvaske gjennom et forsikringsforetak må kunden innbetale premie til foretaket, og foretaket må foreta utbetaling til kunden eller en tredjemann. Innbetaling av premie med midler som er utbytte fra straffbare handlinger vil være hvitvasking.

Det ble avdekket forsikringsbedrageri med tap på totalt 391,8 millioner kroner i 2021. Det avdekkes flest bedrageri av private skadeforsikringer, men det største tapet beløpsmessig er ved svindel av syke- og uføreprodukter.[134] Utbetaling ved forsikringsbedrageri vil i stor grad være ferdig hvitvasket når det utbetales. Bedrager kan enkelt legitimere denne inntekten ovenfor myndighetene hvis primærkriminaliteten (forsikringsbedrageri) ikke avdekkes.

Forsikringssaker knyttet til luksusgjenstander som klokker og vesker er økende. Forsikringssaker tilknyttet bil, båt, og andre kjøretøy har også vært stigende det siste året. Her rapporteres det gjerne om mindre skadesaker, hvor målet ikke nødvendigvis er å skape stor profitt, men hvitvaske mindre beløp.

Innen livsforsikring kan kunder som rapporterer høy forsikringspremie i forhold til inntekt være en indikator på hvitvasking. Det samme gjelder selskaper som har avvik mellom innmeldte personer til pensjon og reelt antall ansatte, eller selskaper som oppretter foretak med obligatorisk tjenestepensjon og forsikringer for en rekke ansatte mens de ansatte i realiteten ikke arbeider for bedriften. Produkter som er mest egnet 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.

131 Finanstilsynet, «Årsrapport 2021», 2022.
132 Økokrim, «Statistikk MT-rapporter», hentet: 28.10.2022.
133 Skadeforsikring omfattes ikke av EUs hvitvaskingsdirektiv, og det anses dermed ikke som et risikoområde i forhold til hvitvasking i EU-sammenheng. Hvitvaskingsforskriften gir for øvrig unntak fra krav om kundetiltak ved tegning av skadeforsikringspoliser, reiseforsikringspoliser og kredittforsikringspoliser. Hvitvaskingsloven omfatter ikke pensjonskasser.
134 FinansNorge, «Forsikringssvindel i Norge. Svikstatistikk for avdekkede saker i 2021», 2022.

Forsikringsforetak kan også utnyttes til hvitvasking ved bruk av «feilinnbetaling» av forsikringspremie, med etterfølgende tilbakebetaling av midlene, og ved at det tegnes forsikring på objekter som er kjøpt med utbytte fra en straffbar handling. Når det utbetales erstatning for skade på det forsikrede objektet, innebærer forsikringsutbetalingen at midlene hvitvaskes.

Bransjen ser økt profesjonalisering hos aktører som hvitvasker via forsikring, og at eksempelvis regnskapsførere bistår med gjennomføringen.

Sårbarheter
Tilsyn har avdekket mangler ved etterlevelsen av hvitvaskingsregelverket hos forsikringsforetak og forsikringsformidlere. I flere tilfeller har foretakene hatt mangelfulle risikovurderinger og rutiner, og utilstrekkelig opplæring. Rutinene bærer ofte preg av å være lite operasjonelle. Videre observeres det at foretakene ikke skiller mellom rutiner og prosesser for svik og for anti-hvitvasking. Dette underbygges av informasjon fra bransjeorganisasjoner som tilsier at de fleste tilfeller av mistanke om hvitvasking har fremkommet i forbindelse med foretakenes behandling av sviksaker.

At det tidligere har vært lite fokus på forsikringsbransjen som en bransje hvor det foreligger risiko for hvitvasking kan i seg selv gjøre bransjen mer attraktiv for hvitvasking i tiden fremover.

Risiko
Det er samlet sett MODERAT risiko knyttet til hvitvasking i forsikringsbransjen.

Individuelle livsforsikringsavtaler med stort innslag av spare-/investeringselement har en noe høyere risiko for hvitvasking på grunn av muligheten til å innbetale store beløp og fleksibiliteten i forbindelse med uttak. Skadeforsikring har lav risiko.

Når forsikring omsettes via mellomledd, øker risikoen fordi det kan medføre en ansvarspulverisering, hvor forsikringsformidleren kan anta at forsikringsselskapet utfører kundetiltakene og vice versa.

4.9. Eiendomsmeglere

Per 31. desember 2021 var det 537 foretak med konsesjon som eiendomsmeglingsvirksomhet i Norge. Eiendomsmeglere sendte 1 777 MT-meldinger av totalt 16 513 i 2021.[135] EFE melder om en gradvis økt rapportering fra eiendomsmeglere de siste fem årene. Totalt rapporterte eiendomsmeglere syv prosent av det totale antallet MT-rapporter i perioden 2016–2021. Fra 2020 til 2021 opplevde Økokrim en 60 prosent økning i meldinger om mistenkelige transaksjoner fra eiendomsmeglere.

Eiendomsmeglere, eiendomsmeglingsforetak samt rettshjelpere og advokater som driver eiendomsmeglingsvirksomhet omfattes av hvitvaskingsregelverket. I 2021, hadde de i overkant av 250 000 formidlinger til en samlet verdi av 844 milliarder kroner.

Trusler
Eiendomsmarkedet er kapitalintensivt, noe som muliggjør hvitvasking av store beløp i enkelttransaksjoner.[136] Kriminelle aktører investerer i privatboliger og næringsbygg, både i Norge og i utlandet.[137]

I mange tilfeller er de involverte omhandlet med narkotikakriminalitet, svart arbeid, menneskesmugling og bedrageri.

Økokrim erfarer at enkelte eiendomsmeglere benyttes som tilretteleggere for hvitvasking via eiendom ved blant annet urettmessig låneopptak og refinansiering. Ved at eiendomsmeglere legger til rette for en uforholdsmessig høy prisvurdering av boliger kan boligeier få høyere refinansiert boliglån, eventuelt høyere boligkreditt.[138]

Eiendomsmeglere eller advokater som kun bistår med oppgjør har mindre kjennskap til innholdet i avtalen, partene og salgsobjektet. I de tilfellene hvor en enkelt advokat opptrer som oppgjørsmegler kan risikoen være større da oppgjøret ikke må behandles i oppgjørsavdelingen til et meglerkontor. Ved hvitvasking kan det gjøres forsøk på å skjule hvem som er reell rettighetshaver, for eksempel ved bruk av blankoskjøte.

Andre modus kan være at innbetaling til megler kommer fra andre enn kjøper, eller at utbetaling skjer til andre enn selger. Bransjen erfarer også tilfeller hvor det gis bud av en privatperson med forbehold om at de skal utpeke en kjøper/hjemmelshaver.

Antall MT-rapporter som omhandler bruk av blankoskjøte har økt de siste fem år, men utgjør likevel ikke mange i omfang.[139] Klientkontoer kan også benyttes til å motta illegale midler, gjennomføre transaksjoner som legitimerer midlene, eller ved utbetaling til andre enn partene i handelen.

135 Økokrim, «Statistikk MT-rapporter», hentet: 28.10.2022.
136 Finanstilsynet, «Risikovurdering – Hvitvasking og terrorfinansiering», 2019.
137 NTAES, «Situasjonsbeskrivelse – Arbeidslivskriminalitet 2019», 2020.
138 Økokrim, «Temarapport profesjonelle aktører», 2021.
139 EFE, «Temarapport Blanko-skjøter», 2022.

Sårbarheter
De fleste eiendomsmeglingsforetak har nå etablert et anti-hvitvaskingssystem. Advokatmeglerne har i noen grad etablert et anti-hvitvaskingssystem. Finanstilsynet erfarer derimot svakheter i virksomhetenes etterlevelse av hvitvaskingsregelverket, hva gjelder risikovurdering, rutiner, kundetiltak.

Finanstilsynet erfarer at eiendomsmeglingsvirksomheter. Rapporteringspliktige som driver sin virksomhet på mindre steder kan unnlate å gjennomføre nødvendige kundetiltak ut fra personlig kjennskap til partene i handelen. Videre kan det være vanskelig for megler å avdekke om utenlandske selskapsstrukturer benyttes for å tilsløre reelle eiere eller om det benyttes stråmenn for å plassere illegal formue i norsk eiendom.

Enkelte eiendomsmeglingsvirksomheter formidler eiendommer beliggende i utlandet hvor det kan være vanskelig for megler å avdekke om eiendomsverdien er reell, om selskapsstrukturer benyttes for å tilsløre reelle eiere, eller om det benyttes illegale midler dersom oppgjøret ikke går gjennom virksomhetens klientkonto, men i stedet skjer direkte mellom kjøper og selger eller en lokal tilbyder av slike tjenester.

En annen sårbarhet er eiendomsmegleres begrensede mulighet for å ettergå informasjonen som mottas fra kunder, utover det som er oppgitt i egenerklæring.[140] Bransjen opplever at det er sårbarheter knyttet til sammenblanding av private midler og midler knyttet til næringsvirksomhet da det er enkelt å trikse med regnskapstall som sendes til eiendomsmegler. Det samme gjelder gaver og private lån. Det kan være utfordrende å få tilstrekkelig dokumentasjon på hvor midlene som er gitt i gave stammer fra.

Risiko
Totalt sett anses hvitvaskingsrisikoen for eiendomsmeglere å være BETYDELIG.

Risikoen for hvitvasking knyttet til ordinære salgsmeglingsoppdrag for bolig- og fritidseiendom anses å være lavere.

Risikoen er større i tilfeller hvor eiendomsmeglere eller advokater som tilbyr eiendomsmeglingsoppdrag kun bistår med oppgjør, siden oppgjørsmegleren har mangelfull kjennskap til innholdet i avtalen, partene og salgsobjektet. Ved megling av rehabiliteringsprosjekter, nyboligprosjekter samt næringseiendommer er også risikoen vurdert som høyere.

Advokatmeglere vurderes å ha en generelt høyere risiko for hvitvasking og lavere sannsynlighet for å avdekke mistenkelige forhold. De har ofte rene oppgjørsoppdrag – også for boliger under oppføring, der de driver en begrenset virksomhet i et mindre foretak uten rammeverk i form av risikostyring og internkontroll eller innspill fra andre advokater. Og dersom det er etablert et anti-hvitvaskingssystem, er dette ofte ikke innrettet med tanke på eiendomsmeglingsvirksomheten.

140 Dagens Næringsliv, «Skal avdekke hvitvasking og terrorfinansiering, må bruke Google som bakgrunnssjekk», 2021.

4.10. Autoriserte regnskapsførere

Per 1. januar 2022 var det 12 093 autoriserte regnskapsførere og 2 779 regnskapsførerforetak i Norge. Regnskapsførere sendte 104 MT-meldinger av totalt 16 513 i 2021.[141]

Regnskapsførerbransjen omfatter 10-20 større regnskapsførerforetak og –grupperinger, mens hovedtyngden består av mindre foretak med få ansatte, hvorav en rekke av disse driver regnskapsføringsvirksomheten i enkeltpersonforetak. Om lag 90 prosent av regnskapsførerforetakene har færre enn ti ansatte.

Trusler
Autoriserte regnskapsførere kan bli benyttet til å skape legitimitet for sine oppdragsgivere. De kan tilrettelegge for hvitvasking gjennom fiktiv fakturering, skatte- og avgiftsunndragelse, arbeidslivskriminalitet samt tilsløring av reelle rettighetshavere og midlenes opprinnelse.

En annen måte regnskapsførere kan bistå kriminelle på, er ved mangelfull oppfølgning. Et slikt tilfelle ble avdekket under en etterforskning. Her ble det klart at ekstern regnskapsfører ikke var kritisk nok til den dokumentasjon de fikk overlevert, i tillegg til å være kreativ i føring av regnskap. Dette muliggjorde de kriminelle handlingene. I et annet tilfelle forsømte regnskapsfører sitt ansvar for å utarbeide dokumentasjon for flere av transaksjonene i foretaket, samt etablere rutiner for korrekt bokføring.

Det eksisterer regnskapsforetak som utfører regnskapstjenester for virksomheter tilknyttet de organiserte kriminelle miljøene. Deres funksjon knyttes til godkjenning og tilpasning av regnskapspapirer slik at de tåler ettersyn av kontrollmyndigheter

Et regnskapsforetak skal blant annet bistå næringsdrivende med kunnskap om hvordan de kan tappe selskaper og begå kriminalitet knyttet til konkurser.

Det er også regnskapsforetak hvor kundelisten inkluderer en betydelig andel kjente kriminelle aktører innenfor arbeidslivskriminalitet. Flere av regnskapsførerne kan også knyttes til ulike typer kriminalitet, særlig økonomisk, samt at de har felles næringsinteresser som kjente kriminelle aktører. Enkelte regnskapsførere er registrert med eierskap/roller i foretak hvor de benytter eget regnskapsforetak til å utføre regnskapet. Dette reduserer sannsynligheten for at eventuell kriminalitet blir avdekket.

Regnskapsførerforetak tilbyr også rådgivningstjenester, og ved levering av slike tjenester kan foretakene utnyttes som ledd i hvitvasking, særlig i forbindelse med skatte- og selskapsrådgivning.

141 Økokrim, «Statistikk MT-rapporter», hentet: 28.10.2022.

Sårbarheter
Autoriserte regnskapsførere er utsatt for misbruk av kriminelle fordi tjenestene til regnskapsfører skaper tillit til at virksomheten drives i samsvar med lovgivningen. Regnskapsførere som har fullmakt til å belaste oppdragsgivers konto for utføring av betaling, kan bli utnyttet direkte som ledd i hvitvasking.

Finanstilsynets erfaring viser gjennomgående mangelfull kunnskap og oppmerksomhet rundt ulike trusler, særlig kunnskap om hvorfor oppdragsgivere i enkelte bransjer kan utgjøre en trussel. Tilsynserfaringer viser til dels omfattende mangler og fravær av utarbeidelse av virksomhetsinnrettet risikovurdering i tilsynsenhetene, samt gjennomgående mangler i fastsatte rutiner.

Bransjen selv peker på at verifisering av opplysninger, særlig for utenlandske selskaper og statsborgere, er en utfordring. Det nasjonale eierskapsregisteret er heller ikke en tilstrekkelig kilde til å få oversikt over reelle rettighetshavere.

Risiko
Risikoen forbundet med hvitvasking knyttes til regnskapsførerens evne til å forhindre eller avdekke at oppdragsgiver er involvert i hvitvasking vurderes å være BETYDELIG.

Mindre regnskapsførervirksomheter er mer utsatt for involvering i hvitvaskingsoperasjoner sammenlignet med større virksomheter. Større regnskapsvirksomheter har imidlertid større risiko for å bli involvert i grensekryssende hvitvaskingsoperasjoner.

Autoriserte regnskapsførere har oppdragsgivere i alle typer bransjer. Oppdragsgivere som driver i høyrisikobransjer vil medføre en økt risiko for at regnskapsfører blir utnyttet som ledd i hvitvasking. Det krever erfaring og kjennskap til en kunde før man gjenkjenner et transaksjonsmønster som indikerer hvitvasking. Nye kundeoppdrag vil derfor innebære større risiko for å ikke oppdage hvitvasking. Når regnskapsførere opptrer i rollen som rådgiver, vurderes risikoen å være særlig høy.

4.11. Statsautoriserte revisorer

Per 1. januar 2022 var det 8 417 statsautoriserte revisorer, og 458 revisjonsforetak i Norge. Revisorer sendte 41 MT-meldinger av totalt 16 513 i 2021.[142] Revisjonsbransjen er dominert av de fem største revisjonsforetakene som til sammen har en markedsandel på om lag 70 prosent målt etter revisjonshonorar. Det følger av revisorloven § 9-1 at revisor er allmennhetens tillitsperson ved lovfestet revisjon av revisjonspliktiges årsregnskap og revisorbekreftelser.

Trusler
Revisorer gir et foretak legitimitet gjennom sine bekreftelser. Det at et foretak har valgt en statsautorisert revisor kan gjøre det lettere å tilrettelegge eller begå økonomisk kriminalitet. Politiet har mindre informasjon om revisorer som begår lovbrudd enn andre typer profesjonelle tilretteleggere.

Enkelte revisorer antas allikevel å godkjenne regnskap uten særlig kontroll, eller at de mer aktivt bistår kriminelle. Disse revisorene knyttes ofte til foretak som opererer i gråsonen for hva som er lovlig og ulovlig.

Statsautoriserte revisorer har fått tilbakekalt sin godkjenning for blant annet manglende innhenting av dokumentasjon; manglende dokumentasjon av utført revisjon; for ikke å ha forholdt seg nøytralt ved å ha «reparert» regnskapet til klienter; og mangelfull vurdering ved inngåelse av kundeforhold, deriblant oppfølgning av forhold påpekt av tidligere revisor og kontroller iht. hvitvaskingsloven.

Flere revisorer er tilknyttet internasjonale nettverk og har oppdragsgivere med internasjonal tilknytning. Dette øker trusselen for å bli brukt som ledd i hvitvasking. Finanstilsynet har avdekket at revisor har påtatt seg oppdrag for utenlandske aktører uten å gjennomføre tilstrekkelige tiltak for å identifisere reelle rettighetshavere eller personen som handlet på vegne av oppdragsgiver.

Revisjonsselskaper tilbyr også rådgivningstjenester, og det er ofte ved levering av slike tjenester at foretakene utnyttes som ledd i hvitvasking, særlig i forbindelse med skatte- og selskapsrådgivning.

Sårbarheter
Revisorer er utsatt fordi tjenestene skaper tillit til at virksomheten drives i samsvar med lovgivningen. Revisors gjennomgang skjer normalt etter at eventuelle hvitvaskingstransaksjoner har funnet sted. Det kan medføre at det er vanskeligere å avdekke ulovlige forhold.

Finanstilsynet har avdekket til dels omfattende mangler og fravær av utarbeidelse av virksomhetsrettet risikovurdering i tilsynsenhetene. Videre er det avdekket gjennomgående mangler i fastsatte rutiner, som gjør revisorforetakene sårbare for å bli utnyttet som ledd i hvitvasking.

142 Økokrim, «Statistikk MT-rapporter», hentet: 28.10.2022.

Tilsyn har avdekket at revisorer unnlater å utføre enkelte plikter etter hvitvaskingsloven, eksempelvis identifikasjon av politisk eksponerte personer, fordi de selv anser å ha svært god kjennskap til personene som handler på vegne av kunden. I områder der tilfang av oppdragsgivere er begrenset, kan det heller ikke utelukkes at frykten for å miste inntektsgrunnlag kan påvirke etterlevelsen av hvitvaskingsregelverket.

Risiko
Risikoen for hvitvasking vurderes som MODERAT. Liten grad av aktsomhet fra revisor kan imidlertid føre til at tillit etableres til virksomheter som er involvert i hvitvasking.

Mindre revisjonsvirksomheter er generelt mer utsatt for å bli utnyttet til hvitvasking sammenlignet med større virksomheter, som er del av et nettverk og kjennetegnes av høy profesjonalitet. Større revisjonsvirksomheter som inngår i et internasjonalt nettverk er derimot utsatt for å bli involvert i multinasjonale hvitvaskingsoperasjoner.

4.12. Advokater

Per 31. desember 2021 var 8538 personer registrert som praktiserende advokater. Advokater sendte 16 MT-meldinger av totalt 16 513 i 2021.[143]

Advokater er rapporteringspliktige når de på vegne av klient utfører finansielle transaksjoner, bistår ved planlegging eller utføring av transaksjoner for en klient i forbindelse med kjøp og salg av fast eiendom eller virksomhet, forvaltning av en klients penger, verdipapir eller andre aktiva.

Advokater er også rapporteringspliktige ved åpning eller forvaltning av bank- eller verdipapirkonto, fremskaffelse av nødvendig kapital til opprettelse, drift eller ledelse av selskap, og ved opprettelse, drift eller ledelse av selskap, fond eller lignende juridisk person eller formuesmasse, herunder utenlandsk trust eller tilsvarende juridisk arrangement. Advokater er også rapporteringspliktige når de opptrer som bostyrere (med unntak for ved konkurs).[144]

Trusler
Det er advokater som er siktet eller mistenkt for økonomisk kriminalitet. Ofte gjelder det skattesvik, bedrageri, konkurskriminalitet, regnskapskriminalitet, økonomisk utroskap/underslag eller hvitvasking.

Misbruk av klientkonto

En advokat har stilt klientkonto til disposisjon for en rekke personer dømt for alvorlig økonomisk kriminalitet og i praksis fungert som en betalingsformidler, inkludert overføringer av kryptovaluta.

Internasjonale erfaringer viser at fiktive lån settes opp for å muliggjøre finansielle transaksjoner til og fra klienters kontoer, noe som bidrar til legitimering av ulovlige midler. Tilsynsrådet for advokatvirksomhet har også avdekket flere tilfeller hvor advokater bistår med låneformidling og oppgjør uten å kunne dokumentere særlig kunnskap om realiteten bak låneavtalene, og saker hvor advokater brukes for å skjule reelle eierforhold i et foretak. Tilsynsrådet har i den senere tid avdekket flere eksempler på at advokater i realiteten driver ren betalingsformidling via sin klientkonto.[145]

Enkelte advokater har også tilrettelagt for økonomisk kriminalitet ved bruk av klientkonto. Klientkontoen benyttes blant annet til å unndra kreditorgjeld, bedrageri og hvitvasking. Tilsynsrådet erfarer flere tilfeller der det er grunn til å mistenke at advokater bevisst bistår kriminelle aktører/nettverk med å flytte penger som ledd i en hvitvaskingsprosess. Tilsynsrådet har også erfart at advokater ubevisst har bistått kriminelle aktører ved å gjennomføre transaksjoner der advokaten ikke kjenner til eller har vansker med å avklare det underliggende grunnlaget for overføringen. Det samme gjelder der midlene kanaliseres til andre enn partene i det opprinnelige avtaleforholdet.

143 Økokrim, «Statistikk MT-rapporter», hentet: 28.10.2022.
144 Bostyrere i konkurs er ikke omfattet av ny hvitvaskingslov, men er underlagt en rapporteringsplikt etter konkursloven § 122 a.
145 Dette er mulig også i strid med finansforetaksloven § 2-3 første, jf. tredje ledd.

Sårbarheter
Advokatstanden nyter generelt høy tillit i samfunnet, og bruken av advokat til å foreta transaksjoner gir høy legitimitet. Bruk av advokatens klientkonto sørger for anonymitet rundt pengeoverføringer og er derfor spesielt egnet til å hvitvaske midler.

Siste års tilsynsaktivitet har ifølge Tilsynsrådet avdekket en generelt svak risikoforståelse blant advokater når det gjelder egen virksomhet, samt en manglende forståelse av rekkevidden av lovens transaksjonsbegrep.[146] Det avdekkes ofte svakheter i foretakenes virksomhetsinnrettede risikovurdering. Det har også blitt avdekket svikt i etterlevelsen av interne rutiner, blant annet som følge av mangelfulle internkontrollrutiner i de større advokatforetakene. Tilsynsrådet tror mørketallene er store hva gjelder brudd på advokaters rapporteringsplikt etter hvitvaskingsloven da det er avdekket flere transaksjoner som skulle vært rapportert/stanset.

Hvitvaskingsloven er ifølge Tilsynsrådet dårlig tilpasset advokaters virksomhet, noe som i seg selv utgjør en sårbarhet. Tilfeller der penger skifter eier ved at advokaten, etter klientenes ønske, har slått sammen eller overført midler tilhørende ulike klienter på restkontoene i advokatregnskapet skjer uten sporbar fysisk overføring av midler, noe som skjuler transaksjoner. Bruk av advokaters klientkonto er videre ikke underlagt særskilt regulering når det gjelder hvilke typer transaksjoner advokaten kan bistå med.

Det er advokatforetak som trolig kontrolleres av andre enn de personene som formelt står oppført som daglig leder og/eller eier av foretaket. Dette kan være personer uten advokatbevilling og som på ulike måter kan knyttes til et kriminelt miljø. Tilsynsrådet frykter at kriminelle aktører kan få kontroll med virksomheten i advokatforetak ved at advokater av ulike årsaker befinner seg i et avhengighetsforhold til bakmenn som har til hensikt å utnytte advokatvirksomheten til kriminell virksomhet.

Risiko
Risikoen for hvitvasking knyttet til advokater er vurdert å være BETYDELIG.

Risikoen knytter seg særlig til bruk av klientkonto, ettersom opplysninger om transaksjoner via denne kontoen er beskyttet av advokatens lovbestemte taushetsplikt. Risikoen for misbruk øker der advokaten har mangelfull kunnskap om formålet med en transaksjon, for eksempel der advokatens bistand er begrenset til å motta eller videreformidle et oppgjør. Uklarheter vedrørende hvitvaskingslovens rekkevidde leder også til svakere rutiner og økt hvitvaskingsrisiko.

146 Hvitvaskingsloven § 4 annet ledd bokstav c.

4.13. Innenlandske selskaper som tilbyr spilltjenester

I 2020 spilte nordmenn for 51 milliarder kroner i det regulerte spillmarkedet. Alle som arrangerer spill som krever tillatelse etter lotteriloven, pengespilloven eller totalisatorloven er omfattet av hvitvaskingsregelverket. Det er bare Norsk Tipping, Norsk Rikstoto og enkelte av de store landsdekkende lotteriene som kan tilby regulerte pengespill på nett fra Norge. Innenlandske spillselskap sendte 129 MT-meldinger av totalt 16 513 i 2021.[147]

Ny pengespillforskrift forslår å innføre registrert spill på databingo. Forskriften trer i kraft 1.1.23.

Trusler
Sportsspill, spillterminaler, bingo og fysisk kasino i form av spill på skip er særlig utsatt for å bli brukt til hvitvasking på grunn av høy gevinstandel, anonymt spill og bruk av kontanter. Ved sportsspill kan også resultat manipuleres, noe etterforskning av større kampfiksingssaker i Europa har vist. Hvitvasking kan også foregå ved bruk av lånte eller falske identiteter, og falske eller stjålne debetkort, ved registrering av spillekonto som kan benyttes til for eksempel oppbevaring av kriminelt utbytte.[148]

En kjent modus for hvitvasking innen spillmarkedet er at kriminelle benytter ulovlig ervervede midler til å betale for spill. Eventuelle gevinster vil fremstå som legale midler som kan dokumenteres med spillekvittering. Kjøp av spillkvitteringer for å legitimere midlers opphav er også en kjent modus for hvitvasking i bingobransjen. Spillkontoer kan også benyttes for å tilsløre midlenes opprinnelse ved eksempelvis å sette inn kontanter på en spillekonto og deretter overføre beløpet til en bank. Illegalt utbytte kan tilsløres ved å gjennomføre en rekke kontantinnskudd hos flere forskjellige kommisjonærer.

Sårbarheter
Lotteritilsynet har fra tidligere års tilsyn avdekket at aktører ikke har hatt tilstrekkelig gode risikovurderinger for å forebygge og avdekke hvitvasking. Mange risikovurderinger er generiske og tar ikke høyde for geografiske forhold, kunder og andre spesifikke risikoer. Tidligere har Lotteritilsynet erfart at flere kontrollerte bingovirksomheter har hatt ansatte uten tilstrekkelig opplæring. Tilsyn i 2022 har ikke avdekket alvorlige avvik.

Ved bruk av kontanter er det vanskelig å spore midlenes opprinnelse. Enkeltbeløpene er gjerne små, og kommisjonærer har begrenset kompetanse og kapasitet til å avsløre hvitvasking.

Risiko
Risikoen for hvitvasking via innenlandske spillselskaper vurderes som LAV. Risikoen vurderes imidlertid å være høyere for bingobransjen i og med at bingobransjen har en relativt stor kontantomsetning og kontanthåndtering, man kan spille anonymt og spillterminaler kan teoretisk sett manipuleres til å omgå regulatoriske krav. Dette øker risikoen for hvitvasking. Dersom det ikke blir mulig å benytte kontanter til spill på bingo, vil dette redusere risikoen for hvitvasking i bingobransjen.

147 Økokrim, «Statistikk MT-rapporter», hentet: 28.10.2022.
148 Lotteri- og stiftelsestilsynet, «Risikovurdering – Hvitvasking og terrorfinansiering, oktober 2021», 2021.

Del 2

Risikovurdering terrorfinansiering

Terrorvirksomhet er en særlig alvorlig kriminalitetstype, som i vesentlig grad også er avhengig av finansiering og støtte fra sympatisører og bakmenn. Det er derfor avgjørende å adressere finansieringen for å forebygge og bekjempe denne kriminaliteten mest mulig.

Fra: Regjeringens strategi for bekjempelse av hvitvasking, terrorfinansiering og finansiering av spredning av masseødeleggelsesvåpen, juni 2020

1. Oppbygging og metode

1.1. Trussel – Sårbarhet – Risiko

I terrorfinansieringsdelen av NRA 2022 er mye av oppbygningen lik de foregående publikasjonene når det gjelder struktur og inndeling av kapitler.

Det internasjonale og deretter det norske trusselbildet for terrorisme blir først presentert. Deretter blir de ulike truslene og sårbarhetene omtalt.

Sårbarhetene som blir presentert, har vært omtalt i tidligere utgaver av NRA. Det er likevel noen mindre endringer. Noen av sårbarhetene som presenteres, er også sammenfallende med de vi ser innen hvitvasking. For å unngå gjentagelser, vil vi henvise til aktuelle kapitler i den delen av NRA som omhandler hvitvasking.

1.1.1. Sannsynlighetsord

I denne vurderingen bruker vi et sett med standardiserte sannsynlighetsord. Formålet med dette er å skape en mer ensartet beskrivelse av sannsynlighet i vurderingene og derigjennom redusere uklarhet og misforståelser. Begrepene og de tilhørende beskrivelsene av begrepenes betydning er utarbeidet i et samarbeid mellom politiet, PST og Forsvaret.

Nasjonal standard	Beskrivelse	NATO standard
Meget sannsynlig	Det er meget god grunn til å forvente …	Over 90 % sannsynlighet
Sannsynlig	Det er grunn til å forvente …	Mellom 60–90 % sannsynlighet.
Mulig	Det er like sannsynlig som usannsynlig …	Mellom 40–60 % sannsynlighet
Lite sannsynlig	Det er liten grunn til å forvente …	Mellom 10–40 % sannsynlighet.
Svært lite sannsynlig	Det er svært liten grunn til å forvente …	Under 10 % sannsynlighet

1.1.2. Terrortrusselskala

Det er PSTs trusselvurdering som er lagt til grunn når terrortrusselen i Norge omtales. PSTs terrortrusselskala har til hensikt å gi et samlet uttrykk for terrortrusselsituasjonen og graden av alvorlighet i situasjonen. Mens sannsynlighetsordene representerer PSTs vurdering av sannsynlighet for at det vil skje forsøk på en terrorhandling, gir denne skalaen uttrykk for grad av alvorlighet i situasjonen.

Nivå	Begrep	Kort forklaring
5	Ekstraordinær trusselsituasjon	Det er gjennomført en terroraksjon, eller foreligger en uavklart trussel i Norge
4	Høy terrortrussel	Flere aktører har evne og vilje til å gjennomføre terror i Norge
3	Moderat terrortrussel	En eller flere aktører kan ha evne og vilje til å gjennomføre terror i Norge
2	Lav terrortrussel	Enkelte aktører kan ha vilje til å gjennomføre terror, men mangler evne til å gjennomføre planene
1	Ingen kjent terrortrussel	Det pågår ulike typer aktivitet i ekstreme miljøer, men det foreligger ingen kjennskap til aktører som har vilje til å gjennomføre terror i Norge

Det er innhentet informasjon fra PSTs egne trusselvurderinger og relevante rapporter. Informasjon fra Etterretningstjenestens ugraderte trusselvurdering FOKUS 2021 og FOKUS 2022, gir en god oversikt over det internasjonale bildet når det gjelder terrorisme. Informasjon har også kommet fra samarbeid med finansnæringen og deres innspill.

Financial action task force (FATF) publiserer en rekke rapporter hvor terrorfinansiering, og moduser for denne type kriminalitet, er analysert og presentert. Disse rapportene er basert på informasjon og erfaringer fra medlemslandene og internasjonale aktører som FN, Verdensbanken, Europol, INTERPOL mm. Noe av den beskrevne modusen erfarer vi i Norge og noe er mindre relevant for norske forhold.

- Money Laundering and Terrorist Financing Risks Arising from Migrant Smuggling (March 2022)
- Ethnically or Racially Motivated Terrorist Financing (June 2021)
- Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing (September 2020)

Årlig publiserer Europol en ugradert rapport over terrortrusselen i Europa, den såkalte TESAT rapporten, denne rapporten gir også en svært god oversikt over terrorhendelser og avvergede hendelser i Europa, moduser og trender.

1.1.3. Definisjon terrorfinansiering

Terrorfinansiering defineres i straffeloven § 135. For terrorfinansiering straffes den som rettsstridig yter, mottar, sender, fremskaffer eller samler inn penger eller andre formuesgoder med hensikt eller viten om at midlene helt eller delvis skal brukes

a. til å utføre en handling som nevnt i §§ 131, 134 eller §§ 137 til 144,
b. av en person eller gruppe som har til formål å begå handlinger som nevnt i § 131, § 134 eller §§ 137 til 144, når personen eller gruppen har tatt skritt for å realisere formålet med ulovlige midler,

c. av et foretak som noen som nevnt i bokstav b eier eller har kontroll over, eller
d. av et foretak eller en person som handler på vegne av eller på instruks fra noen som nevnt i bokstav b.

På samme måte straffes den som stiller banktjenester eller andre finansielle tjenester til rådighet for personer eller foretak som nevnt i første ledd bokstav b, c eller d. Straffeloven § 136 a rammer også elementer av terrorfinansiering: «(...) den som (...) yter økonomisk eller annen materiell støtte til en terrororganisasjon (...)»

2. Bakgrunn – Terrorfinansiering

I tråd med det trusselbildet som er meddelt i PSTs årlige trusselvurdering vektlegges terrortrusselen som like sannsynlig fra høyreekstremistiske miljøer som fra ekstreme islamistiske miljøer i Norge. Finansieringen til disse miljøene både i Norge og utlandet har for øvrig ulike modus. Risikoen for og konsekvensene av terrorfinansiering er også ulik i de ulike miljøene.

«Terroraktivitet er en særlig alvorlig form for kriminalitet, fordi den truer borgernes grunnleggende trygghet og frihet. Det er derfor av stor betydning med tiltak som rammer både potensielle terrorister og deres støttespillere og aktive sympatisører. Klarer man å forebygge og forhindre tilførselen av midler til terroraktivitet, kan man også hindre terrorangrep». (fra Regjeringens strategi for bekjempelse av hvitvasking, terrorfinansiering og finansiering av spredning av masseødeleggelsesvåpen, juni 2020.)

Finansiell eller materiell støtte til terror er etter norsk rett et selvstendig lovbrudd og defineres som en terrorrelatert handling. Straffebudene rammer ulike former for finansiering og støtte av terrorvirksomhet i og utenfor Norge, som finansiering av konkrete terrorhandlinger og støtte til terrororganisasjoner eller enkeltterrorister.[149]

I følge FN og FATF er organisert kriminalitet en viktig finansieringskilde for terror-, milits- og opprørsgrupper som truer regional og internasjonal sikkerhet. Som eksempel har ISIL finansiert sin terror gjennom ulovlig salg av olje og kulturskatter, kidnapping for løsepenger, skattlegging, smugling og plyndring.

Når det gjelder fremmedkrigere som tidligere reiste fra Norge til ISIL-kontrollerte områder, erfarte PST at de i stor grad har vært selvfinansierte. De har brukt egne midler til å betale reise, klær og utstyr i forkant av utreisen. Egne midler har vært inntekt, enten lønnsinntekt eller sosiale ytelser, salg av egne eiendeler og verdigjenstander samt penger fra familie. Men det har også i tillegg forekommet misbruk av kredittkort, lån og stipender.

149 Se vedlegg – Straffelovens bestemmelser om terrorfinansiering og Lov om tiltak mot hvitvasking og terrorfinansiering mv. (hvitvaskingsloven) med forskrifter.

3. Trusselnivå

Terrortrusselnivået i Norge er MODERAT. Det betyr at en eller flere aktører kan ha evne og vilje til å gjennomføre terror i Norge. Terrortrusselnivået uttrykker den samlede trusselen for all type ideologisk, politisk og religiøst motivert vold i Norge.

Alle trusselvurderinger er beheftet med usikkerhet, og trusselbildet påvirkes av mange faktorer. Uforutsigbarhet og usikkerhet knyttet til potensielle enkelthendelser og mer langsiktige negative utviklingstrekk i Vesten gjør at vi erfarer raske endringer.

Terrorfinansieringstrusselen sees i sammenheng med den generelle terrortrusselen, og det gjelder trussel både fra ekstrem islamisme (IX) og høyreekstremisme (HX). Med det som bakteppe, er det viktig å klargjøre det nåværende trusselbildet.

3.1 Internasjonal terrorisme

Det er personer og løse nettverk av sympatisører, uten sterke bånd til internasjonale terrororganisasjoner, som utgjør terrortrusselen mot Norge og Europa i 2022. Det gjelder både for ekstrem islamisme og høyreekstremisme.

De europeiske nettverkene av militante islamister er mer robuste i dag enn de var før ISILs opprettelse. Nettverkene består av flere personer, med mer erfaring og tettere kontakt på tvers av landegrenser. Det meste av aktiviteten i nettverkene er knyttet til radikalisering av personer eller grupper, finansiering av nettverk og andre typer støttevirksomhet. Hendelser som oppfattes å krenke islam eller muslimer kan gi rask økning i angrepsaktiviteten. ISIL og al-Qaida vil fortsette å oppfordre sine støttespillere i Europa til å gjennomføre angrep, men Norge er ikke av de mest framtredende målene i Vesten.

Både ISIL og AQ fortsetter å prioritere oppbygging av sine filialer i Asia og Afrika heller enn å prioritere angrep mot Vesten. De vil imidlertid prioriterekapasitetsbygging og angrep mot lokale myndigheter og militære mål i områdene de har filialer.

3.1.1. Høyreekstremisme en vedvarende trussel[150]

Etter 2019 har antall høyreekstreme terrorangrep i Vesten gått ned. Det skyldes blant annet fravær av hendelser som tidligere har mobilisert høyreekstreme, som flyktningstrømmer til Europa og større høyreekstreme terrorangrep som inspirerer til etterfølgelse. Like fullt er de høyreekstreme miljøene i Europa fremdeles store og uoversiktlige.

Flere høyreekstreme miljøer har de senere årene blitt mer transnasjonale og styrkes gjennom internasjonal nettverksbygging. Det skyldes blant annet en dreining blant flere høyreekstreme mot idéer som forener på tvers av landegrenser. Miljøene forenes om antiliberalt og antidemokratisk tankegods. Dagsaktuelle saker som innvandring og klimakrisen utnyttes av høyreekstreme miljøer for mobilisering og rekrutering.

150 Etterretningstjenesten, «FOKUS 2022», 2022.

«Anonymitet på digitale plattformer og fravær av hierarkiske organisasjoner bidrar til et uoversiktlig trusselbilde.»

Overlapp mellom høyreekstremisme og antistatlig tankegods vedvarer: Høyreekstreme finner sammen med vaksinemotstandere og antistatlige aktører i konspirasjonsteorier.

«Høyreekstreme miljøer blir mer transnasjonale og forenes om antiliberalt og antidemokratisk tankegods.»

Fra TESAT kan en videre lese at i de europeiske landene er dommene på terror høye. I 2021 var det hele 423 dommer for terrorlovbrudd. Domfellelsesraten for terrorisme er fortsatt høy i Europa, alle høyreekstreme og venstreekstreme tiltaler endte i domfellelse, mens for islamsk ekstremisme var domfellelsesraten 84 prosent.

Av 388 arrestasjoner for terror relaterte lovbrudd, var 14 arrestert for finansiering. I alle sakene var det privatpersoner som finansierte en terrororganisasjon, og ikke en direkte finansiering av et spesifikt terrorangrep.

> Terrorism remains a key threat to the EUs internal security. 15 completed, foiled and failed attacks were recorded in the EU in 2021.The four completed attacks and one left-wing terrorist attack.
>
> Fra: Europols European Union Terrorism situation and Trend report 2022, TESAT

> Lone actors remain the primary perpetrators of terrorist and violent extremist attacks in Europe. However, attack plots involving several actors were also disrupted in 2021. Individuals carrying out attacks alone have been associated mainly with jihadist terrorism and right-wing terrorism and violent extremism. This does not necessarily mean that these individuals act in complete isolation. Online community building often plays a key role, as it connects peers virtually on a global scale. This drives radicalisation and provides access to terrorist propaganda, instructional material and opportunities for procurement of weapons and explosives precursors
>
> Fra: Europols European Union Terrorism situation and Trend report 2022, TESAT

3.2 Terrorfinansiering fra og i Norge[151]

Det overordnede terrortrusselnivået i Norge er MODERAT, og dette gjelder trusselen fra ekstrem islamisme og høyreekstremisme, venstreekstremisme (VX), personer med antistatlige overbevisninger (AX), Klima, miljø og naturvern samt trusselen mot myndighetspersoner.

3.2.1 Ekstrem islamisme – IX

Kontakten mellom norske ekstremister og terrorgrupper i utlandet er en vedvarende bekymring. Selv om ekstreme islamistiske miljøer i Vest-Europa for tiden ikke viser høy aktivitet, er de større enn de var før ISIL ble etablert. Digital og fysisk kontakt mellom personer i Norge og

151 Innholdet i dette kapittelet er i stor grad hentet fra PSTs nasjonale trusselvurdering for 2021 og 2022.

disse miljøene vil fra tid til annen fortsette og bidra til å øke terrorfaren. Løslatelse av terrordømte i Norge og andre europeiske land vil fortsette å påvirke terrortrusselen.

Nedprioritering av kontraterrorarbeidet i Norge og andre europeiske land kan gi ekstremister et større handlingsrom både på fysiske og digitale arenaer.

Jihadistisk propaganda på nett vurderes å forbli en viktig kilde til radikalisering så vel som en mobiliserende faktor for angrep. Selv om ISILs fysiske kalifat er knust, og både ISIL og AQ har opplevd mange tap av ledere de siste årene, produserer begge gruppene stadig ny propaganda og terroroppfordringer spres på nett. Samtidig fortsetter historisk propaganda å være forholdsvis lett tilgjengelig ettersom den stadig republiseres av tilhengere.

Skillet mellom digitale og fysiske nettverk vil ofte være absolutt. I året som kommer forventer vi også at radikalisering fortsatt vil skje i fysiske relasjoner i fengsler, på religiøse arenaer og på skoler.

Der er få tegn på at personer som har vært radikalisert deradikaliseres. Både i Norge og i andre land ser vi at kjente ekstremister overfører tankegodset til sine barn. Ettersom vi aldri har hatt flere ekstremister enn i perioden 2012-2017 og at mange av disse har fått barn, må vi forvente at vi vil se en ny generasjon ekstremister. Tilknytning til et konfliktområde vil også fortsette å bidra til radikalisering hos enkelte.

Finansiering av IX terror

Ettersom ISIL nå kontrollerer et langt mindre geografisk område, er også ISILs inntekter fra tidligere erobrede områder sterkt redusert eller fraværende. Utgifter til våpen og ammunisjon, lønn til medlemmene og økonomisk støtte til familier som har mistet medlemmer i krigen, trening, rekrutering, smugling av mennesker inn og ut av konfliktsoner m.m er vesentlige.

For å skaffe midler til sin drift og aktivitet er både ISIL, Al-Qaeda og deres tilknyttede grupperinger avhengig av økonomisk støtte fra sitt internasjonale nettverk av meningsfeller, og fra familier til fremmedkrigerne.

Fortsatt er det betalingsforetak og uregistrerte betalingsforetak (som hawalaaktører) som viser seg å være de viktigste aktørene for transaksjonene. Men bruken av virtuell valuta er i sterk vekst. Dette blir også understreket i FATFs analyser.

FATF ser også en sammenheng mellom smugling av immigranter og terrorfinansiering. Det er store summer som går til kriminelle nettverk som driver med menneskesmugling. Man ser at disse pengene i hovedsak blir hvitvasket, men en kan heller

Eksempel på norsk dom i terrorfinansieringssak:

Tilbake til 2018 underrettet Enheten for finansiell etterretning ved Økokrim PST om mistenkelige økonomiske transaksjoner tilknyttet en mann i 40 årene. PST startet etterforsking med tiltale om terrorfinansiering etter straffeloven § 135 første ledd bokstav b og andre ledd.

ikke utelukke at noe går til terrorfinansiering. (FATF rapport «Money laundering and Terrorist Financing Risks arising from imigrant smuggling, Mars 2022)

Det er stadig forespurt og aktuelt med såkalte indikatorlister for terrorfinansiering. Lister med indikatorer blir delt med kontrolletater og finansnæringen. Disse indikatorlistene har blitt hensyntatt i bankenes risikovurderinger og screeningprogram.

Indikatorene som tidligere ble delt med blant annet finansnæringen, knyttet seg ofte til den såkalte fremmedkrigersituasjonen. Flere dro til Syria for å krige for den Islamske stat, ISIL. Disse fremmedkrigerne hadde en del felles kjennetegn, både i deres radikaliseringsprosess og i deres forberedelser før avreise. Innkjøp av relevant utstyr og klær, avslutning av ulike abonnement, store kontantuttak, maksimering av uttak og handel på kredittkort m.m. var indikatorer som kunne varsle en planlagt reise. Selv om fremmedkrigerproblematikken er mindre gjeldende i dag, kan dette endre seg.

Indikatorer har fortsatt aktualitet i dag, men de kan være mer differensiert. I dagens situasjon er det færre fellesnevnere når det gjelder støttevirksomhet. Finansiering av terror er i hovedsak enkeltindivider som utfører, uten et fast mønster eller med klare indikatorer. Dette kompliserer arbeidet for både politi, kontrolletater og finansnæringen.

Samtidig som PST startet etterforskingen av 40 åringen, ble et nettverk i Tyskland etterforsket av tysk politi for terrorfinansiering av ISIL i Syria. Etterforskingen i Norge og Tyskland avdekket et internasjonalt nettverk som finansierte ISIL. PST og tysk politi samarbeidet om den videre etterforskingen. Finsk politi ble også involvert, og landene koordinerte en felles politiaksjon sommeren 2019.

Etterforskingen av 40 åringen, ledet politiet til en 30 åring som hadde bistått med pengeoverføringene. Han ble pågrepet på hjemstedet og ved ransaking hos han fant politiet 391 000 kroner under madrassen, samt kladdebøker med noe som så ut som et hawala regnskap. Videre etterforsking viste at han ved tre anledninger hadde overført til sammen 465 000 kroner til en kjent ISIL-kriger i Syria, på vegne av 40-åringen.

40 åringen ble dømt til 5 års fengsel for å ha overført til sammen 465 000 kroner fordelt på flere transaksjoner til en fremmedkriger i ISIL. Den andre tiltalte, mannen i 30-årene, ble frifunnet for terrorfinansiering, men domfelt for brudd på finansieringsforetaksloven på grunn av ulovlig hawala-virksomhet. Han ble dømt til å betale en bot pålydende 25 000 kroner, samt å tåle inndragning av 391 000 kroner.

Dommen fra Borgarting lagmannsrett som ble avsagt i juni 2022, er nå rettskraftig, da anken ble avvist av Høyesterett i oktober 2022.

3.2.3 Høyreekstremisme – HX

PST vurderer det som fortsatt mulig at høyreekstreme vil prøve å gjennomføre terrorangrep i Norge i 2022. Mange høyreekstremister vil fremdeles forenes om konspirasjonsteorier som hevder at den hvite rase utsettes for et folkemord, og at den vestlige kulturen vil forsvinne. Dette begrunnes blant annet med innvandring fra ikke-vestlige land og lave fødselstall blant hvite.

Høyreekstremister fremstiller dette som en eksistensiell trussel.

Det er i første rekke akselerasjonister (se tekstboks) som vurderes å utgjøre den største trusselen blant høyreekstremistene. Vi forventer fortsatt tilfeller der høyreekstremister i Norge vil bli radikalisert av akselerasjonistisk tankegods. Norske myndigheter og politikere vil fortsatt bli anklaget for landssvik ved at de angivelig legger til rette for det påståtte hvite folkemordet, og er derfor sentrale i høyreekstremisters fiendebilde.

Høyreekstremister vil fortsette å bruke dagsaktuelle saker, som koronapandemien og klimasaken, for å bekrefte og videreføre sine overbevisninger.

Digitale plattformer vil fremdeles være de viktigste arenaene for radikalisering til høyreekstremisme. De mest sentrale arenaene er digitale applikasjoner der høyreekstremister kan kontakte hverandre, ytre ekstreme synspunkter og dele høyreekstremt materiale.

Radikalisering vil skje både i norske, nordiske og transnasjonale digitale nettverk der det pågår diskusjoner rundt ideologi, fiendebilder og våpen. Flere av de transnasjonale nettverkene er mer voldsforherligende og inneholder mye terroroppfordrende propaganda. Deltakelse i slike høyreekstreme nettverk kan bidra til at enkelte utvikler et ønske om å begå volds- eller terrorhandlinger.

Særtrekk ved Finansiering av HX terror
I juni 2021 publiserte FATF en rapport «Ethnically or racially Motivated Terrorism Financing», rapporten tar for seg finansiering av høyre radikale miljø, og Norge er et av landene som har kommet med innspill her.

Akselerasjonisme er en retning innen høyreekstremisme. Sentralt er ideen om at en rasekrig er nært forestående, og at det haster med å fremskynde en samfunnskollaps mens hvite fremdeles er i demografisk flertall i Vesten, for å redde den hvite rase. Akselerasjonister fremhever terror som et viktig verktøy for å destabilisere samfunnet og igangsette rasekrigen. Gjerningspersoner i flere utførte og avvergede høyreekstreme terrorhandlinger i Vesten de siste årene har vært inspirert av dette tankegodset.

Ytre høyre er en samlebetegnelse for høyreradikale og høyreekstreme ideologier og har to sentrale kjennetegn: For det første ideen om at stat og folk skal være en enhet. Grupper som ikke regnes å tilhøre denne enheten, anses som en trussel. For de andre er ytre høyre enten motstandere av demokratiet som styreform, eller så utfordrer de sentrale liberale verdier som demokratiet bygger på. Det som skiller høyreekstremister fra høyre-radikale, er deres syn på demokratiet og deres aksept for vold for å skape politisk endring. Høyreekstremister ønsker å avvikle demokratiet og aksepterer vold for å nå politiske mål. Dette gjelder imidlertid ikke for de høyreradikale. Både høyre-ekstremister og høyreradikale er imidlertid ofte skeptiske til myndighetene, som anses som korrupte.

Rapporten konkluderer blant annet med at høyreekstreme terrorangrep i hovedsak er utført av selvfinansierte enkeltpersoner, og at høyreekstreme grupperinger benytter seg av mange ulike finansieringsmetoder.

Donasjoner til høyreekstreme miljø i utlandet er i stor grad samlet inn via crowdfunding plattformer. Mange som sympatiserer med høyreekstremisme er aktive på sosiale medier, forum, gaming chatterom osv. De har stor tillit til plattformer som samler inn penger, og motivatorene i de høyreekstreme miljøene når da lett ut til en stor tilhengerskare. Betaling til disse nettbaserte plattformene kan gjøres i virtuell valuta, og avsender forbli lettere anonym. Private donasjoner er også utbredt i de høyreekstreme miljøene. Inntekter fra konserter, festivaler fight-clubs og andre arrangement er også store inntektskilder, spesielt i Mellom-Europa. Da covid-restriksjonene forbød store ansamlinger, falt disse inntektene. I enkelte høyre ekstreme miljø ser en også en forbindelse og samarbeid med organiserte kriminelle.

> Limitations in concerts and events in the COVID-19 era have driven right-wing extremist groups to seek alternative methods of funding for their activities. An increased number of online campaigns on social media, forums, gaming chat rooms and other internet platforms, have been organised in support of the right-wing extremist scene. These activities not only provide funds, but also help promote their ideology, create opportunities for future recruitment and build relationships between different right wing extremist adherents. The monetising of online profiles through the right-wing extremist scene has also been observed. Right-wing extremists also show an interest in cryptocurrencies.
>
> Fra: Europol, European Terrorism Situation and trend report 2022 - TESAT

3.2.4 Venstreekstremisme -VX

Det vurderes som **svært lite sannsynlig** at venstreekstremister vil forsøke å gjennomføre terrorhandlinger i 2022. Venstreekstremisme i Norge vil forbli et marginalt fenomen med et fåtall aktive grupper. Venstreekstremistenes ideologiske overbevisning er forankret i voldsforherligende varianter av kommunisme, anarkisme og anti-fascisme. Vi forventer fortsatt et lite omfang av nyrekruttering til de gruppene som eksisterer i Norge. Bekjempelse av høyreekstremisme vil fortsatt være den samlende kampsaken for venstreekstremister. Norske venstre ekstremister har en bred tolkning av fenomenet høyreekstremisme. Fiendebildet omfatter derfor alt fra organiserte høyreekstreme miljøer til høyreradikale grupper og enkeltpersoner. Enkelte venstreekstremister vil fortsette å gjennomføre politisk motiverte voldshandlinger samt konfrontere og offentlig sjikanere personer de anser som høyreekstreme. Dette bidrar til at polariseringen mellom miljøene videreføres. For flere venstreekstremister inngår også politiet i fiendebildet, men primært i tilfeller der politiet er til stede i det offentlige rom for å verne om ytringsfriheten, som under demonstrasjoner.

3.2.5 Trusselen fra personer med antistatlige overbevisninger - AX

Det vurderes som **lite sannsynlig** at personer med antistatlige overbevisninger vil forsøke å utføre terrorhandlinger i Norge. Det er en generell høy tillit til myndighetene i Norge, noe som gjør at antistatlig tankegods har et begrenset potensial for vekst sammenlignet med flere andre land. Vi har imidlertid registrert økt aktivitet blant personer med antistatlige overbevisninger de siste årene, også i Norge.

4. Sårbarheter – Risiko

Å avdekke og hindre transaksjoner som skal støtte terrorisme, er en stor utfordring. Ofte er slike transaksjoner fordekt og svært vanskelig å spore, særlig når det benyttes ikke-rapporteringspliktige aktører. Da forblir ofte avsender og/eller mottaker skjult.

I den ugraderte Nasjonale trusselvurderingen fra PST i 2021 kunne en lese:

«Norske ekstreme islamister vil imidlertid fortsatt støtte globale terror-organisasjoner, samt ekstremister i regionale konflikter de selv har en tilknytning til. Det foregår kontinuerlig innsamlingsaksjoner på ulike nettfora til støtte for ekstremister og terrorgrupper. Noe av aktiviteten skjer under dekke av å være ulike former for nødhjelp. I tillegg er det sannsynlig at det vil foregå innsamlingsaksjoner i enkelte moskeer og muslimske kultursentre, til støtte for ekstreme grupper. Slik innsamling kanaliseres ut av landet gjennom banker eller hawala».

Begrepet hawala kan være noe uklart i denne sammenhengen. Det er et system for pengeoverføring og betalinger over landegrenser og et alternativ til bankvesenet. Det er basert på tillit og islamske tradisjoner. I denne sammenhengen kan hawala forklares at penger er overført via uregistrerte betalingsformidlere, noe som fordekker opprinnelige sender og mottaker. Noen av disse hawala-aktørene kan være registrert som en frivillig organisasjon, og de misbruker dermed NPO ordningen. Hawala-aktører kan igjen benytte seg av registrert betalingsformidlere og bankvesen.

4.1 Banker

Rapporteringspliktige foretak synes å ha enkelte utfordringer knyttet til avdekking og bekjempelse av terrorfinansiering. En utfordring synes å være tilpassing av risikoforståelse og tiltak når risikobildet endres, eksempelvis utvikling av nye scenarier for å fange opp terrorfinansiering gjennom høyreekstreme grupperinger.

Finanstilsynet erfarer at kunnskapen og bevisstheten hos bankene om terrorfinansiering er varierende. Faktorer som bankenes størrelse, antall kunder, sammensetningen av kundemasse, kompleksitet i tjeneste- og produkttilbud samt internasjonal eksponering påvirker risikoen for misbruk til terrorfinansieringsformål.

I bankenes risikovurdering på hvitvaskingsområdet er det et krav at terrorfinansiering vurderes selvstendig, og at det foreligger gode rutiner for håndtering av dette. Finanstilsynet erfarer at enkelte mindre og mellomstore banker ikke i tilstrekkelig grad inntar risikoen for terrorfinansiering i sin etterlevelse av hvitvaskingsloven. Finanstilsynet har også observert at større banker etterlever kravet om at terrorfinansiering risikovurderes, men at etterlevelsen utover dette varierer. Når bankene har liten bevissthet om problematikken på overordnet plan, ei heller ingen terrorfinansieringsscenarier i transaksjonsovervåkningssystemene og ingen rutiner for å håndtere dette, så er forutsetningene for å avdekke konkrete terrorfinansieringsforhold svake.

Risikoen er at transaksjoner som skulle vært stoppet basert på sanksjonsregimet blir gjennomført og går til kriminalitet.

Antall meldinger fra de rapporteringspliktige i henhold til hvitvaskingsloven om mistenkelige transaksjoner med mistanke om terrorfinansiering har de siste årene vært ganske stabilt, med en liten nedgang i antallet de siste par årene. Dette kan skyldes at krigen i Syria og Irak har stilnet, og at fokuset på finansiering av fremmedkrigere ikke er så stort.

Av det høye antallet av mistenkelige transaksjoner (MT) som blir meldt til EFE, er om lag 3 prosent huket av for mistanke om terrorfinansiering. I 2019 var det 366 såkalte MT rapporter, i 2020 409 rapporter og i 2021 299 rapporter. Det er bankene som melder inn da fleste mistenkelige transaksjonene, hele 68 prosent.[152]

Trusselbildet er stadig i endring, og det er derfor viktig at finansinstitusjonene har oppdaterte indikatorlister på terrorfinansiering i sitt overvåkingssystem for transaksjoner. Dialog og kunnskapsdeling med politiet er derfor svært viktig for å oppnå god etterlevelse.

En av flere indikatorer på en mistenkelig transaksjon knyttet til terrorfinansiering kan være at pengene går til konfliktområder. Slik trusselbildet ser ut nå, med mange hjemvendte fremmedkrigere i Europa og fremmedkrigere som er ferdige med soning og er ute i samfunnet igjen, er det viktig å ikke ha for stor oppmerksomhet rettet mot destinasjonen pengene går til. Penger til terrorisme trenger ikke kun å gå til konfliktområder. Det kan bli for snevert, og dermed kan en gå glipp av en slik transaksjon som burde vært meldt. Som tidligere påpekt har ISIL og AQ etablert seg med celler i mange land, og med sympatisører i enda flere land.

Også de høyreekstreme miljøene har et internasjonalt nettverk, med grensekryssende transaksjoner. Det kan være utfordrende å avdekke disse transaksjonene, for det er ikke åpenbart at pengene går til kjente konfliktområder.

4.2 Sanksjonsforskrifter

De rapporteringspliktige har krav og rutiner for å sikre at de internasjonale vedtatte sanksjons- og tiltaksforskriftene følges. Banker kjøper inn systemer for screening mot de ulike sanksjonslistene. Finanstilsynets erfaring er at systemene som benyttes genererer en stor grad av feiltreff, noe som øker risikoen for at bankene ikke reagerer på adekvat måte når treffene er korrekte, og at undersøkelser for å avkrefte feiltreffene medfører unødvendig ressursbruk.

En annen sårbarhet knyttet til terrorfinansieringstrusselen og sanksjonslister er at sanksjonsscreening kun fanger opp kjente individer og grupper, mens risikoen for terrorfinansiering ofte kan knyttes til personer som ikke er fanget opp av sanksjonsregimet. Det er derfor av stor betydning for bekjempelsen av terrorfinansiering at de rapporteringspliktige har flere systemer for å avdekke terrorfinansiering.

152 EFE, «Trendrapport 2021», 2022.

4.3 Betalingsforetak med konsesjon og agenter for EØS-registrerte foretak

De større betalingsforetakene har sanntidsregler og annen transaksjonsovervåkning som skal avdekke terrorfinansiering og finansiering av fremmedkrigere. Det gjøres også noe overvåkning av åpne kilder. Flere av betalingsforetakene spesialiserer seg på overføringer til høyrisikoland som gjerne også er konfliktsoner med liten eller ingen bankinfrastruktur.

Finanstilsynet har tidligere meddelt at de har den oppfatning at både de norske betalingsforetakene og agentene for de større utenlandske betalingsoverføringsnettverkenes gjennomføring av kundetiltak ikke etterlever hvitvaskingslovens krav.

De fleste agenter av EØS-registrerte betalingsforetak har agentvirksomheten som bigeskjeft. De er avhengige av opplæring og oppfølging fra selskapene de representerer for å følge opp de norske kravene. Det er også en sårbarhet at agentene ikke har forutsetninger til å kjenne kundene når deres gjennomføring av transaksjoner i stor grad skjer på drop in-basis.

Kombinasjonen av mangelfulle kundetiltak og pengetransaksjoner til konfliktområder gjør risikoen for at slike tjenester blir brukt til terrorfinansiering høy.

Enkelte norske og utenlandske betalingsforetak benytter seg av pengetransport for å frakte kontanter ut av landet. Bakgrunnen for dette er at enkelte betalingsagenter har vanskeligheter med å opprette konto i norske banker for videreføring av pengene.

Når norske og utenlandske betalingsforetak frakter kontanter ut av Norge via pengetransportører, kan det innebære at myndighetenes kontroll med pengenes opprinnelse og mottaker minsker. Det er også risiko for at summen som faktisk føres ut av landet er større enn den som blir oppgitt til fraktselskapet, fordi det er mangelfull kontroll av summene som blir oppgitt.

4.4 Uregistrerte betalingsforetak

Det er en sårbarhet at uregistrerte betalingsforetak sender penger til og fra Norge, fordi disse aktørene representerer en særlig stor risiko for finansiering av hvitvasking og terror. Hawala aktører sorterer inn under denne gruppen.

Det forekommer at organisasjoner registrerer seg som en frivillig organisasjon (NPO), men i hovedsak driver med betalingsformidling. De misbruker da NPO-ordningens integritet og driver forretningsvirksomhet. Organisasjonene har da hverken konsesjon fra Finanstilsynet eller agentavtale med et EØS-registrert betalingsforetak, og de rapporterer ikke transaksjonene til Valutaregisteret eller sender meldinger om mistenkelige transaksjoner til Enheten for finansiell etterretning. Det gjør at den opprinnelige avsenderen og den endelige mottakeren forblir ukjent for myndighetene, og det igjen kan være en metode for å hvitvaske penger eller finansiere terrorisme.

En ser også at enkeltpersoner opererer som betalingsformidlere. I begge tilfeller trenger aktørene en bankkonto, og det blir derfor viktig at bankene kjenner sine kunder godt og har varslingssystemer som fanger opp aktørens ulovlige aktivitet. Se omtalte dom på terrorfinansiering.

Se Økokrims omtale under «Hawala og ulovlig utførsel av kontanter».

4.5 Pengeinnsamling og crowdfunding

Pengeinnsamling i Norge er ikke lovregulert, og alle kan drive pengeinnsamling, enten som organisasjon eller privatperson. Det er ingen krav til registrering eller underretting. Ved for eksempel naturkatastrofer og akutte humanitære kriser - hvor mange ønsker å gi penger og bidra til hjelp - kan useriøse aktører se muligheter til underslag eller finansiering av terrorisme. Dette er en sårbarhet og krever givers aktsomhet.

Innsamling av penger via sosiale medier kan i enkelte tilfeller tilsløre den opprinnelige giveren. Flere kjente utenlandske og norske ekstremistiske organisasjoner og miljøer ber om finansiell støtte på sosiale medier. Ofte blir det oppgitt ønske om innbetalinger via ulike, gjerne krypterte, betalingsplattformer.

Crowdfunding, også kalt folkefinansiering, samler bidrag fra ofte et stort antall mennesker. Det er gjerne mindre beløp til støtte for ideer og prosjekter. Penger blir overført via nettet til ulike plattformer. Kontrollen med slike plattformer kan være utfordrende spesielt dersom crowdfunding plattformen administreres fra ett land, men pengene blir overført videre til andre land. Den digitale fundraising teknologien er komplisert og kan bli oversett av kontrolletater. Overførslene til plattformene kan også skje med virtuell valuta, noe som vanskeliggjør kontrollen ytterligere.

I februar 2021 ble en person dømt til to års fengsel i Østerrike for å ha finansiert og vært medlem i en terror- og kriminell organisasjon. Den domfelt hadde samlet inn penger via Facebook til en IS kriger i Syria, samt spredd IS propaganda og oppfordret personer til å bli med i terrororganisasjonen.

4.6 Virtuell valuta

Fortsatt er internett en viktig arena for spredning av terroroppfordrende propaganda. Dette vil bidra til radikalisering og terror-planlegging, som også har innvirkning på finansiering.

Med dagens digitale løsninger og globale samhandling over internett er det viktig og utfordrende å holde oversikt og kontroll over selskaper som tilbyr finansielle tjenester i Norge. Ulike nyere betalingstjenester etterlater seg elektroniske spor som det kreves kunnskap om og analyseverktøy for å avdekke.

Vekslere og oppbevaringstjenester av virtuell valuta er underlagt hvitvaskingsregelverket. Det stilles dermed krav til tilbyderne om økt kunnskap om terrorfinansieringstrusler ved bruk av tjenestene. Ettersom bransjen er relativt ny, og tidligere uregulert, er det svært sprikende kompetanse hos aktørene. Det vil trolig ta noe tid før bransjen er tilstrekkelig moden for å ha de rette mekanismene på plass for å bekjempe hvitvasking og terrorfinansiering på en tilstrekkelig måte.

FATF rapporterer at den største endringen innen terrorfinansiering den siste tiden er en stadig økende bruk av virtuell valuta. Virtuell valuta blir mer brukt som en betalingskanal for fundraising aktiviteter, og samtidig blir virtuell valuta misbrukt til å overføre penger til terrorisme. Det er påvist at f.eks ISIL med sine regionale kontakter både i Asia og Afrika har delt kunnskap om hvordan med sine støttespillere på hvordan de kan bruke virtuell valuta for å skjule transaksjoner.

Virtuell valuta er et digitalt og grensekryssende produkt, der tjenestetilbyderen ikke har en tydelig tilknytning til ett enkelt land, kombinert med at vekslere og oppbevaringstjenester av virtuell valuta vurderes å ha en høy iboende risiko for hvitvasking og terrorfinansiering.

Det er en risiko for at kriminelle aktører søker seg til tjenestetilbydere som ikke er underlagt registreringsplikt av Finanstilsynet.

Se Økokrims omtale under «Bruk av kryptovalutavekslere og miksere».

4.7 E-pengeforetak

Det handles for betydelige beløp i Norge med forhåndsbetalte anonyme betalingskort fra utlandet. Slike kort skjuler hvem som bruker kortet, informasjonen begrenser seg til beløp og utsteder. Slike kort kan være egnet for å hvitvaske penger, men kortene kan også finansiere terrorisme.

4.8 NPO – Frivillig sektor

Hvert år blir betydelige pengesummer sendt ut av landet av frivillige organisasjoner (NPO), med det formål å støtte veldedig virksomhet. I enkelte tilfeller kan giver bli forledet til å tro at pengene går til humanitære formål, mens de i realiteten går til kriminelle.

Målet er å hindre at NPO-sektoren mottar eller samler inn penger og flytter de med det formål å finansiere terrorisme. Dette er også viktig fra et annet perspektiv, nemlig å bevare NPO-sektorens integritet.

Mye av kontrollen av NPO-sektoren er frivillig, og det er en sammenheng mellom i hvor stor grad en NPO er registrert, hvilke incentivordninger den har og hvor godt den blir kontrollert. Det er de NPO-ene som i liten grad registrerer seg som utgjør størst risiko for at pengene går til kriminelle formål, herunder finansiering av terrorisme.

Som en NPO i Norge kan man registrere seg både i Enhetsregisteret, Frivillighetsregisteret, Frivillighet Norge, Innsamlingskontrollen. I tillegg kan man søke på å få motta offentlig støtte, momskompensasjon og en skattefradragsordning.

Når man registrerer seg i flere register og mottar offentlig støtt, økes krav om kontroll og rapportering.

NPOer som ønsker å finansiere kriminalitet, vil unngå for mye kontroll og prøver derfor å unngå dette. Organisasjoner, som kun velger å registrere seg i Enhetsregisteret, og har som hoved-oppgave å samle inn penger til konfliktområder, er de det knyttes mest usikkerhet og risiko ved.

5. Kilder – NRA 2022 Terrorfinansiering

EFE, «Trendrapport», 2021.

Europol, «European Union Terrorism Situation and Trend report 2022 (TE-SAT)», 2022.

FATF, «Ethnically or racially motivated terrorist financing», juni 2021.

FATF, «Money Laundering and Terrorist Financing Risks Arising from Migrant Smuggling», mars 2022.

FATF, «Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing - Public Sector», september 2020.

FN v/Sikkerhetsrådet, «Security Council Committee pursuant to resolutions 1267 (1999) 1989 (2011) and 2253 (2015) concerning Islamic State in Iraq and the Levant (Da'esh), Al-Qaida and associated individuals, groups, undertakings and entities», 2020.

Forsvarets etterretningstjeneste, «Fokus», 2022.

PST, «Nasjonal trusselvurdering (NTV)», 2022.

PST, «Nasjonal trusselvurdering (NTV)», 2021.

Regjeringen.no, «Regjeringens strategi for bekjempelse av hvitvasking, terrorfinansiering og finansiering av spredning av masseødeleggelsesvåpen», juni 2020.

Økokrim, «Trusselvurdering» 2022.

Vedlegg til nasjonal risikovurdering hvitvasking og terrorfinansiering

Del 3

Norges antihvitvaskings- og terrorfinansierings-regime

Oppdatert per oktober 2022

1. Internasjonalt rammeverk

1.1. Financial Action Task Force (FATF)

FATF er et mellomstatlig samarbeidsorgan som ble etablert i 1989 av G7-gruppen. FATF er en selvstendig enhet, men mandatet og oppgavene har en sterk tilknytning til G20 og beslutninger som blir fattet på ministermøtene.

Mandatet til FATF fastsettes på ministernivå av medlemslandene. Formålet er å fastsette standarder og sikre implementering av rettslige og operative tiltak for å bekjempe hvitvasking og finansiering av terror. FATF består av 37 medlemsland, 2 regionale organisasjoner, 9 assosierte medlemsgrupper og 23 observatører (som Egmont Group, Verdensbanken, Europol, FN og Eurojust). Formålet med FATF er å få til en enhetlig internasjonal tilnærming til bekjempelsen av hvitvasking og finansiering av terror. FATF har fastsatt 40 anbefalinger som er en internasjonal standard for bekjempelsen av hvitvasking og finansiering av terror. I tillegg er det fastsatt kriterier for å måle om medlemslandene har implementert anbefalingene, og om de gir de forventede resultatene, slik som antall analyser for finansiell etterretning, straffesaker, inndragning, med mer.

FATFs 40 anbefalinger[153] og krav til nasjonal etterlevelse av standardene (Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems)[154] er grunnlaget for regimet mot hvitvasking og terrorfinansiering i Norge. FATF legger til grunn at medlemslandene skal ha en risikobasert tilnærming til hvitvasking og finansiering av terror. Basert på de identifiserte risikoene skal det utarbeides en nasjonal policy på området, og det skal være mekanismer på plass som ivaretar kravet om implementering, ressursallokering og samarbeid mellom berørte aktører.[155] Den nasjonale risikovurderingen for hvitvasking og terrorfinans er en del av dette.

1.2. EUs hvitvaskingsdirektiv

Europaparlamentets- og rådsdirektiv (EU) 2017/849 om tiltak for å beskytte det finansielle system mot hvitvasking og terrorfinansiering ble vedtatt 20. mai 2015. Direktivet er EUs fjerde hvitvaskingsdirektiv. Direktivet ble tatt inn i EØS-avtalen i desember 2018.

Et endringsdirektiv ble formelt vedtatt i mai 2018 og er til vurdering for innlemmelse i EØS-avtalen. Innlemmelse av direktivkravene i EØS-avtalen vil innebære endring i det norske anti-hvitvaskings- og terrorfinansieringsregelverket. Disse endringene er i all hovedsak allerede gjennomført.

153 FATF, «The FATF Recommendations; International Standards On Combating Money Laundering And The Financing Of Terrorism & Proliferation», 2012.
154 FATF, «Methodology for assessing technical compliance with the FATF recommendations and the effectiveness of AML/CFT systems», februar 2013.
155 Anbefaling 1 og 2.

20. juli 2021 presenterte EU Kommisjonen en pakke bestående av fire regelverksforslag med det formål å styrke EUs regler og innsats mot hvitvasking og terrorfinansiering (AML/CFT. Kjernen i forslaget til regelverkspakke er opprettelsen av en ny EU-tilsynsmyndighet for bekjempelse av hvitvasking av penger og finansiering av terrorisme, og som igjen skal bidra til mer enhetlige AML/CFT-tilsyn i EU/EØS og styrke samarbeidet mellom medlemslandenes finansielle etterretning (FIU). En rekke bestemmelser som i dag er vedtatt i direktivs form, forslås gjennomført i en ny forordning. Forslaget til nytt direktiv, vil erstatte EUs fjerde hvitvaskingsdirektiv, samt at det foreslås innført nye bestemmelser som har til hensikt å styrke medlemslandenes AML/CFT-tilsynsmyndigheter og FIUer. Det foreligger også et forslag til omarbeiding av en forordning som vil gjøre det mulig å spore overføringer av visse kryptoeiendeler.

1.3. FN

FNs sikkerhetsråds resolusjoner (UNSCR) gir også føringer. Særlig relevant her er UNSCR 2253, UNSCR 1267 og UNSCR 1373, som fastsetter og styrker regimet for sanksjoner mot terrorfinansiering og finansiering av spredning av masseødeleggelsesvåpen.

1.4. The Egmont Group

The Egmont Group er en internasjonal sammenslutning for enheter for finansiell etterretning (Financial Intelligence Units (FIU-er)). 164 FIU-er fra hele verden er medlemmer i Egmont. Enheten for finansiell etterretning i Økokrim (EFE)[156] er Norges FIU og ble medlem av Egmont i 1995. Det er et kriterium i FATF at medlemslandenes FIU skal være medlem i Egmont. Kriteriene for medlemskap fastsettes ved FATFs anbefalinger, Egmonts Charter og Principles for Information Exchange between FIUs. De to sistnevnte er bindende for EFE.

FATF og Egmont Group jobber også for å utvikle et nærmere samarbeid for å sikre at FIU-enes operative erfaringer og kompetanse skal nyttiggjøres bedre i det internasjonale samarbeidet, herunder ved FATFs evalueringer, rapporter om strategisk analyse og policydiskusjoner.

156 EFE er nærmere beskrevet under pkt. 3.2.

2. Nasjonal lovgivning

2.1. Lov om tiltak mot hvitvasking og terrorfinansiering mv. (hvitvaskingsloven) med forskrifter

Gjeldende hvitvaskingsregelverk fremgår av lov 1. juni 2018 om tiltak mot hvitvasking og terrorfinansiering mv. (hvitvaskingsloven) og forskrift 14. september 2018 om tiltak mot hvitvasking og terrorfinansiering (hvitvaskingsforskriften).

Hvitvaskingslovens formål er å forebygge og avdekke hvitvasking og terrorfinansiering, jf. § 1. Loven angir i § 4 hvem som er rapporteringspliktige, og i §§ 9 flg. gis regler om kundetiltak og løpende oppfølgning. Dersom rapporteringspliktige avdekker forhold som kan indikere at midler har tilknytning til hvitvasking eller terrorfinansiering, skal det foretas nærmere undersøkelser, jf. § 25. Dersom det etter de nærmere undersøkelsene er forhold som gir grunnlag for mistanke om hvitvasking eller terrorfinansiering, skal rapporteringspliktige oversende opplysninger om forholdene til Økokrim ved Enheten for finansiell etterretning, jf. § 26. Mistenkelige transaksjoner skal som hovedregel ikke gjennomføres før Økokrim er underrettet, jf. § 27. Økokrim har da muligheten til i særlige tilfeller å gi pålegg om at transaksjonen ikke skal gjennomføres.

I hvitvaskingsforskriften er det gitt nærmere regler om kundetiltak og løpende oppfølging av kunden (kapittel 4), undersøkelse og rapportering (kapittel 5) samt behandling av personopplysninger og andre opplysninger (kapittel 6).

2.2. Straffelovens bestemmelser om hvitvasking

Hvitvasking er straffsanksjonert i straffeloven §§ 337 (simpel hvitvasking), 338 (grov hvitvasking), 339 (mindre hvitvasking), 340 (uaktsom hvitvasking) og 341 (forbund om hvitvasking). En endring i forhold til reglene i straffeloven av 1902 er at medvirkning til hvitvasking nå er straffbart. Bortsett fra en nedjustering av strafferammen ble det ikke foretatt realitetsendringer i forhold til straffeloven av 1902. Innholdet i bestemmelsen er nærmere omhandlet i Ot.prp. nr. 53 (2005–2006) om lov om endringer i straffeloven 1902 og utleveringsloven (gjennomføring av FN-konvensjonen mot korrupsjon).

Straffeloven §§ 337 *første ledd bokstav a* inneholder gjerningsbeskrivelsen for hvitvasking av utbytte som en bistandshandling til andre og erstatter straffeloven 1902 § 317 første ledd annet alternativ. *Første ledd bokstav b* gjør det straffbart å hvitvaske utbytte fra egne straffbare handlinger (selvvask) og viderefører straffeloven 1902 § 317 annet ledd. *Annet ledd* retter seg mot hvitvasking av surrogater og viderefører straffeloven 1902 § 317 første ledd tredje punktum. *Tredje ledd* viderefører straffeloven 1902 § 317 tredje ledd om at hvitvaskeren kan straffes, selv om den som begikk primærlovbruddet var utilregnelig eller mindreårig. *Fjerde ledd* angir strafferammen og bestemmer at hvitvasking kan straffes med bot eller fengsel inntil to år. Dette er en nedjustering i forhold til straffeloven 1902 § 317. Begrunnelsen er at

strafferammen skal gi et mer realistisk bilde av straffutmålingspraksis i dag, og det er ikke meningen at hvitvasking skal bedømmes mindre alvorlig enn i dag.

2.3. Straffelovens bestemmelser om terrorfinansiering

Terrorfinansiering er straffesanksjonert i straffeloven §§ 135 og 136 a. Nevnte paragrafer gjennomfører FNs terrorfinansieringskonvensjon artikkel 4 bokstav a, jf. artikkel 2 og FNs sikkerhetsråds resolusjon 1373 (2001) OP 1 (b) og (d) med flere. Bestemmelsene rammer det å samle inn og fremskaffe penger eller andre økonomiske midler til terrorhandlinger eller til noen som begår slike handlinger.

Straffeloven § 135 rammer både den som «yter» eller «mottar», og den som passivt tar imot penger som er samlet inn av andre, for så å gi dem videre til støtte til en terrorhandling eller til noen som begår slike handlinger. Bestemmelsen omfatter også den som «sender» – sørger for at midlene overføres til andre – i tillegg til den som «fremskaffer eller samler inn», altså mellommenn som skaffer til veie økonomiske midler ved innsamlinger eller lignende.

Det er ikke et krav at det ved oversendelse er klart hvilken terrorhandling midlene skal finansiere, eller at midlene alene er tilstrekkelige til å finansiere terrorhandlinger. Bestemmelsen rammer også den som fremskaffer eller samler inn midler som delvis skal finansiere terrorhandlinger. Det trenger heller ikke være den tiltenkte bruken, men om mottageren er en person eller enhet som begår eller forsøker å begå terrorhandlinger, som kan danne grunnlag for straff. Det kan dermed være straffbart å gi økonomisk støtte til slike personer eller organisasjoner, selv om støtten er tiltenkt personens eller organisasjonens eventuelle lovlige virksomhet.

Bestemmelsen rammer også den som stiller finansielle tjenester til rådighet for terrorister eller terrorgrupper, for foretak som eies eller kontrolleres av terrorister eller terrorgrupper, eller for noen som handler på vegne av eller på instruks fra disse. Med «finansielle tjenester» forstås blant annet ulike banktjenester – som betalingstjenester, lån og kreditter – og ulike typer rådgivning og investeringstjenester etter verdipapirhandelloven.

Straffeloven § 135 omfatter altså alle elementer av finansiell støtte, men antas å være mest anvendelig ved finansiering i form av penger eller formuesgoder av en viss størrelse. For tilfeller av støtte i form av mindre pengebeløp, eller for eksempel anskaffelse av utstyr, kan straffeloven § 136 a komme til anvendelse.

Straffeloven § 136 a tilsvarer straffeloven 1902 § 147 d. Den rammer etter sin ordlyd «(…) den som danner, deltar i, rekrutterer eller yter økonomisk eller annen materiell støtte til en terrororganisasjon (…)». Materiell støtte kan være for eksempel i form av å levere utstyr til en fremmedkriger.

2.4. Finansielle sanksjoner og restriktive tiltak – frysforpliktelser

Ny lov om gjennomføring av internasjonale sanksjoner trådte i kraft 16.4.2021. Sanksjonsloven erstatter to fullmaktslover fra 1968 og 2001, som frem til i dag har vært brukt til å gjennomføre i norsk rett folkerettslig, bindende FN-sanksjoner og EUs restriktive tiltak som Norge slutter opp om. I all hovedsak videreføres reglene i den gamle sanksjonsloven. Norge er folkerettslig forpliktet til å gjennomføre sanksjoner vedtatt av FNs sikkerhetsråd, og har i tillegg hatt som praksis å gjennomføre restriktive tiltak vedtatt av EU. Begge deler skjer gjennom vedtakelse av forskrifter med hjemmel i sanksjonsloven.

Utenriksdepartementet og Finanstilsynet har utgitt en veiledning om finansielle sanksjoner/restriktive tiltak. Veilederen gir en beskrivelse av lovbestemmelser og retningslinjer for gjennomføring av FNs og EUs frysforpliktelser. En ny oppdatert versjon vil komme høsten 2022.

2.5. Båndlegging

FNs sikkerhetsrådsresolusjon 1373 om frys- og listeføringsforpliktelser er gjennomført i norsk rett ved bestemmelser i politiloven § 17 g om båndlegging (frys) av midler tilhørende personer som med god grunn mistenkes for overtredelse av eller forsøk på overtredelse av straffeloven §§ 131, 133, 134, 135, 136 eller 136 a.

3. Regimets aktører og koordinering

3.1. De rapporteringspliktige

I henhold til hvitvaskingsloven (2018) § 4 er følgende juridiske personer rapporteringspliktige:

a. bank
b. kredittforetak
c. finansieringsforetak
d. Norges Bank
e. e-pengeforetak
f. foretak som driver valutavirksomhet
g. betalingsforetak og andre som har rett til å yte betalingstjenester
h. verdipapirforetak
i. forvaltningsselskap for verdipapirfond
j. forsikringsforetak
k. foretak som driver forsikringsformidling som ikke er gjenforsikringsmegling
l. verdipapirsentraler, i tilfeller der verdipapirsentralen ikke benytter ekstern kontofører som er rapporteringspliktig. For kontohavere og utstedere som har ekstern kontofører som er rapporteringspliktig, er det kontoføreren som er rapporteringspliktig
m. foretak som driver depotvirksomhet
n. forvalter av alternative investeringsfond
o. låneformidlingsforetak

Loven gjelder også for følgende juridiske og fysiske personer i utøvelsen av deres yrke:

a) statsautoriserte og registrerte revisorer, godkjente revisjonsselskaper og revisorer som er ansvarlig for revisjon av regnskap for kommune, fylkeskommune eller kommunalt eller fylkeskommunalt foretak. Tilbyr personer eller foretak som nevnt i første punktum virksomhetstjenester, er de uansett underlagt loven på dette grunnlaget.
b) autoriserte regnskapsførere og autoriserte regnskapsførerselskaper. Tilbyr personer eller foretak som nevnt i første punktum virksomhetstjenester, er de uansett underlagt loven på dette grunnlaget.
c) advokater og andre som ervervsmessig eller stadig yter selvstendig rettshjelp, når de på klientens vegne utfører finansiell transaksjon eller en transaksjon som gjelder fast eiendom, eller når de bistår ved planlegging eller utføring av transaksjon for klient i forbindelse med
    1. kjøp og salg av fast eiendom eller virksomhet
    2. forvaltning av en klients penger, verdipapir eller andre aktiva
    3. åpning eller forvaltning av bank- eller verdipapirkonto
    4. fremskaffelse av nødvendig kapital til opprettelse, drift eller ledelse av selskap
    5. opprettelse, drift eller ledelse av selskap, fond eller en lignende juridisk person eller formuesmasse, herunder utenlandsk trust eller tilsvarende juridisk arrangement
d) eiendomsmeglere og eiendomsmeglingsforetak

e) tilbydere av virksomhetstjenester
f) personer med begrenset tillatelse til å yte betalingstjenester
g) tilbydere av spilltjeneste

Forhandlere av gjenstander er ikke rapporteringspliktige og kan ikke motta vederlag i kontanter på 40 000 kroner eller mer eller tilsvarende beløp i utenlandsk valuta. Skattekontoret fører kontroll med at dette blir overholdt, jf. § 5.

Tilbydere av vekslingstjenester mellom virtuell valuta og offisiell valuta, mellom ulike virtuelle valutaer, og oppbevaringstjenester for virtuell valuta, omfattes av gruppen rapporteringspliktige, jf. § 1-3 i forskrift til hvitvaskingsloven.

3.2 Enheten for finansiell etterretning

Enheten for finansiell etterretning (EFE) er den avdelingen i Økokrim som behandler rapportene om mistenkelige transaksjoner som sendes inn av de rapporteringspliktige. EFE har i motsetning til straffesaksteamene i Økokrim ikke etterforskning eller straffesaksarbeid som primære oppgaver, men er Norges nasjonale enhet for finansiell etterretning (Financial Intelligence Unit (FIU)), og er å betrakte som en etterretningsenhet med nasjonalt ansvar.

EFE er opprettet på bakgrunn av FATF-anbefalingene, som pålegger medlemslandene å etablere nasjonale FIU-er for mottak, analyse og videreformidling av finansiell informasjon knyttet til mulig hvitvasking og finansiering av terror.

EFEs hovedoppgaver er å motta rapporter om mistenkelige transaksjoner (MT-rapporter) fra rapporteringspliktige etter hvitvaskingsloven, å analysere informasjonen og å videreformidle informasjon til rett instans. Opplysningene EFE mottar behandles og videreformidles i tråd med politiregisterloven og forskriftens bestemmelser. EFE kan formidle informasjon i form av etterretningsrapporter, informasjon i politiets etterretningssystem, anmeldelser, politirapporter i eksisterende straffesaker, strategiske rapporter, årsrapporter og i form av publisering på hvitvasking.no, foredrag ved ulike studier ved Politihøgskolen samt foredrag for politidistrikter der det har vært behov eller etterspurt. Mottagerne av etterretningsinformasjon er i all hovedsak politiet, inkludert PST, forvaltningsorganer med kontrolloppgaver samt andre lands FIU-er. I tillegg formidles det informasjon til privat sektor. Dette gjelder særlig formidling av moduser og trender til de rapporteringspliktige. På bakgrunn av initiativ fra Egmont Group og FATF har EFE på lik linje med andre FIU-er formidlet informasjon om fenomenet fremmedkrigere med mer til privat sektor. Formålet med dette er å sette dem best mulig i stand til å identifisere transaksjoner som har tilknytning til finansiering av terror.

EFE er et nasjonalt kompetansesenter for spørsmål relatert til hvitvasking og terrorfinansiering. EFE følger med på kriminalitetsutviklingen blant annet gjennom deltagelse i aktuelle internasjonale fora, som FATF, Egmont Group og INTERPOL, og holder løpende kontakt med samarbeidspartnere og spesielt de rapporteringspliktige, for å bidra til kompetanse- og metodeutvikling.

Det nasjonale regimet mot hvitvasking og finansiering av terror skal som bemerket innledningsvis være risikobasert. Med bakgrunn i dette, og i tråd med det særskilte internasjonale fokuset som er på finansiering av terror, har EFE dreid mye av sin aktivitet mot dette feltet. Dette er spesielt synlig i innsatsen på operativ analyse. Mye av samarbeidet på operativt nivå har skjedd ved deltagelse i nasjonale samarbeidsprosjekter med terrorfinansiering som en av flere moduser. Dette har vist seg å være en fornuftig og effektiv måte å få delt informasjon på. Samarbeidet med PST er særlig viktig i denne sammenhengen.

3.3 Finanstilsynet

Det følger av lov 7. desember 1956 nr. 1 om tilsynet for kredittinstitusjoner, forsikringsselskaper og verdipapirhandel mv. (finanstilsynsloven) § 1 at Finanstilsynet skal føre tilsyn med en rekke foretak og personer, herunder de som faller under Finanstilsynets tilsyn etter hvitvaskingsloven § 43 annet ledd bokstav a og hvitvaskingsforskriften § 1-3 sjette ledd.

Det følger av finanstilsynsloven § 3 at tilsynet skal påse at foretak det har tilsyn med virker på hensiktsmessig og betryggende måte «i samsvar med lov og bestemmelser gitt i medhold av lov». Det fremgår videre av samme bestemmelse at foretakene plikter å gi alle opplysninger som tilsynet måtte kreve og å la tilsynet få innsyn i og i tilfelle få utlevert dokumenter, protokoller, regnskapsopplysninger og annet tilgjengelig materiale.

Finanstilsynet gjennomfører hvitvaskingstilsyn både som særskilte tematilsyn og som en del av ordinære tilsyn med de rapporteringspliktige. Tilsynene omfatter blant annet undersøkelser av foretakenes identifisering og håndtering av risikoen foretaket er eksponert for, at interne rutiner beskriver foretakets gjennomføring av regelverket og den faktiske etterlevelsen av regelverket og de interne rutinene.

Finanstilsynet har en rekke virkemidler der foretakene ikke etterlever hvitvaskingsloven. De kan gi rapporteringspliktige foretak under tilsyn pålegg om retting og tvangsmulkt for å rette en pågående lovovertredelse, overtredelsesgebyr til foretak eller enkeltpersoner, og ledelseskarantene. Ved alvorlige overtredelser av foretakenes lovpålagte plikter kan Finanstilsynet tilbakekalle institusjonens konsesjon eller tillatelse.

3.4 Tilsynsrådet for advokatvirksomhet

Det følger videre av lov 13. august 1915 nr. 5 (domstolloven) § 225 første ledd at Tilsynsrådet for advokatvirksomhet fører tilsyn med advokater. Tilsynsrådet har adgang til å meddele irettesettelser og advarsler, og dersom det mener at det bør treffes vedtak om tilbakekall av advokatbevilling, kan det fremme slikt forslag overfor Advokatbevillingsnemnden. I hvitvaskingsloven (2018) er tilsynsmyndighetene gitt hjemler til å ilegge flere typer forvaltningstiltak og administrative sanksjoner, slik som ledelseskarantene og overtredelsesgebyr.

3.5 Skatteetaten

Skatteetaten har fått i oppgave å kontrollere at forhandlere av gjenstander ikke mottar 40 000 kroner eller mer i kontanter. Kontroll som nevnt foran kan gjennomføres i forbindelse med etatens øvrige kontroller av relevante kontrollobjekter (forhandlere av gjenstander). Skatteetaten er ikke tilsynsmyndighet tilsvarende Finanstilsynet og Lotteritilsynet, og det blir lagt til grunn at kontrollomfanget skal balanseres mot etatens øvrige kontrollvirksomhet basert på vurderinger av risiko og vesentlighet.

3.6 Lotteritilsynet

Lotteritilsynet fører tilsyn med tilbydere av spilltjenester. Dette omfatter enerettstilbyderne Norsk Tipping og Stiftelsen Norsk Rikstoto og det private lotterimarkedet (f.eks. bingo og spill på skip)

Tilsynsvirksomheten er innrettet mot at tilbydere av spilltjenester har tilfredsstillende interne rutiner for gjennomføring av hvitvaskingsregelverket og at disse etterleves.

3.7 Politiets sikkerhetstjeneste

Politiets sikkerhetstjeneste (PST) skal forhindre at terror og terrorfinansiering foregår i og fra Norge. I tillegg skal PST avverge at Norge utnyttes som transittland for penger til terrorformål. PST er direkte underlagt Justis- og beredskapsdepartementet (sideordnet med Politidirektoratet) og er en del av den norske politietaten.

PST skal opprette forebyggende sak når det innledes undersøkelser med sikte på å bekrefte eller avkrefte at noen forbereder et straffbart forhold innenfor PSTs ansvarsområde etter politiloven § 17 b. Forebyggende saker om terror og terrorfinansiering kan avsluttes eller håndteres med mottiltak i det forebyggende sporet. I enkelte tilfeller fører undersøkelser i forebyggende øyemed til at det etableres en mistanke, jf. straffeprosessloven § 224, som begrunner etablering av en etterforskning i straffeprosessuell forstand. PST har ansvar for etterforskning av avvergende terror- og terrorfinansieringssaker.

Som nasjonal sikkerhetstjeneste har PST et nært samarbeid med mange etater, institusjoner og andre aktører i Norge. Med de viktigste samarbeidspartnerne er det et formalisert samarbeid, og med andre er det samarbeid og kontakt ved behov. Etterretningstjenesten og PST har etablert et felles etterretning -og koordineringssenter, som skal sørge for effektiv informasjonsflyt mellom enhetene.

Enheten for finansiell etterretning (EFE) ved Økokrim og PST har også styrket sitt samarbeid for å enklere kunne avdekke og etterforske terrorfinansiering, og prosjektet har vært samlokalisert i PST sine lokaler.

PST har et utstrakt samarbeid med andre lands politimyndigheter og sikkerhets- og etterretningstjenester. Det omfattende internasjonale nettverket er avgjørende for å forebygge alvorlig kriminalitet mot norske interesser.

PST driver omfattende opplæring og foredragsvirksomhet om bekjempelse av finansiering av terror og masseødeleggelsesvåpen for både offentlig sektor og private aktører, spesielt finansnæringen.

3.8 Politiet

Politiet består av PST, Politidirektoratet, tolv politidistrikter, særorganene Kripos, Økokrim, Politiets utlendingsenhet, Utrykningspolitiet og Politihøgskolen. Politidistriktene og særorganene er administrativt og faglig underlagt Politidirektoratet[157], mens riksadvokaten har ansvaret for den overordnede faglige ledelsen av straffesaksbehandlingen i politiet. Politiet startet gjennomføringen av nærpolitireformen i 2016. Reformen innebærer struktur- og organisasjonsendringer i politidistriktene, og antall politidistrikter ble redusert fra 27 til 12.

Fra 2005 har alle politidistrikter vært pålagt å opprette egne økoteam, som har et særskilt ansvar for å bekjempe økonomisk kriminalitet. Økoteamene er bemannet med politi, jurister og revisorer, og den tverrfaglige kompetansen skal gjøre økoteamene i stand til å behandle større økonomiske straffesaker. Økoteamene skal som hovedregel være samlokalisert og skjermet fra andre oppgaver. Manglende kapasitet er en av hovedutfordringene for politiet og for økoteamene. Nærpolitireformen skal sikre mer robuste fagmiljøer med større kapasitet og økt kompetanse til å etterforske økonomisk kriminalitet. De fleste sakene innen økonomisk kriminalitet, herunder hvitvasking, etterforskes i politidistriktene.

Økt fokus på terror har ført til at politiet har økt sin innsats mot, og prioritering av, arbeid mot terror og terrorfinansiering.

3.9 Tolletaten

Tolletaten beskytter samfunnet mot ulovlige og restriksjonsbelagte varer og sikrer statens inntekter gjennom riktige grunnlag for toll og avgifter. Gjennom dette bidrar etaten til å beskytte bedrifter og arbeidsplasser mot konkurranse fra uærlige aktører.

Fra 1. oktober 2020 består Tolletaten av tolldirektør med to staber og seks divisjoner med nasjonalt ansvar, hvorav grensedivisjonen og vareførselsdivisjonen er de to største. Tolletaten bidrar til etterlevelse av toll- og vareførselsreglene samt regelverkene til en rekke andre statlige etater, herunder blant annet regelverk for skatter og avgifter, valuta, narkotika, alkohol, tobakk, legemidler, våpen, farlige stoffer, næringsmidler, dyr, miljø, avfall og immaterielle rettigheter.

157 PST er direkte underlagt Justis- og beredskapsdepartementet.

Tolletaten håndhever regelen om at medbragt valuta ut over grensebeløpet skal deklareres. Tolletaten kan ved avdekking av brudd på deklareringsplikten ilegge et administrativt overtredelsesgebyr på 20 prosent av beløpet eller anmelde forholdet hvis det mistenkes at valutaen stammer fra utbytte av straffbare handlinger, hvitvasking eller lignende. Ved anmeldelse tilbakeholdes hele beløpet, og saken overføres politiet for vurdering, forelegg, videre etterforskning og dom. Tolletaten rapporterer saker jevnlig til EFE.

Tolletaten sørger også for at alle deklarerte beløp som bringes inn eller ut av landet registreres i Valutaregisteret som fysiske transaksjoner.

3.10 Overordnet koordinering og samarbeid mellom aktørene i regimet

Et særtrekk ved det nasjonale arbeidet mot hvitvasking og finansiering av terror er at det er tverretatlig og tverrfaglig. Det innebærer at det ikke er en enkelt etat eller organ som sitter med eneansvaret for arbeidet, men at det er summen av alle de ansvarlige etaters innsats som er avgjørende. Dette illustreres særlig ved FATFs Effectiveness-kriterier, hvor samhandling og flyt av informasjon er grunnleggende faktorer for en effektfull nasjonal innsats. I forlengelsen av dette er det ikke eksistensen av innsatsen alene som skal evalueres. Det avgjørende er til syvende og sist de resultatene man klarer å frembringe gjennom samarbeidet. Måleparametere for dette er blant annet antall dommer for hvitvasking og finansiering av terror og dommer og forelegg for inndragning.

Sammenhengen i systemet kan illustreres ved at tilsynsmyndighetene må føre et risikobasert tilsyn for å fange opp mangler i effektiviteten i de rapporteringspliktiges preventive systemer, deretter at de rapporteringspliktige fanger opp de mistenkelige transaksjonene og rapporterer disse til EFE. EFE må ha tilgang til de nødvendige kildene og være i stand til å utføre operative og strategiske analyser, som så formidles til politiet. Det som formidles må være av en slik kvalitet og ha et innhold som gjør at det kan benyttes i politiets videre arbeid med å bekjempe kriminalitet og å sikre midler. Politiet må ha den kompetansen som trengs for å utnytte den informasjonen som blir formidlet. Tilsvarende synergier er til stede for flere deler av den nasjonale innsatsen, herunder også for finansiering av terror.

Det er særlig to faktorer som er av avgjørende betydning for en vellykket nasjonal innsats: at det er en overordnet styring og målretting av arbeidet fra toppen og ned, og at alle aktører har en risikobasert tilnærming til sine oppgaver.

For å sikre en koordinert innsats og god samhandling mellom etatene i kampen mot hvitvasking, terrorfinansiering og finansiering av spredning av masseødeleggelsesvåpen er det nedsatt et tverretatlig kontaktforum. Kontaktforumet består av representanter for

- Justis- og beredskapsdepartementet
- Finansdepartementet
- Utenriksdepartementet
- Finanstilsynet

- Politidirektoratet
- Politiets sikkerhetstjeneste (PST)
- Riksadvokatembetet
- Skattedirektoratet
- Tolldirektoratet
- Økokrim

Kontaktforum ledes av Justis- og beredskapsdepartementet. Lederen for Norges delegasjon til Financial Action Task Force (FATF) deltar fast i møtene.

Etter tema og behov, og minst én gang pr. år, skal representanter for følgende etater inviteres i møtene:
- Tilsynsrådet for advokatvirksomhet
- Lotteritilsynet
- Nasjonalt tverretatlig analyse- og etterretningssenter (NTAES)
- Politihøgskolen

Øvrige departementer eller etater inviteres etter behov.

Privat sektor skal involveres i arbeidet:
- Finans Norge, som representant for den største gruppen rapporteringspliktige foretak etter hvitvaskingsloven, møter som fast observatør ved relevante dagsordenspunkter.
- Øvrig privat sektor skal konsulteres gjennom deltakelse i relevante prosesser.

Sekretariatsansvaret går på rundgang mellom Økokrim, Finanstilsynet og POD.

3.11 Utviklingstrekk – samarbeid og informasjonsdeling

Samarbeid mellom offentlige etater og næringsliv er en forutsetning for å lykkes. Nasjonal innsats blir best og gir størst resultat hvis alle aktører virker mot samme mål. Informasjon må deles. Eksempler på dette kan være AMK-regionskontorene, NTAES og andre samarbeidsfora.

Et gjennomgående trekk på området for finansiering av terror er et utstrakt samarbeid og samordning av arbeidet i FATF og Egmont Group. Dette berører både internasjonal policyutvikling og kunnskapsdeling om trender og moduser for finansiering av terror. Forholdet til privat sektor og viktigheten av et nært samarbeid med denne er særlig vektlagt. Viktigheten av samarbeid og informasjonsdeling mellom landene, mellom landenes myndigheter og mellom myndigheter og privat sektor er også understreket av FNs sikkerhetsråd.

På det nasjonale nivået har PST og EFE et tett samarbeid om terrorfinansieringsarbeidet og samarbeider om planlegging og gjennomføring av kurs og foredrag til finansnæringen. Samarbeidet mellom EFE og politiet har økt på terrorfinansieringsområdet. I tillegg har Finanstilsynet og EFE et løpende samarbeid både på operativt og strategisk nivå. Finanstilsynet har også utstrakt kontakt med de rapporteringspliktige og de relevante næringsorganisasjonene.