Universitetet i Stavanger

DET TEKNISK-NATURVITENSKAPELIGE FAKULTET

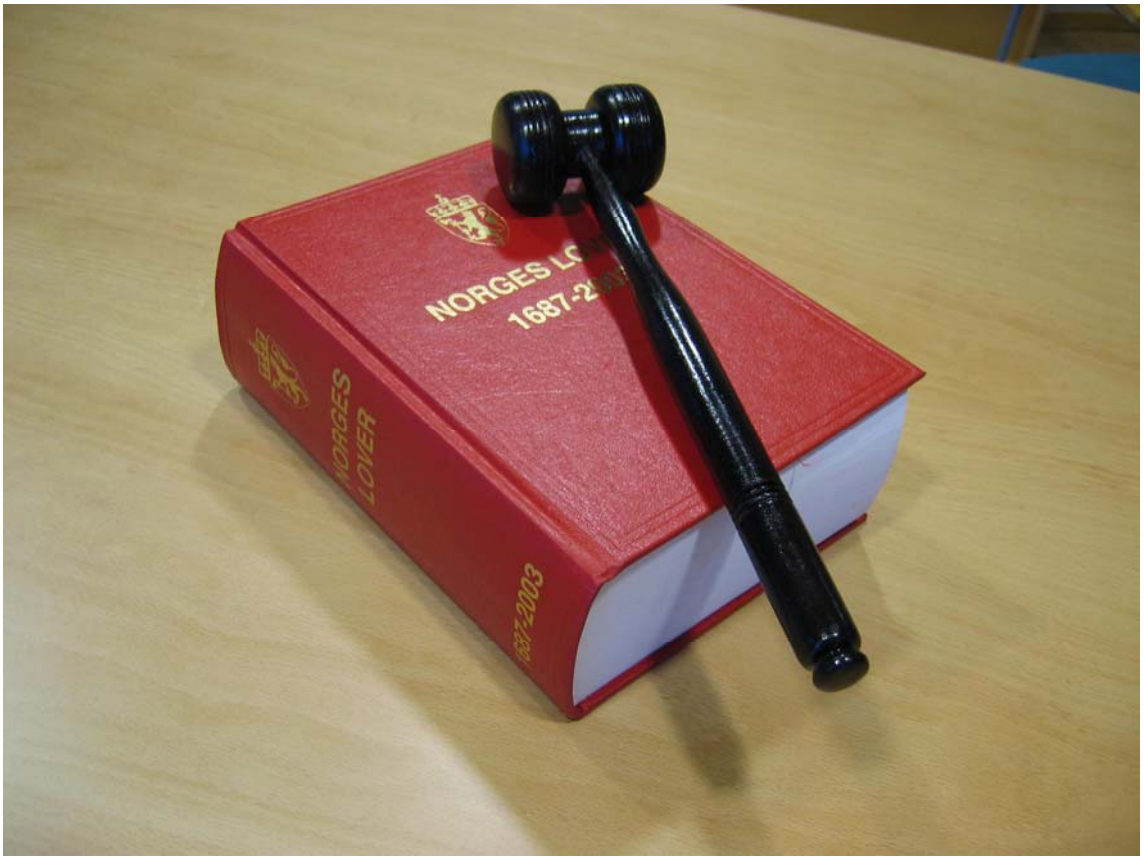
MASTEROPPGAVE

Studieprogram/spesialisering: Industriell Økonomi	Vår.....semesteret, 20..... Åpen / Konfidensiell
Forfatter: Håvard M. I. Sørensen	…… (signatur forfatter)
Fagansvarlig: Lasse B. Andersen Veileder(e): Lasse B. Andersen	
Tittel på masteroppgaven: Hvitvasking – en trussel for samfunnet og den norske banknæringen? Engelsk tittel:	
Studiepoeng: 30	
Emneord: Hvitvasking Økonomisk kriminalitet Årsakssammenhenger Bayesiansk nettverk	Sidetall: …… + vedlegg/annet: …… Stavanger, …….. dato/år

Universitetet i Stavanger

Hvitvasking – en trussel for samfunnet og den norske banknæringen?

"En studie av aktuelle scenarioer, konsekvenser og influerende faktorer"



INNHOLD

SAMMENDRAG

Hvitvasking av penger er et stort problem for samfunnet. På den ene siden fører skatteunndragelser og hvitvasking i liten skala til at velferdssystemet vårt blir underminert, og kan miste sin funksjon. På den andre siden benyttes hvitvasking av penger til finansiering av terror. I de siste 20 år har det vært et stadig økende fokus på hvivasking som terrorfinansiering, og verden fikk for alvor øynene opp den 11. september 2001 da USA ble angrepet i den største terroraksjonen i historien.

Gjennom en stadig større internasjonlisering tas det stadig nye metoder i bruk for å hvitvaske penger. Dette gir store utfordringer for alle lands bekjemping av hvitvasking, og et stadig større internasjonalt samarbeid er påkrevet.

Et annet problem, er at verden blir stadig mer teknologisk, og man kan lett overføre store pengesummer ved et par tastetrykk. Dette gir også store utfordringer for hvitvaskingsbekjempelsen.

I Norge ble det innført en egen hvitvaskingslov i 2004. I 2009 ble denne revidert i forhold til internasjonal standard, og da spesielt i forhold til anbefalingene til FATF (the Financial Action Task Force).

Denne oppgaven ser på hvitvasking som et problem i Norge og utlandet, og hva som gjøres for å bekjempe dette både på nasjonalt og internasjonalt plan. Oppgaven tar for seg hvitvaskingslovverket, hvordan trendene for hvitvasking er, og hvordan utviklingen har vært over tid. Til slutt ser den på årssaksammenhengene i forhold til hvitvasking, og hva slags barrierer og kontrollfunksjoner vi har mot dette.

KAPITTEL 1 - PROBLEMSTILLING

1.1 BAKGRUNN:

Med hvitvasking menes å sikre utbytte fra straffbar handling. For at utbyttet skal kunne brukes av gjerningsmennene, må det integreres i den legale økonomien. Formålet med hvitvaskingen er å få det til å se ut som at det er ervervet på lovlig måte, og å skjule den illegale opprinnelsen (www.hvitvasking.no – A).

Utbytte fra straffbar handling kan for eksempel være penger generert fra organisert kriminalitet, som narkotikahandel, menneskesmugling og våpensmugling, ransutbytte, penger tilegnet gjennom underslag, skatteunndragelse, bedrageri, misbruk av selskapsformer, innsidehandel eller korrupsjon (www.hvitvasking.no – A).

Motivet bak mange kriminelle handlinger er å skape profitt for den eller de personene som står bak handlingen. Når kriminalitet genererer stort utbytte må gjerningspersonene finne en måte å kontrollere midlene på uten å tiltrekke seg eller den underliggende straffbare handlingen oppmerksomhet. Hvitvaskingsprosessen er derfor avgjørende for å kunne nyte fordelene av utbyttet uten å vekke mistanke. Dette skjer ved å tilsløre midlenes opprinnelse, endre form eller flytte utbyttet til et sted hvor det er mindre sannsynlig å tiltrekke oppmerksomhet (www.hvitvasking.no – A).

Bekjempelse av hvitvasking og terrorfinansiering er høyt prioritert i det internasjonale samfunn. Formålet er å beskytte det internasjonale finanssystemets integritet og stabilitet, undergrave finansiering av terrorisme, og gjøre det vanskeligere for kriminelle å sitte igjen med utbytte fra sine forbrytelser (www.hvitvasking.no – A).

Problemstilling for norske banker.

- En stadig økende internasjonalisering og transparens gjør hvitvasking til en stadig større utfordring. Dette gjør at den norske banknæringen må overvåke både det norske og internasjonale markedet for å forhindre hvitvasking. Ny hvitvaskingslov og kontrollrutiner er utviklet for å bistå bankene i å få kontroll på hvitvasking (www.hvitvasking.no – B).

Hvitvasking skader virksomhetens omdømme

- Dersom en virksomhet involveres i hvitvasking, enten i form av at ansatte har latt seg bestikke, eller ved at virksomheten ikke har stilt spørsmål ved midlenes opprinnelse, skader dette både den enkelte virksomhet og bransjens omdømme. Bekjempelse av hvitvasking bidrar dermed til å beskytte virksomheten mot å bli misbrukt av kriminelle. Ved å ha gode rutiner for risikohåndtering beskyttes også virksomhetens ansatte (www.hvitvasking.no – B).

Konsekvenser for økonomisk utvikling

- Ujevn regulering av handels- og finansinstitusjoner på tvers av landegrensene utnyttes av aktører som driver med hvitvasking. Et par tastetrykk kan flytte enorme pengesummer i løpet av sekunder, ofte til skatteparadiser eller finanssentre som tilbyr anonyme kundeforhold. Det gjør det vanskeligere for myndigheter å spore penger som stammer fra kriminalitet. For å sikre et forretningsvennlig miljø, som er en betingelse for bærekraftig økonomisk utvikling, er det viktig å forhindre at ulike lands finanssektor taper kontroll til kriminelle. Hvitvasking utgjør en risiko for stabiliteten i finanssystemet, bidrar til forstyrrelser i internasjonale kapitalstrømmer, og underminerer hele den legale økonomien (www.hvitvasking.no – B).

Mangel på synlige ofre

- Det er sagt at hvitvasking som regel ikke har noen direkte synlige ofre, men dette må ses i sammenheng med ofte en underliggende voldelig kriminalitet. Hvitvasking har ofte tette koblinger til transnasjonal organisert kriminalitet, som narkotikatrafikk, våpensmugling, smugling av kvinner og barn til prostitusjon og hallikvirksomhet, internasjonal terrorisme og korrupsjon, og dette er gjensidig forsterkende fenomener (www.hvitvasking.no – B).

Rammer enkeltindivider

- Hvitvasking har som regel ingen synlige ofre, men enkeltpersoner rammes også indirekte. Hvitvasking bidrar blant annet til reduserte skatteinntekter og svekker statens kontroll med økonomien. Når pengene som skal komme

skattebetalerne til gode havner i kriminelle hender, forringes velferdsstatens grunnpilar. Dette svekker folks rettsoppfatning (www.hvitvasking.no – B).

1.2 MÅLSETTING OG DELIVERABLES:

Målsetting med arbeidet:

- Kartlegge omfang og trender av hvitvasking i norsk banknæring.
- Hvitvaskingsloven – hva er nytt i revisjon 2009
- Analysere årsaker og konsekvenser knyttet til hvitvasking i norsk banknæring.
- Kartlegge barrierer/ kontrollmekanismer mot hvitvasking i den norske banknæringen. Hvor er svakhetene? Hva kan forbedres?

1.3 SCOPE OF WORK / ARBEIDSOMFANG:

Omfanget av arbeidet er avgrenset i forhold til:

- Hovedfokus på norsk banknæring, men kikker også litt på det internasjonale samarbeidet.
- Hvitvaskings andel av samlet oprisk eksponering.
- Se på hvitvasking i forhold til definisjonen av operasjonell risiko;

"Risikoen for tap som følge av utilstrekkelige eller sviktende interne prosesser eller systemer, menneskelige feil, eller eksterne hendelser.". Definisjonen omfatter juridisk risiko, men ikke strategisk risiko og omdømmerisiko som må vurderes særskilt. [Basel II – fra Kredittilsynet]

1.4 GENERELT OM HVITVASKING

Hvitvasking i norsk banknæring.

Som et ledd i å bekjempe hvitvasking har Norge i likhet med svært mange andre land en særlov som pålegger finansinstitusjoner (som banker, meglerforetak og forsikringsselskaper), advokater, eiendomsmeglere, revisorer, regnskapsførere og forhandlere av verdifulle gjenstander å rapportere mistenkelige transaksjoner (MT-rapporter) til Økokrim. Hvitvaskingsloven med forskrifter trådte i kraft i 2004 og var en videreføring av finansieringsvirksomhetslovens § 2-17. Formålet med rapporteringsplikten er å gjøre det enklere å avdekke profittmotivert kriminalitet

samtidig som det kan hindre at de rapporteringspliktige brukes som kanaler for hvitvasking. MT-rapportene gir Økokrim og politiet nyttig etterretningsinformasjon for å kartlegge kriminelle aktører og nettverk, og for derigjennom å velge ut straffesaker. Antallet oversendte MT-rapporter til Økokrim har økt de siste årene, fra ca. 1 000 rapporter i 2001 til over 7 500 i 2007. Økningen i antallet rapporter gjenspeiler sannsynligvis heller økningen i antallet rapporteringspliktige samt deres økte bevissthet til hvitvasking enn at det forekommer mer hvitvasking nå enn tidligere.

Samarbeidet i FATF – the Financial Action Task Force – er sentralt. Dette er en del av et bredere internasjonalt engasjement mot økonomisk kriminalitet, som også omfatter samarbeid på politisiden og mellom skattemyndigheter, og FN-konvensjoner mot korrupsjon(EFE:2010).

KAPITTEL 2 – HVITVASKINGSLOVEN

Hvitvaskingsloven ble innført i 2004, og revidert i 2009, for å hindre finansiering av terror og annen kriminalitet gjennom økonomisk kriminalitet og hvitvasking av penger.

"Rapporteringspliktig" er en fellesbetegnelse på de foretak, virksomheter og personer som er omfattet av hvitvaskingsregelverket, jf. opplistingen i hvitvaskingsloven § 4, og punkt 2.2.2.

Kampen mot hvitvasking og økonomisk kriminalitet avhenger av samarbeid mellom alle deler av samfunnet. De bestemmelser regjeringen har bestemt knyttet til kontantbetaling for forhandlere av gjenstander gjenspeiler dette. Diskusjonen har gått mellom utvidet kundekontroll og rapporteringsplikt, slik regjeringen har foreslått, eller å erstatte bestemmelsene om forhandlere av gjenstander og innføre et kontantforbud for beløp over 100.000 kroner.

Regjeringen bestemte at beløpsgrensen på 40 000 kroner videreføres fra 2004. Selv om kontanttransaksjoner av en slik størrelsesorden er uvanlig i Norge, legges det vekt på at beløpsgrensen etter direktivet og FATF-anbefalingene er 15 000 euro (ca. 120 000 kroner) – norske regler går dermed betraktelig lenger i å omfatte kontanttransaksjoner enn det som følger av internasjonale forpliktelser og anbefalinger. (EFE:2010).

2.1 BAKGRUNN

Departementets utgangspunkter i utvikling av lovarbeidet er basert på følgende:

Generelt er det slik at utforming av lovregler for kriminalitetsbekjempelse vil måtte bero på en avveining av ulike hensyn. Tradisjonelt vil det kunne oppstå et motsetningsforhold mellom hensynet til effektiv kriminalitetsbekjempelse og personvernhensyn. En slik avveining vil i utgangspunktet bero på en skjønnsmessig vurdering, siden det dreier seg om hensyn av svært ulik karakter og den enkelte borger vil kunne tillegge slike hensyn ulik vekt. Våre internasjonale forpliktelser kan imidlertid begrense handlingsrommet i slike avveininger. Dette er i stor grad tilfellet når det gjelder innføring av nye norske regler mot hvitvasking og finansiering av terrorisme (Finansdepartementet:2004 – A).

Uavhengig av våre internasjonale forpliktelser, tilsier imidlertid de utviklingstrekk en ser innen den økonomiske kriminaliteten generelt og innen hvitvasking spesielt etter departementets vurdering at en nå styrker regelverket knyttet til hvitvasking av utbytte av straffbare handlinger. Dette tilsier etter departementets syn at en på enkelte punkter går noe lenger enn det som kreves etter våre internasjonale forpliktelser. Det vises til at hvitvasking av utbytte har en åpenbar innvirkning på veksten i økonomisk kriminalitet. Store økonomiske gevinster som utledes av kriminelle handlinger medfører et økende behov for de kriminelle til å kunne sette ulovlig ervervede midler i omløp for å kunne skjule opprinnelsen og dermed kunne nyte godt av midlene. Bekjempelse og forebyggelse av hvitvasking vil derfor være et viktig og effektivt hjelpemiddel i kampen mot økonomisk kriminalitet (Finansdepartementet:2004 – A).

Når virksomheten benyttes som ledd i hvitvasking av utbytte, er det fare for skadevirkinger for så vel virksomhetens soliditet og stabilitet, som virksomhetens troverdighet og tillit. Tradisjonelt sett anses den finansielle sektor for å være særlig utsatt for misbruk til hvitvaskingsformål. Internasjonale erfaringer, herunder FATFs typologiundersøkelser, viser at tendensen går i retning av at de kriminelle i tillegg benytter andre kanaler for å hvitvaske midler som stammer fra kriminelle handlinger. Det er derfor viktig at ikke-finansielle virksomheter og personer bringes aktivt inn i arbeidet med å bekjempe økonomisk kriminalitet. Av særlig betydning er det å samtidig iverksette tiltak som hindrer de kriminelle i å benytte profesjonell bistand til hvitvaskingsformål. Det vises bl.a. til at advokaters og revisorers taushetsplikt vil kunne utnyttes i slike operasjoner (Finansdepartementet:2004 – A).

Det er en tendens til en økende internasjonalisering av økonomisk kriminalitet. For å sikre en effektiv bekjempelse av slik kriminalitet er det nødvendig å samordne og harmonisere tiltak gjennom internasjonalt samarbeid. Det er av vesentlig betydning at internasjonale tiltak gjennomføres i norsk rett. Dette gjelder særlig fordi kapitalbevegelser over landegrensene er liberalisert. Slik liberalisering medfører bl.a. at kapital med tilknytning til straffbare handlinger mv. vil kunne tilflyte land som har mindre effektive lovregler mot hvitvasking mv. enn andre sammenlignbare land. En slik situasjon bør en unngå i Norge, og vi bør derfor tilstrebe å ha lovregler på linje med de som gjelder internasjonalt (Finansdepartementet:2004 – A).

Det er viktig at det settes en høy standard for beskyttelse av den finansielle sektor og andre yrkesgrupper mot skadevirkningene av hvitvasking av utbytte fra kriminell virksomhet. Tiltak mot hvitvasking av utbytte vil også kunne bidra til å spore opp midlenes opprinnelse og gjøre det mulig å finne ut hvem som står bak de straffbare handlingene og hvitvaskingen (Finansdepartementet:2004 – A).

Tilsvarende hensyn gjør seg gjeldene i forhold til terrorfinansiering. Angrepene i USA 11. september 2001 er ansett som det alvorligste angrepet mot en stat og dens befolkning som noen gang er gjennomført av terrorister. Avdekkingen av den geografiske rekkevidden av infrastrukturen for finansiering av terrorhandlinger, har medført at fokus er rettet mot mulige mottiltak for å kunne avdekke og bryte ned slike strukturer. Også i Norge er arbeidet mot finansiering av terrorhandlinger gitt høy prioritet (Finansdepartementet:2004 – A).

Hvitvasking av utbytte fra straffbare handlinger og innsamling av midler til finansiering av terrorhandlinger skjer vanligvis i flere operasjoner og på mange ulike måter. Den tekniske utviklingen har gjort det mulig å raskt overføre midler mellom forskjellige land, noe som kan bidra til å gjøre det enklere for kriminelle å skjule opprinnelsen til midlene eller hensikten med overføringen. Det er viktig at regler mot hvitvasking og terrorfinansiering oppdateres med henblikk på å møte de utfordringer den teknologiske utviklingen medfører (Finansdepartementet:2004 – A).

Hvitvasking av utbytte og finansiering av terrorisme vil ofte skje gjennom de samme kanaler (særlig det finansielle system). Dette gjør det naturlig å behandle tiltak mot slike aktiviteter i samme lov. Det er imidlertid viktig å være klar over de grunnleggende forskjeller mellom de to situasjonene. Hvitvasking av utbytte har som formål å konvertere ulovlige midler til lovlige midler. Terrorfinansiering har imidlertid som formål å anvende midler (lovlige eller ulovlige) til ulovlige formål (Finansdepartementet:2004 – A).

2.2 DE VIKTIGSTE PUNKTENE I LOVEN

Hovedhensikten med hvitvaskingslovverket er å begrense finansiering av terror ved hjelp av hvitvasking som middel. Da terrorfinansiering er såpass omfangsrikt og får store konsekvenser for samfunnet på tvers av landegrensene er det ved nettopp terrorfinansiering hovedfokus ligger. De viktigste punktene i hvitvaskingslovverket er:

Hvitvaskingsloven § 5 fastsetter hovedprinsippene i det nye regelverket om risikobasert kundekontroll og løpende oppfølging:

> *§ 5. Risikobasert kundekontroll og løpende oppfølging*
>
> *Rapporteringspliktige skal foreta kundekontroll etter §§ 6 til 13 og løpende oppfølging etter § 14. Kundekontroll og løpende oppfølging skal foretas på grunnlag av en vurdering av risiko for transaksjoner med tilknytning til utbytte av straffbare handlinger eller forhold som rammes av straffeloven §§ 147 a, 147 b eller 147 c, der risikoen vurderes ut fra type kunde, kundeforhold, produkt eller transaksjon. (Se avsnitt 2.2.1 for nærmere info om staffelovens § 147).*
>
> *Rapporteringspliktige skal kunne påvise at omfanget av utførte tiltak er tilpasset den aktuelle risiko.*

Rapporteringspliktige pålegges i § 5 en plikt til å foreta en risikobasert kundekontroll der omfanget og intensiteten av kundekontrolltiltakene tilpasses antatt risiko for hvitvasking og terrorfinansiering. Det innebærer at institusjonene pålegges omfattende plikter med hensyn til å gjennomføre risikobaserte og skjønnsmessige vurderinger. Regelverket innebærer skjerpede tiltak mot hvitvasking og terrorfinansiering, og at ressursene skal brukes der risikoen for hvitvasking og terrorfinansiering er størst (Finanstilsynet:2009).

Hvitvaskingsloven kapittel 2 ”Kundekontroll og løpende oppfølging”, og hvitvaskingsforskriften kapittel 2 fastsetter flere konkrete kundekontrolltiltak, og inneholder nye bestemmelser som innebærer en vesentlig utvidelse og presisering av regelverket i forhold til den tidligere hvitvaskingslovens krav om identitetskontroll, som ikke hadde en slik risikodifferensiert tilnærming (Finanstilsynet:2009).

Identitetskontroll er erstattet med den utvidede plikten til å foreta kundekontroll ("Customer due diligence" – CDD). Regelverket bygger på det såkalte kjenn din kunde-prinsippet som internasjonalt anses for å være et av de viktigste virkemidlene for å forhindre at det finansielle systemet misbrukes til hvitvasking eller terrorfinansiering (Finanstilsynet:2009).

Risikobasert kundekontroll vil ofte kunne innebære tre ulike hovednivåer for kundekontrolltiltak tilpasset antatt risiko for hvitvasking og terrorfinansiering. Her vil det imidlertid kunne være store individuelle forskjeller fra foretak til foretak og fra bransje til bransje:

- "Forsterkede kontrolltiltak" i situasjoner med antatt høy/forhøyet risiko for hvitvasking og terrorfinansiering. Det vises her til hvitvaskingsloven § 15, § 16 og § 7 fjerde ledd, og forskriften § 11.
- "Forenklet kundekontroll" i situasjoner med antatt lav risiko for hvitvasking og terrorfinansiering. Det vises her til hvitvaskingsloven § 13 og forskriften § 10.
- Normal kundekontroll i situasjoner med verken høy eller lav risiko for hvitvasking og terrorfinansiering.

Det fremgår av hvitvaskingsloven § 5 annet ledd at rapporteringspliktige skal kunne påvise at omfanget av utførte tiltak er tilpasset den aktuelle risiko. Dette er en ny bestemmelse i hvitvaskingsregelverket. Det er meget viktig at den enkelte rapporteringspliktige overfor tilsynsmyndighetene kan klart påvise at den operasjonelle risiko, som hvitvasking og terrorfinansiering innebærer, er konkret vurdert og tilstrekkelig tatt hensyn til ved omfanget og intensiteten av kundekontrolltiltakene. Loven § 23 første ledd fastsetter videre at rapporteringspliktige skal ha forsvarlige interne kontroll- og kommunikasjonsrutiner som sikrer oppfyllelse av pliktene i loven. Disse rutinene skal forelegges for og fastsettes på øverste nivå hos den rapporteringspliktige, jf. hvitvaskingsloven § 23 annet ledd (Finanstilsynet:2009).

2.2.1 STRAFFELOVENS §§ 147 – LOV MOT TERROR

§ 147a. *En straffbar handling som nevnt i §§ 148, 151 a, 151 b første ledd jf. tredje ledd, 152 annet ledd, 152 a annet ledd, 152 b, 153 første til tredje ledd, 153 a, 154, 223 annet ledd, 224, 225 første eller annet ledd, 231 jf. 232, eller 233 anses som en terrorhandling og straffes med fengsel inntil 21 år når handlingen er begått med det forsett*

a) å forstyrre alvorlig en funksjon av grunnleggende betydning i samfunnet, som for eksempel lovgivende, utøvende eller dømmende myndighet, energiforsyning, sikker forsyning av mat eller vann, bank- og pengevesen eller helseberedskap og smittevern,
b) å skape alvorlig frykt i en befolkning, eller
c) urettmessig å tvinge offentlige myndigheter eller en mellomstatlig organisasjon til å gjøre, tåle eller unnlate noe av vesentlig betydning for landet eller organisasjonen, eller for et annet land eller en annen mellomstatlig organisasjon.

Straffen kan ikke settes under minstestraffen som er bestemt i straffebudene som er nevnt i første punktum.

Med fengsel inntil 12 år straffes den som med slikt forsett som nevnt i første ledd, truer med å begå en straffbar handling som nevnt i første ledd, under slike omstendigheter at trusselen er egnet til å fremkalle alvorlig frykt. Får trusselen en følge som nevnt i første ledd bokstavene a, b eller c, kan fengsel inntil 21 år idømmes. Medvirkning straffes på samme måte.

Med fengsel inntil 12 år straffes den som planlegger eller forbereder en terrorhandling som nevnt i første ledd, ved å inngå forbund med noen om å begå en slik handling.

§ 147b. *Med fengsel inntil 10 år straffes den som fremskaffer eller samler inn penger eller andre formuesgoder, med det forsett at formuesgodene helt eller delvis skal finansiere terrorhandlinger eller andre overtredelser av § 147 a.*

På samme måte straffes den som stiller penger eller andre formuesgoder, eller banktjenester eller andre finansielle tjenester til rådighet for

a) en person eller et foretak som begår eller forsøker å begå lovbrudd som nevnt i § 147 a,
b) et foretak som noen som nevnt i bokstav a eier eller har kontroll over, eller
c) et foretak eller en person som handler på vegne av eller på instruks fra noen som nevnt i bokstavene a eller b.

Medvirkning straffes på samme måte.

§ 147c. *Med fengsel inntil 6 år straffes den som*

a) offentlig oppfordrer noen til å iverksette en handling som nevnt i §§ 147 a første eller annet ledd eller 147 b første eller annet ledd med hensikt om slike følger som beskrevet i § 147 a første ledd bokstav a til c, eller lov 20. mai 2005 nr. 28 §§ 138 til 144,

b) rekrutterer noen til å begå en handling som nevnt i §§ 147 a første eller annet ledd eller 147 b første eller annet ledd med hensikt om slike følger som beskrevet i § 147 a første ledd bokstav a til c, eller lov 20. mai 2005 nr. 28 §§ 138 til 144, eller

c) gir opplæring i metoder eller teknikker som er særlig egnet til å utføre eller bidra til utførelsen av en handling som nevnt i §§ 147 a første eller annet ledd eller 147 b første eller annet ledd, med hensikt om slike følger som beskrevet i § 147 a første ledd bokstav a til c, eller lov 20. mai 2005 nr. 28 §§ 138 til 144, med forsett om at ferdighetene skal brukes til dette.

Består handlingen i fremsettelse av et budskap, er den også offentlig når budskapet er fremsatt på en måte som gjør det egnet til å nå et større antall personer.

Medvirkning straffes på samme måte.

Kilde: www.lovdata.no

2.2.2 DEFINISJON AV RAPPORTERINGSPLIKTIG

2.2.2.1 HVEM ER RAPPORTERINGSPLIKTIG

Hvitvaskingslovens § 4 gir en oversikt over hvem som faller inn under loven som rapporteringspliktig til ØKOKRIM:

Loven gjelder for følgende virksomheter og juridiske personer:

- Finansinstitusjoner,
- Norges Bank,
- e-pengeforetak,
- Foretak og personer som driver virksomhet som består i overføring av penger eller pengefordringer,
- Verdipapirforetak,
- Forvaltningsselskaper for verdipapirfond,
- Forsikringsselskap,

- Pensjonskasser,
- Postoperatører ved formidling av postsendinger,
- Verdipapirregistre,
- Andre foretak hvis hovedvirksomhet er omfattet av punktene 2 til 12 og 14 i vedlegg I til direktiv 2000/12/EF om adgang til å starte og utøve virksomhet som kredittinstitusjon, herunder utlånsvirksomhet, fondsmegling, betalingsformidling, finansiell leasing, rådgivnings eller andre tjenester knyttet til finansielle transaksjoner samt utleie av bankbokser.

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

- Statsautoriserte og registrerte revisorer,
- Autoriserte regnskapsførere,
- Eiendomsmeglere og boligbyggelag når det drives eiendomsmegling,
- Forsikringsmeglere,
- Prosjektmeglere,
- Valutameglere,
- Advokater og andre som ervervsmessig eller stadig yter selvstendig juridisk bistand, når de bistår eller opptrer på vegne av klienter ved planlegging eller utførelse av finansielle transaksjoner eller transaksjoner som gjelder fast eiendom eller løsøregjenstander som nevnt i nr. 8;
- Forhandlere av gjenstander, herunder auksjonsforretninger, kommisjonærer og lignende, ved transaksjoner i kontanter på 40 000 norske kroner eller mer eller et tilsvarende beløp i utenlandsk valuta. Transaksjoner med betalingskort omfattes kun når det er bestemt i forskrift fastsatt av departementet;
- Personer og foretak som mot vederlag tilbyr tilsvarende tjenester som nevnt i nr. 1 til 8.

Loven gjelder også for foretak og personer som utfører tjenester på vegne av eller for rapporteringspliktige. Departementet kan i forskrift fastsette regler som gir loven anvendelse for spillvirksomhet, inkassoforetak og regulerte markeder (www.hvitvasking.no – D).

2.2.2.2 NÅR SKAL DET RAPPORTERES

Dersom det oppstår mistanke om at en transaksjon har tilknytning til utbytte av en straffbar handling eller til forhold som rammes av straffeloven § 147 a eller § 147 b, skal det foretas undersøkelser for å få bekreftet eller avkreftet mistanken.

Dersom undersøkelsene ikke kan avkrefte mistanken skal opplysninger om den aktuelle transaksjonen og de forhold som har medført mistanke oversendes til ØKOKRIM i form av en MT-rapport så snart som mulig.

Oversendelse av en MT-rapport ikke er en politianmeldelse. Formålet med rapporteringsplikten er å gjøre det enklere å avdekke profittmotivert kriminalitet og å hindre at finansinstitusjoner og andre rapporteringspliktige misbrukes i hvitvaskingssammenheng. De rapportene ØKOKRIM mottar, blir analysert ved Enheten for finansiell etterretning. Opplysningene i rapportene bearbeides for å gjøre dem tilgjengelig for sentrale og lokale politiorganer, andre kontrollmyndigheter, eller andre lands hvitvaskingsenheter. De bearbeidede opplysningene videreformidles så i form av etterretningsrapporter, analyser eller anmeldelser. Rapportene ØKOKRIM mottar fra rapporteringspliktige danner derfor et grunnlag for mulighetene til å kunne avdekke denne type kriminalitet. De impliserte i rapporten får ikke, og skal ikke ha, informasjon om at vedkommende er rapportert til EFE/ØKOKRIM. Det er først når det er åpnet straffesak og personen får status som mistenkt, at vedkommende får vite om at det foretas undersøkelser (www.hvitvasking.no – E).

2.2.2.3 STRAFF FOR MANGLENDE RAPPORTERING

Overtredelse av hvitvaskingsloven kan gi bøter, eller i særlig skjerpende omstendigheter kan fengsel inntil 1 år anvendes, jfr. hvitvaskingsloven § 28.

Dersom rapporteringspliktig er en del av en hvitvaskingsoperasjon, både uaktsomt eller med hensikt, kan vedkommende straffes for hvitvaskning, jfr. Straffeloven § 317:

"Den som mottar eller skaffer seg eller andre del i utbytte av en straffbar handling, eller som yter bistand til å sikre slikt utbytte for en annen, straffes for heleri …"

"Som å yte bistand regnes blant annet det å innkreve, oppbevare, skjule, transportere, sende, overføre, konvertere, avhende, pantsette eller la investere."

Strafferammen er bøter eller fengsel inntil 2 år for uaktsomt heleri, bøter eller fengsel inntil 3 år for forsettelig heleri og fengsel i inntil 6 år for grovt heleri (www.hvitvasking.no – F).

2.3 HVA ER NYTT I REVISJON 2009

Ny hvitvaskingslov og tilhørende forskrift trådte i kraft 15. april 2009. Den viktigste endringen i det nye regelverket er innføring av risikobasert kundekontroll og løpende oppfølging. Kravet om personlig fremmøte ved identitetskontrollen er erstattet av risikobaserte kundekontrolltiltak. Plikten til å foreta kundekontroll går vesentlig lenger enn identitetskontrollen i det tidligere hvitvaskingsregelverket. Kundekontroll omfatter registrering av kundeopplysninger, bekreftelse av kundens identitet og identiteten til eventuelle reelle rettighetshavere, samt innhenting av opplysninger om kundeforholdets formål og tilsiktede art. Kundeforhold med antatt høy risiko for hvitvasking og terrorfinansiering utløser forsterkede kontrolltiltak. Omfanget og intensiteten av kundekontrolltiltakene beror på en konkret risikobasert vurdering. Det gis adgang til å bruke elektronisk legitimasjon i tillegg til fysisk legitimasjon. All rapportering av mistenkelige transaksjoner til Økokrim skal skje elektronisk via Altinn. Pensjonskasser omfattes ikke lenger av kretsen av rapporteringspliktige. Utover de forannevnte endringene, er regelverket i stor grad en videreføring av det tidligere regelverket på området (Finanstilsynet:2009).

Det nye hvitvaskingsregelverket omfatter lov 6. mars 2009 nr. 11 om tiltak mot hvitvasking og terrorfinansiering mv., og forskrift 13. mars 2009 nr. 303 om kontrollutvalget for tiltak mot hvitvasking (Finanstilsynet:2009).

Lovforarbeidene er viktige kilder til å forstå reglene. De viktigste forarbeidene er NOU 2007: 10, Ot.prp.nr 3 (2008-2009), samt innst.O.nr. 42 (2008-2009). Disse omtales også henholdsvis som Utredningen, Proposisjonen og Innstillingen.

Innholdet i hvitvaskingsregelverket kan deles inn i tre hovedplikter:

- Plikt for rapporteringspliktige til å foreta risikobasert kundekontroll, samt plikt for institusjonene til å oppbevare kopi av legitimasjonsdokumentene, eventuell referanse til elektronisk legitimasjon samt transaksjonsopplysninger.
- Plikt til å foreta løpende oppfølging av kundeforhold og transaksjoner, samt undersøke mistenkelige transaksjoner og plikt til å rapportere til Økokrim elektronisk via Altinn dersom mistanken ikke avkreftes ved nærmere undersøkelser.
- Plikt for rapporteringspliktige til å etablere forsvarlige interne kontroll- og kommunikasjonsrutiner, iverksette opplæringsprogrammer og utpeke særskilt person på øverste nivå hos den rapporteringspliktige med ansvar for å følge opp disse rutinene.

Den nye loven og forskriften avløser lov 20. juni 2003 nr. 41 om tiltak mot hvitvasking av utbytte fra straffbare handlinger mv. (hvitvaskingsloven) og tilhørende forskrift 10. desember 2003 nr. 1487 (Finanstilsynet:2009).

2.3.1 PLIKTEN TIL Å FORETA KUNDEKONTROLL

Hvitvaskingsloven § 6 fastsetter hvilke situasjoner som utløser kundekontroll.

> *§ 6. Plikt til å foreta kundekontroll*
>
> *Rapporteringspliktige skal foreta kundekontroll ved*
>
> *1. Etablering av kundeforhold*
>
> *2. Transaksjon som gjelder 100 000 norske kroner eller mer, for kunde som den rapporteringspliktige ikke har et etablert kundeforhold til.*
>
> *3. Mistanke om at en transaksjon har tilknytning til utbytte av straffbar handling eller forhold som rammes av straffeloven §§ 147 a, 147 b eller 147 c*
>
> *4. Tvil om hvorvidt tidligere innhentede opplysninger om kunden er korrekte eller tilstrekkelige.*
>
> *Beløpsgrensen i første ledd nr. 2 beregnes samlet for transaksjoner som gjennomføres i flere operasjoner som ser ut til å kunne ha sammenheng med hverandre. Dersom beløpet*

ikke er kjent når transaksjonen gjennomføres, skal kundekontrollen foretas så snart den rapporteringspliktige blir kjent med at beløpsgrensen er oversteget.

Departementet kan i forskrift fastsette nærmere regler om når kundeforhold skal anses etablert.

Lovbestemmelsens tre første alternativer samsvarer med den tidligere hvitvaskingslovens legitimasjonskontroll. Alternativ nr. 4 "tvil om hvorvidt tidligere innhentede opplysninger om kunden er korrekte eller tilstrekkelige", er en ny situasjon som utløser krav om kundekontroll (Finanstilsynet:2009).

Kundekontroll foretas ved "etablering av kundeforhold". Loven forutsetter altså at man kan være kunde uten at det etableres et kundeforhold. For slike "leilighetskunder" som faller under terskelen for etablert kundeforhold er det bare ved transaksjoner over 100 000 kroner eller ved mistanke, det skal foretas kundekontroll, jf. nr. 2 og 3. Hvorvidt det er etablert et kundeforhold i lovens forstand vil bero på en konkret vurdering, hvor blant annet forholdets varighet, art og formål vil være momenter av betydning. Dersom det opprettes en forbindelse av en viss varighet, vil det i de aller fleste tilfeller være opprettet et kundeforhold. Kortvarige forbindelser vil imidlertid også kunne anses som etablering av kundeforhold. I Utredningen nevnes som eksempel at opprettelse av bankkonto i alle tilfeller anses som etablering av kundeforhold, selv om det ved opprettelsen er klart at kontoen vil benyttes i et enkeltstående tilfelle og avsluttes etter kort tid. Enkeltstående innskudd av kontanter eller betaling av giro i en bank, uten at det skal opprettes bankkonto i en bank, vil ikke innebære etablering av kundeforhold (Finanstilsynet:2009).

Det er fra regjeringen reist spørsmål om tolkningen av uttrykket "kundeforhold" i forhold til kausjonister og garantister. Kredittilsynet legger til grunn at kausjonister og garantister ikke faller inn under begrepet kunde i hvitvaskingsloven, og dermed ikke omfattes av de formelle kravene til kundekontroll i hvitvaskingsregelverket. På annet grunnlag enn hvitvaskingsregelverket må imidlertid den rapporteringspliktige vite hvem kausjonist eller garantist er (Finanstilsynet:2009).

2.3.2 GJENNOMFØRING AV KUNDEKONTROLLEN

Hvitvaskingslovens § 7 første ledd fastsetter fire konkrete kundekontrolltiltak:

> *§ 7. Gjennomføring av kundekontroll*
>
> *Kundekontroll som nevnt i § 6 skal omfatte*
>
> *1. registrering av opplysninger som nevnt i § 8,*
>
> *2. bekreftelse av kundens identitet på grunnlag av gyldig legitimasjon,*
>
> *3. bekreftelse av identiteten til reelle rettighetshavere på grunnlag av egnede tiltak, og*
>
> *4. innhenting av opplysninger om kundeforholdets formål og tilsiktede art.*

Hovedregelen er at de nevnte kundekontrolltiltakene skal gjennomføres *før* etablering av kundeforholdet, eller gjennomføring av transaksjoner i henhold til loven § 6 nr. 2 og 3. Det vises her til hvitvaskingsloven § 9 første ledd (Finanstilsynet:2009).

Kredittilsynet legger til grunn at som hovedregel skal kundekontrolltiltak 1,2 og 4 gjennomføres ved samtlige kundeforhold med unntak av kundeforhold som omfattes av "Forenklet kundekontroll". Omfanget og intensiteten av de aktuelle kontrolltiltakene beror på en konkret risikobasert vurdering, jf. loven § 5 første ledd (Finanstilsynet:2009).

2.3.2.1 KUNDEKONTROLLTILTAK NR. 1

Kundekontrolltiltak nr. 1 fastsetter et krav om å identifisere kunden ved "registrering av opplysninger". Plikten til å registrere opplysninger følger av § 8:

> *§ 8. Registrering av opplysninger*
>
> *Rapporteringspliktige skal registrere følgende opplysninger om kunder:*
>
> *1. Fullt navn eller foretaksnavn,*
>
> *2. fødselsnummer, organisasjonsnummer, D-nummer eller, dersom kunden ikke har slikt nummer, annen entydig identitetskode,*
>
> *3. Fast adresse, og*

4. referanse til legitimasjon som er brukt for å bekrefte kundens identitet.

Plikten til å registrere kundens faste adresse etter første ledd nr. 3 gjelder ikke dersom folkeregisteret har vedtatt at kundens adresse skal være fortrolig eller strengt fortrolig.

Hvitvaskingsregelverket fastsetter ikke noen formkrav til hvordan slik registrering skal skje. Registreringen kan således basere seg på så vel muntlige som skriftlige opplysninger fra kunden til den rapporteringspliktige. Skriftlige opplysninger fra kunden vil imidlertid oftest være en forutsetning for å kunne ettervise at risikovurdering og kundekontrolltiltak faktisk er gjennomført (Finanstilsynet:2009).

Den nevnte registreringsplikten innebærer at kunden som hovedregel identifiseres entydig. Regelverket om registrering av kundeopplysninger er stort sett en videreføring av den tidligere reguleringen på området. Proposisjonens side 49 utdyper dette; "registrering av opplysninger, vil gi mindre rom for risikobaserte tiltak, enn andre kundekontrolltiltak". I tilfelle hvor det er reelle rettighetshavere på eiersiden hos en kunde, vil det imidlertid være en risikobasert vurdering med hensyn til "hvilke opplysninger som er nødvendige i det konkrete tilfellet. Departementet antar at opplysninger som skal registreres om kunden etter lovforslaget § 8 ofte vil være aktuelle også med hensyn til reelle rettighetshavere." (Finanstilsynet:2009).

2.3.2.2 KUNDEKONTROLLTILTAK NR. 2

Kundekontrolltiltak nr. 2 fastsetter at kundens identitet deretter skal bekreftes (verifiseres) "på grunnlag av gyldig legitimasjon". Kravet til å bekrefte identiteten er ufravikelig. Omfanget og intensiteten av kundekontrolltiltaket, er imidlertid risikobasert (Finanstilsynet:2009).

Hvitvaskingsforskriften § 5 fastsetter nærmere krav som gjelder for "Fysisk legitimasjon for fysiske personer". Forskriften § 6 fastsetter de krav som gjelder for "Elektronisk legitimasjon for fysiske personer" (Finanstilsynet:2009).

Hvitvaskingsloven legger til rette for likestilling mellom elektronisk og fysisk legitimasjon for fysiske personer. De nærmere bestemmelsene om elektronisk legitimasjon er gitt i hvitvaskingsforskriften § 6. Elektronisk legitimasjon er etter forskriften bare aktuelt for fysiske personer (Finanstilsynet:2009).

Hvitvaskingsforskriften § 5.

> *§ 5. Fysisk legitimasjon for fysiske personer*
>
> *Gyldig legitimasjon for fysisk person er original av dokumenter som:*
>
> *1. er utstedt av offentlig myndighet, eller av et annet organ som har betryggende kontrollrutiner for dokumentutstedelse og dokumentene har et tilfredsstillende sikkerhetsnivå, og*
>
> *2. Inneholder fullt navn, navnetrekk, fotografi og fødselsnummer eller D-nummer.*
>
> *For fysiske personer som ikke har fått tildelt norsk fødselsnummer eller D-nummer, skal legitimasjonsdokumenter i tillegg til de kravene som følger av i første ledd inneholde fødselsdato, fødested, kjønn og statsborgerskap.*
>
> *Dersom bekreftelse av en fysisk persons identitet skal skje på grunnlag av fysisk legitimasjon uten vedkommendes personlige fremmøte i tråd med hvitvaskingsloven § 7 fjerde ledd, kan bekreftet kopi av dokumenter som nevnt i første og annet ledd benyttes.*
>
> *Krav om at fysisk legitimasjon for fysiske personer inneholder navnetrekk gjelder ikke for pass.*

I tilfeller hvor kunden møter personlig hos rapporteringspliktig, eller foretak rapporteringspliktige utkontrakterer kontrollen til, vil normalt bekreftelsen av kundens identitet skje samtidig (Finanstilsynet:2009).

Finanstilsynet antar at følgende legitimasjonsdokumenter i alle fall vil tilfredsstille lovkravene:

- Gyldig pass eller annet godkjent reisedokument
- Bankkort (norsk)
- Førerkort – original og duplikat (dog ikke førerkort av eldre dato – "grønt førerkort")
- Forsvarsdepartementets ID-kort
- Postens ID-kort utstedt etter 1. oktober 1994
- Nasjonale ID-kort utstedt innenfor EØS-området. Det vises her til forskrift 21. desember 1990 nr. 1028 om utlendingers adgang til riket og

> deres opphold her (utlendingsforskriften) Vedlegg 2 Godkjente identitetsdokumenter.

Begrepet "gyldig legitimasjon" er i utvikling, og opplistingen forsøker ikke å være uttømmende. Den endelige vurderingen hvorvidt legitimasjonen identifiserer kunden på en sikker måte må foretas av rapporteringspliktig (Finanstilsynet:2009).

Det henvises til Forskriftens § 6 for mer informasjon vedrørende elektronisk ID.

2.3.2.3 KUNDEKONTROLLTILTAK NR. 3

Kundekontrolltiltak nr. 3 innfører begrepet reelle rettighetshavere.

Begrepet reelle rettighetshavere er definert i hvitvaskingsloven § 2 første ledd nr. 3:

> *reelle rettighetshavere: fysiske personer som i siste instans eier eller kontrollerer en kunde eller som en transaksjon gjennomføres på vegne av.*

Det er kun fysiske personer som kan være reell rettighetshaver. Uttrykket i *siste instans* viser til at det kan være en kjede av personer, fysiske eller juridiske, som leder til den reelle rettighetshaver (Finanstilsynet:2009).

Når en *fysisk person* er kunde vil som oftest han eller hun også være den reelle rettighetshaver, og kundekontrollen gjøres av denne personen. Hvis en kunde handler på vegne av en annen fysisk person, vil det være sistnevnte som er reell rettighetshaver (Finanstilsynet:2009).

Dersom det er en *juridisk person* som er kunde, kan det være fysiske personer som står bak som kvalifiserer til å være reell rettighetshaver. En fysisk person skal etter hvitvaskingsloven § 2 første ledd nr. 3 i alle tilfelle regnes som reell rettighetshaver dersom vedkommende:

> *a) direkte eller indirekte eier eller kontrollerer mer enn 25 prosent av eierandelene eller stemmene i et selskap, unntatt selskap som har finansielle instrumenter opptatt til notering på et regulert marked i EØS-stat eller er underlagt informasjonsplikt tilsvarende det som gjelder ved notering på et regulert marked i EØS-stat.*
>
> *b) utøver kontroll over ledelsen av en juridisk person på annen måte enn nevnt i bokstav a,*

c) ifølge vedtekter eller på annet grunnlag skal motta 25 prosent eller mer av formuesgodene i en stiftelse, et fond eller en tilsvarende juridisk person eller formuesmasse,

d) har hovedinteressen av opprettelsen eller forvaltningen av en stiftelse, et fond eller en tilsvarende juridisk person eller formuesmasse, eller

e) utøver kontroll over mer enn 25 prosent av formuesgodene i en stiftelse, et fond eller en lignende juridisk person eller formuesmasse.

2.3.2.4 KUNDEKONTROLLTILTAK NR. 4

Kundekontrolltiltak nr. 4 om kundeforholdets "Formål og tilsiktede art" er et nytt krav i hvitvaskingslovgivningen for å fremskaffe nærmere opplysninger om kundeforholdet blant annet for å kunne risikotilpasse kundekontrolltiltakene. Tiltaket inngår som en viktig del av "kjenn din kunde"-prinsippet (Finanstilsynet:2009).

Slike opplysninger om kundeforholdet er også av stor betydning for å kunne *"løpende følge opp eksisterende kundeforhold, herunder påse at transaksjoner som den rapporteringspliktige blir kjent med er i samsvar med den rapporteringspliktiges kjennskap til kunden og dens virksomhet."* Det vises her til hvitvaskingsloven § 14 og kravet om "Løpende oppfølging", som også er en ny bestemmelse i hvitvaskingsregelverket (Finanstilsynet:2009).

Hva slags opplysninger som skal innhentes her, vil måtte bero på en konkret risikobasert vurdering. For kundeforhold med antatt lav til middels risiko for hvitvasking og terrorfinansiering, for eksempel en normal lønnsmottaker og næringsdrivende, student eller pensjonist som har et regelmessig og forutsigbart transaksjonsmønster, vil det etter en konkret vurdering kunne være tilstrekkelig at det registreres for eksempel "brukskonto med betalingsformidling, lån og sparing, forsikring". Denne kundegruppen utgjør en vesentlig del av kundemassen og transaksjonsvolumet i de fleste finansinstitusjoner. Som hovedregel vil det ikke her være påkrevet en mer "detaljert og finmasket" inndeling av disse kundegruppene, for eksempel når det gjelder ulike typer spare- og forsikringsklasser, betalingsmønster, beløpsstørrelse osv. Det vil heller ikke her være naturlig å innhente detaljerte opplysninger om inntekt, formue, arbeidsgiver osv. Rapporteringspliktige må imidlertid etter en konkret vurdering innhente tilstrekkelige kundeopplysninger som

muliggjør "løpende oppfølging" i henhold til lovens § 14. Banker og finansieringsselskaper har et lovpålagt krav om elektronisk overvåkning av transaksjoner. Slik overvåkning vil være et viktig hjelpemiddel for å foreta den "løpende oppfølgingen" av kundeforhold og transaksjoner. De transaksjoner som disse systemene identifiserer som mistenkelige, atypiske, unormale, må etter en konkret vurdering følges opp manuelt (Finanstilsynet:2009).

2.3.3 KONTROLL AV REELLE RETTIGHETSHAVERE

Det er ikke tilstrekkelig for å regnes som reell rettighetshaver at man har en ledende stilling i et selskap eller annen juridisk person. Personer i ledelsen kan likevel være reell rettighetshaver i kraft av å være eier eller ha en annen posisjon som nevnt i bokstavene a) til e) i punkt 2.3.2.3

Hvitvaskingsregelverket skiller mellom *identifisering* og *bekreftelse av identiteten*. Identifiseringen skjer ved å innhente informasjon om kunden/rettighetshaveren. Bekreftelsen av identiteten består i å sjekke hele eller deler av denne informasjonen opp mot troverdige kilder. Identifisering og bekreftelsen av identiteten kan skje i to atskilte faser, som når kunden oppgir en adresse, som så kontrolleres i et register. Ofte vil de to operasjonene foregå samtidig, som for eksempel når kunden legger fram et pass eller førerkort (Finanstilsynet:2009).

Hvitvaskingsloven forutsetter at den rapporteringspliktige gjennomfører en kundekontroll som omfatter det å undersøke om det står reelle rettighetshavere bak en kunde. Dette er et utslag "kjenn din kunde" – prinsippet (Finanstilsynet:2009).

2.3.4 BEKREFTELSE AV IDENTITET

Hvitvaskingsloven § 7 slår fast at identiteten til reelle rettighetshavere skal bekreftes på grunnlag av *egnede tiltak.* Bekreftelsen (verifiseringen) av identiteten til reelle rettighetshavere skal gjøres på grunnlag av en risikovurdering (Finanstilsynet:2009).

Ved kontrollen av kunder gir hvitvaskingsloven og – forskriften kvalitative krav til legitimasjonsbevis ved at det stilles krav om gyldig legitimasjon. Et tilsvarende formelt krav gjelder ikke for bekreftelse av identiteten til reelle rettighetshavere (Finanstilsynet:2009).

Foretak og virksomheter, som ikke har lovpålagt plikt til elektronisk overvåkning, må etablere betryggende manuelle rutiner, eventuelt kombinert med elektroniske løsninger dersom en risikobasert vurdering tilsier det (Finanstilsynet:2009).

2.3.5 KUNDEFORHOLD MED HØY RISIKO

Når det gjelder kundeforhold med antatt høy risiko for hvitvasking eller terrorfinansiering, eksempelvis foretak med komplisert selskaps- og eierstruktur uten at det er noen fornuftig grunn for en slik organisering av virksomheten, kan det etter en konkret risikobasert vurdering være påkrevet å be kunden fremskaffe utdypende opplysninger om eksempelvis næringsvirksomhetens art, omfang og eierforhold. Eksempler på dette kan være nærmere opplysninger fra regnskap og selvangivelser. Hva som er "kilden og opprinnelsen" til de aktuelle midlene som skal plasseres, vil ofte være helt sentrale opplysninger her (Finanstilsynet:2009).

Finanstilsynet legger til grunn at rapporteringspliktige som hovedregel internt registrerer sine kunder ved å benytte fødselsnummer og organisasjonsnummer som kundenummer, jf. hvitvaskingsloven § 8 nr. 2. Kunder som ikke omfattes av de forannevnte kategoriene, for eksempel ikke er registreringspliktige i offentlige registre (lag, foreninger osv.) kan registreres på såkalt konstruert kundenummer. Dersom rapporteringspliktige viderefører praksisen med å registrere et kundeforhold på en fysisk person, for eksempel stifter, kasserer, disponent, vil Finanstilsynet ikke ha noen innsigelser mot en slik praksis (Finanstilsynet:2009).

2.4 HVITVASKINGSARBEID INTERNASJONALT

2.4.1 HVORDAN DET INTERNASJONALE ARBEIDET ER ORGANISERT

Det internasjonale arbeidet er hovedsaklig organisert gjennom FATF (Financial Action Task Force) gjennom FIU (Financial Intelligence Unit) enheter. FATF anbefaler alle land å opprette nasjonale etterretningssentre for mottak, analyse og videreformidling av finansiell informasjon knyttet til mulig hvitvasking og finansiering av terrorisme. (EFE:2010)

2.4.1.1 DE FØRSTE INITIATIVENE

Bekjempelse av hvitvasking er et relativt nytt samarbeidsområde i internasjonal sammenheng, og standarder for tiltak som er implementert i nasjonale lovverk rundt om i verden har sitt utspring i initiativer som forelå først på slutten av 1980-tallet. Bekjempelse av terrorfinansiering ble satt på den internasjonale agendaen etter terroranslagene i USA 11. sepember 2001 (www.hvitvasking.no – C).

2.4.1.2 EUS TREDJE HVITVASKINGSDIREKTIV

EUs tredje hvitvaskingsdirektiv ble vedtatt 26. oktober 2005 og publisert i Official Journal 25. november 2005. Som i de tidligere hvitvaskingsdirektiver er medlemsstatene gitt adgang til å fastsette strengere regler enn det som følger av direktivet. Frist for gjennomføring i nasjonal rett var 15. desember 2007. Direktivet ble inntatt i EØS-avtalen ved EØSkomiteens beslutning nr. 87/2006 av 7. juli 2006. EØS-komiteens beslutning ble godkjent av Stortinget 19. desember 2006. Hovedformålet med tredje hvitvaskingsdirektiv er å forhindre hvitvasking av penger og terrorfinansiering, ved et felles regelverk som er forenlig med den øvrige fellesskapsretten. Regelverket skal blant annet hindre misbruk av den frie kapitalbevegelse og adgangen til å yte finansielle tjenester, og forebygge at stabiliteten og omdømmet til det finansielle system skades. Sentrale virkemidler er plikt til kundeidentifikasjon og registrering av kundeopplysninger, undersøkelsesplikt og rapporteringsplikt for finansinstitusjoner og andre som utøver virksomhet som i særlig grad kan tenkes å bli brukt til hvitvasking og terrorfinansiering (NOU:10 2007).

Det tredje hvitvaskingsdirektiv erstatter direktiv 91/308/EØF (første hvitvaskingsdirektiv) og endringsdirektiv 2001/97/EF (annet hvitvaskingsdirektiv), som er en del av EØS-avtalen. Tredje hvitvaskingsdirektiv er dels en revisjon og dels en videreutvikling av de foregående hvitvaskingsdirektiver. Anvendelsesområdet etter tredje hvitvaskingsdirektiv er utvidet ved at direktivet også retter seg mot terrorfinansiering. Kretsen av pliktsubjekter er utvidet, blant annet ved at forsikringsformidlingsforetak og tilbydere av visse tjenester til truster og selskaper omfattes. Definisjonen av finansinstitusjon er utvidet ved at man har fjernet formuleringen «whose principal activity is» ved henvisning til aktiviteter som nevnt i vedlegg I til direktiv 2000/12/EF (det konsoliderte bankdirektiv). Kravene til

kundekontroll er spesifisert og utvidet, blant annet med krav om identifisering av fysiske personer som eier eller kontrollerer kunden eller som kunden handler på vegne av. Det stilles krav om løpende oppfølging av etablerte kundeforhold. Kundekontroll og løpende oppfølging skal foretas på grunnlag av en risikovurdering, og regelverket åpner i større grad for relativisering av kundekontrollen. Det åpnes også for å legge til grunn kundekontroll gjennomført av tredjeparter. Det er uttrykkelig inntatt forbud mot å etablere kundeforhold eller utføre en transaksjon, samt plikt til å avvikle eksisterende kundeforhold, dersom det ikke er mulig å gjennomføre kundekontroll. Det er innført forbud mot å etablere anonyme bankkonti og forbud mot å ha korrespondentbankforbindelse med tomme bankselskaper (såkalte «shell banks»). Når det gjelder rapporteringsplikten til «financial intelligence unit» (Økokrim, EFE), er det gitt enkelte unntak fra forbudet mot å opplyse tredjepersoner om at rapport er sendt. Tredje hvitvaskingsdirektiv bærer gjennomgående preg av større detaljregulering enn første og annet hvitvaskingsdirektiv (NOU:10 2007).

I flere bestemmelser i tredje hvitvaskingsdirektiv er det gitt hjemmel for Kommisjonen til å fastsette utfyllende rettsakter. Dette er gjort ved kommisjonsdirektiv 2006/70/EF, som ble vedtatt 1. august 2006 og publisert i Official Journal 4. august 2006 (kommisjonsdirektivet). Frist for gjennomføring i nasjonal rett var 15. desember 2007. Kommisjonsdirektivet ble inntatt i EØS-avtalen ved EØSkomiteens beslutning nr. 152/2006 av 8. desember 2006 (NOU:10 2007).

2.4.1.2 WIENKONVENSJONEN

FNs "Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances" (Wienkonvensjonen) markerte startskuddet for internasjonale tiltak mot hvitvasking. Konvensjonen trådte i kraft i desember 1988 og var utformet for å bekjempe hvitvasking av penger fra narkotikahandel. Landene som signerte konvensjonen var enige om at hvitvasking måtte kriminaliseres, internasjonalt samarbeid måtte styrkes, og det måtte vedtas lover for å lette sporing, beslag og inndragning av svarte penger (www.hvitvasking.no – C).

2.4.1.3 BASEL-UTVALGET

For å fronte misbruk av finansinstitusjoner i hvitvaskingsøyemed utstedte Basel-komitéen for banktilsyn erklæringen "Statement of principles on the prevention of criminal use of the banking system for the purpose of money laundering" i desember 1988. Basel-utvalget består av representanter fra sentralbankene og tilsynsmyndigheter fra G10-landene. I likhet med Wienkonvensjonen, fremheves behov for preventiv regulering av banksektoren ved å gjennomføre regler for kundeidentifisering, mistenkelige transaksjoner og oppbevaring av transaksjonsopplysninger, samt behov for samarbeid med rettshåndhevende myndigheter (www.hvitvasking.no – C).

Basel-komiteen publiserte i oktober 2001 rapporten "Customer due diligence for banks". Formålet med rapporten er å fastsette nye tilsynsmessige standarder og være et grunnlag for bankers rutiner og praksis vedrørende "kjenn-din-kunde". Rapporten har et videre tilsynsmessig formål og er ikke begrenset til å bekjempe hvitvasking av penger gjennom det finansielle system. Manglende eller utilstrekkelige "kjenn-din-kunde" rutiner i bankene, vil kunne utsette bankene for alvorlig kunde- og motpartsrisiko, særlig renommé, juridisk- og operasjonell risiko. Videre vil gode rutiner på dette området sikre en mer korrekt og fullstendig oversikt og konsolidering på kundesiden, eksempelvis i relasjon til regelverket for største engasjement. Gode rutiner vedrørende "kjenn-din-kunde", vil således kunne sikre den enkelte banks soliditet og dermed banksystemets integritet (www.regjeringen.no – A).

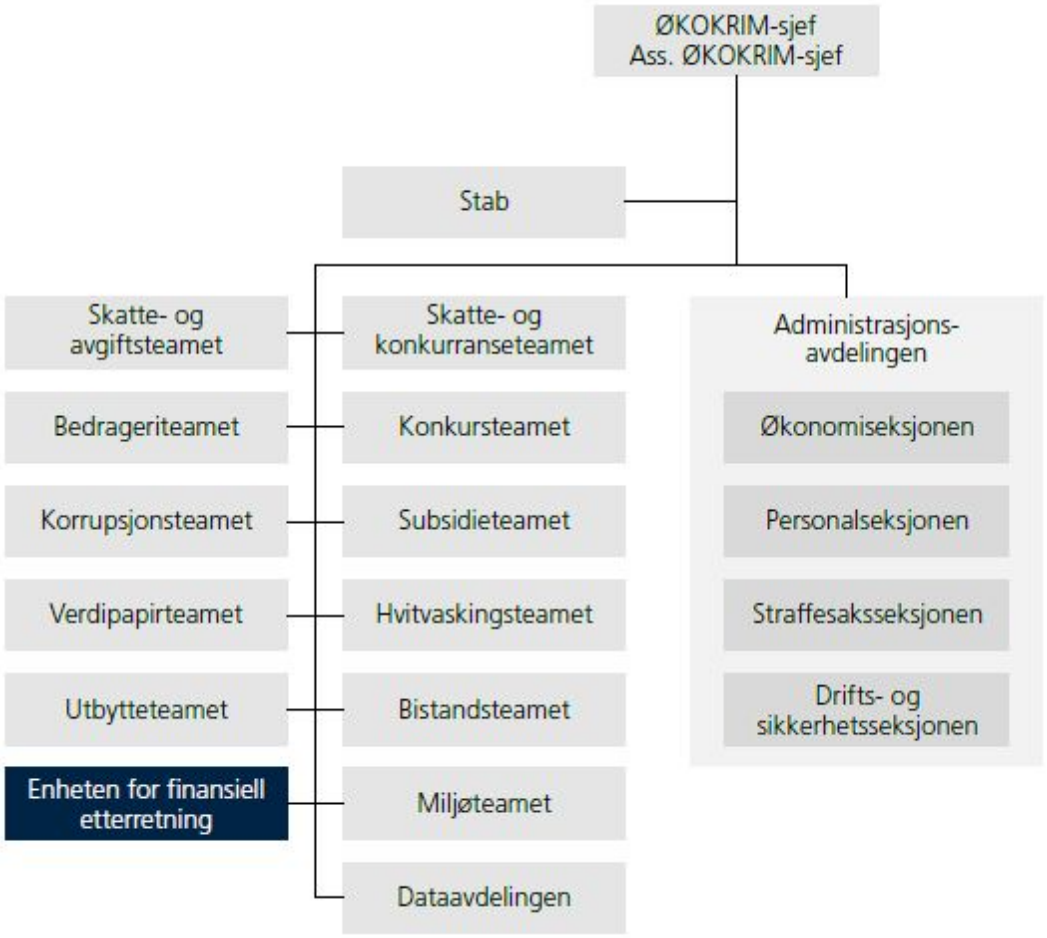
2.4.1.4 PALERMOKONVENSJONEN

Erkjennelsen av at globalisering av økonomien og utviklingen innen transport og kommunikasjonsteknologi ikke bare har skapt store muligheter sosialt og økonomisk, men også skapt store muligheter for organisert kriminalitet, var bakgrunnen for signering av FNs "Convention against transnational Organized Crime" i desember 2000. Konvensjonen representerer et vannskille i kampen mot organisert kriminalitet på grunnlag av å være det første rettslig bindende FN-instrumentet på kriminalitetsfronten. Deltagerne forpliktet seg til å oppta fire lovovertredelser; hvitvasking, deltagelse i en organisert kriminell gruppe, korrupsjon og hindring av etterforskning og rettsforfølgelse, i sine nasjonale lovverk. Motivene bak konvensjonen

er økt internasjonalt samarbeid på vedrørende utlevering, juridisk bistand, overføring av straffesaker og felles etterforskning (www.hvitvasking.no - C).

2.4.2 NORGES ARBEID INTERNASJONALT

Enheten for Finansiell Etterretning (EFE)er et av 13 team ved Økokrim. EFE skiller seg fra de øvrige teamene ved at det er det eneste teamet som ikke driver etterforskning og straffesaksarbeid. EFE er en etterretningsenhet og er Norges nasjonale FIU (Financial Intelligence Unit) (EFE:2010).



Figur 2.4.2 – Organisasjon av EFE i Økokrim (EFE:2010).

2.4.2.1 EFES OPPGAVER

EFEs primære oppgave er å motta og analysere rapporter om mistenkelige transaksjoner (MT-rapporter) fra rapporteringspliktige etter hvitvaskingsloven. Videre skal EFE bearbeide opplysningene for å gjøre dem tilgjengelige for politi- og

forvaltningsorganer med kontrolloppgaver, samt andre lands FIU-er, og videreformidle informasjon til aktuelle instanser når EFE mener vilkårene for det er oppfylt (EFE:2010).

EFE skal være et nasjonalt kompetansesenter for spørsmål relatert til hvitvasking. EFE følger med på kriminalitetsutviklingen og holder løpende kontakt med aktuelle samarbeidspartnere for å bidra til kompetanse- og metodeutvikling i politiet og hos de rapporteringspliktige. EFE deltar i aktuelle internasjonale fora for bekjempelse av hvitvasking, blant annet i FATF og Egmont Group (EFE:2010).

Formål	Oppgaver	Kilder	Produkter	Mottakere av informasjon
Forebygge og bekjempe hvitvasking av utbytte fra straffbare handlinger gjennom formidling av etterretningsinformasjon Bidra til allmennpreventiv virkning av arbeidet mot hvitvasking og finansiering av terrorisme	Motta og analysere rapporter om mistenkelige transaksjoner MT-rapporter) Produsere og videreformidle etterretningsinformasjon Bistå de rapporteringspliktige i etterlevelsen av hvitvaskingsloven Spre kunnskap om kamp mot hvitvasking og terrorfinansiering	MT-rapporter Informasjon fra andre lands FIU-er Informasjon fra politikilder Informasjon fra offentlige registre Informasjon fra åpne kilder Samarbeidspartnere Tips	Etterretningsrapporter Anmeldelser (nye anmeldelser og rapporter i eksisterende straffesaker) Operative analyser Strategiske analyser hvitvasking.no	Norge: - politiet - team ved ØKOKRIM - skattemyndigheter - tollvesenet - NAV - rapporteringspliktige - media Internasjonalt: - andre lands FIU-er - Egmont Group - FATF

Figur2.4.2-2 - Oppsummering av EFEs arbeidsområder (EFE:2010).

EFE erfarer at det internasjonalt stadig rettes større oppmerksomhet mot hvitvaskingstrusselen. EFE inngikk i 2009 flere Memorandum of Understanding (MOU) med andre lands FIUer (Financial Intelligence Unit) og antallet forespørsler fra utlandet har økt fra 2008. Innføringen av Ask (dataprogram) og vedtakelsen av den nye hvitvaskingsloven har vært avgjørende for at FATF i 2009 vedtok å fjerne Norge fra oppfølgingslisten over land som ikke fullt ut følger FATFs 40 anbefalinger om hvitvasking og terrorfinansiering (EFE:2010).

2.4.2.2 EFES BEHANDLING AV MT-RAPPORTER

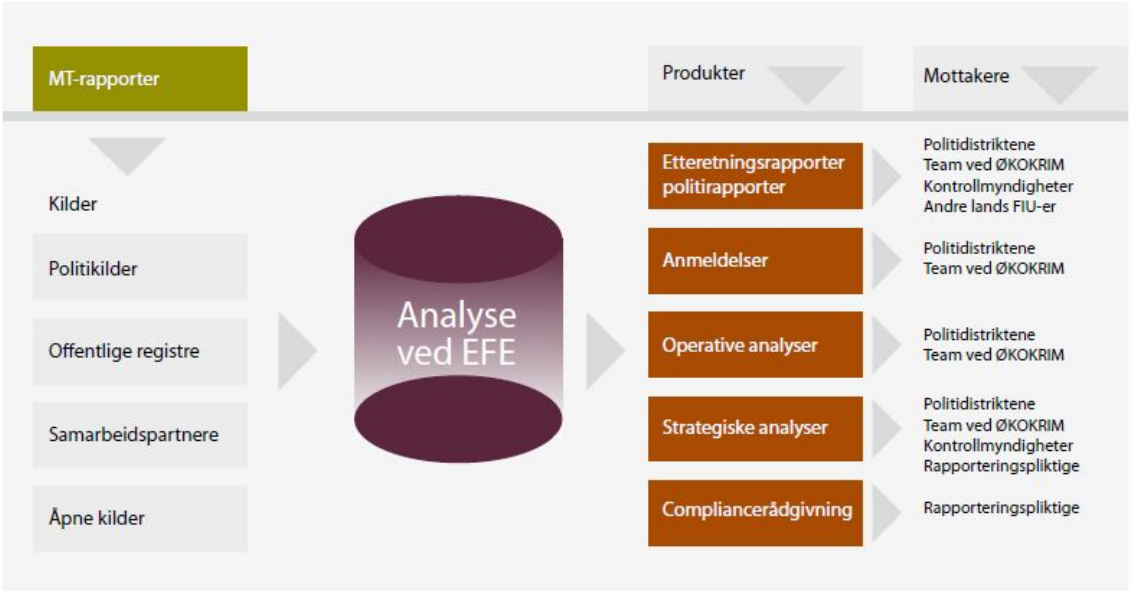
Å sende en MT-rapport til Økokrim er noe annet enn å anmelde en sak til politiet. MT-rapportene behandles som etterretningsinformasjon og danner grunnlaget for EFEs arbeid. Opplysningene i MT-rapportene sammenstilles med annen informasjon

innhentet fra flere ulike kilder. Opplysningene analyseres, og produktet av analysen videreformidles til relevante mottakere. I hvilken form opplysningene formidles avhenger av hvordan EFE vurderer det som fremgår av analysen. I de fleste tilfeller skjer dette i form av etterretningsrapporter (EFE:2010).

EFE er avhengig av kvalitativt gode MT-rapporter for å kunne produsere gode analyser, derfor er rollen til de rapporteringspliktige svært viktig. All informasjon EFE mottar, kan betraktes som brikker i et større puslespill. Jo flere brikker som er på plass, desto bedre bilde får man, dermed blir mulighetene til å utarbeide gode analyser større. Jo fyldigere en analyse er, desto større er sjansene for domfellelse i en eventuell straffesak. Finansiell etterretningsinformasjon er ikke veldig annerledes enn annen etterretningsinformasjon. Informasjonen kan gi tilstrekkelig grunnlag for inngang i nye straffesaker, den kan inngå i eksisterende straffesaker eller andre analyser hos politiet eller andre kontrollmyndigheter, basert på koblinger mellom objekter via transaksjoner og informasjon om hendelser med finansielt tilsnitt (EFE:2010).

Hva som skjer videre med informasjonen EFE sender ut og hvordan den brukes, ligger imidlertid utenfor EFEs formelle kompetanseområde. EFE har således ingen styringsmulighet med tanke på hvorvidt opplysningene kommer til å inngå i en eventuell straffesak. En etterretningsrapport oversendt politiet kan danne grunnlaget for at politidistriktet velger å opprette anmeldelse, eller den kan inngå i en eksisterende eller fremtidig straffesak. Videre kan en etterretningsrapport oversendt for eksempel skattemyndighetene, like gjerne bidra til administrative sanksjoner (tilleggsskatt, tilleggsavgift, inndragning av dagpenger osv.) som til politianmeldelse (EFE:2010).

2.4.2.3 EFES SAKSBEHANDLING



Figur 2.4.2-3 – EFEs saksbehandling (EFE:2010).

2.4.2.4 MT-RAPPORTENES ROLLE

En MT-rapport kan være en liten, men viktig brikke i et mulig bevisbilde. Når EFE mottar en MT-rapport, genererer det nødvendigvis ikke noe grunnlag for å videreformidle opplysningene med én gang, og det blir heller ikke umiddelbart tatt stilling til hvorvidt det er en "god" eller "dårlig" informasjon. Hver nye MT-rapport bidrar til å berike allerede eksisterende informasjon ved at opplysninger ses i sammenheng over tid. Således spiller alle MT-rapporter en viktig rolle helhetsvurderinger og styrker EFEs grunnlag for å videreformidle informasjon til aktuelle instanser på et senere tidspunkt. Det er derfor vanskelig å si noe konkret om gjenbruksverdien av en enkeltstående MT-rapport. En MT-rapport ender ikke nødvendigvis med domfellelse, men i de tilfeller hvor dette skjer, er det en komplisert prosess som går over lang tid. Rettsavgjørelser viser at det i flere straffesaker er anvendt informasjon fra MT-rapporter fra flere år tilbake, slik at alle opplysninger EFE mottar, kan være viktige uavhengig av når opplysningene ble sendt (EFE:2010).

Selv om opplysninger fra MT-rapportene ikke nødvendigvis brukes umiddelbart, betyr ikke det at opplysningene aldri vil bli brukt. I henhold til hvitvaskingsloven § 29 kan mottatte opplysninger oppbevares i inntil 5 år, med mindre det i dette tidsrommet

registreres nye opplysninger. Mottas ikke ytterligere relevant informasjon i løpet av disse årene har EFE plikt til å slette opplysninger som ikke er blitt brukt. EFE ønsker å understreke at det ikke er noe én-til-én forhold mellom MT-rapporter og etterforskningsrapporter/anmeldelser. Det vil si at en etterretningsrapport eller en anmeldelse kan bygge på informasjon fra mange MT-rapporter (EFE:2010).

Utbytte av kriminalitet blir verdiløst dersom de kriminelle ikke klarer å sette midlene i omløp. Hvitvasking er derfor avgjørende for profittmotivert kriminalitet i større skala (EFE:2010).

2.4.3 FATF

FATF – the Financial Action Task Force (heretter omtalt som FATF) står sentralt her. Hva FATF er, kan best beskrives med denne teksten, som er hentet fra deres webside (www.fatf-gafi.org):

"The Financial Action Task Force (FATF) is an inter-governmental body whose purpose is the development and promotion of policies, both at national and international levels, to combat money laundering and terrorist financing. The Task Force is therefore a "policy-making body" which works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas. "

FATF har for øyeblikket (april 2010) 35 medlemmer, hvorav 33 land, og 2 regionale enheter. Listen over medlemmer er:

Argentina	**Finland**	**Japan**	**Singapore**
Australia	**France**	**Kingdom of the Netherlands***	**South Africa**
Austria	**Germany**	**Luxembourg**	**Spain**
Belgium	**Greece**	**Mexico**	**Sweden**
Brazil	**Gulf Co-operation Council**	**New Zealand**	**Switzerland**
Canada	**Hong Kong, China**	**Norway**	**Turkey**
China	**Iceland**	**Portugal**	**United Kingdom**
Denmark	**Ireland**	**Republic of Korea**	**United States**
European Commision	**Italy**	**Russian Federation**	

* THE KINGDOM OF THE NETHERLANDS: THE NETHERLANDS, THE NETHERLANDS ANTILLES AND ARUBA.

I tillegg til disse, ble **India** medlem i 2006 og jobber for å bli et fullverdig medlem. FATF medlemmer og deres prospektive medlemmer, mobiliserer sammen store krefter og et bredt spekter av ekspertise for bekjempelse av hvitvasking og terrorfinansiering. Blant delegasjonene finnes eksperter innen både finansielle, regulerings, juss, og påtalemyndigheter (www.fatf-gafi.org – A).

FATF har disse partnergruppene:

- The Asia/Pacific Group on Money Laundering (APG)
- Caribbean Financial Action Task Force (CFATF)

- The Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL) - formely PC-R-EV
- The Financial Action Task Force on Money Laundering in South America (GAFISUD)
- Middle East and North Africa Financial Action Task Force (MENAFATF) (www.fatf-gafi.org – A).

Økokrims etterforskningsenhet, EFE er representert i den norske FATF-delegasjonen, som ellers består av representanter fra Justisdepartementet, Finansdepartementet, Finanstilsynet og Politidirektoratet. Delegasjonen deltar i plenumsmøter tre ganger årlig i tillegg til ulike arbeidsgrupper (EFE:2010).

EFE deltar også som co-chair i en av arbeidsgruppene til FATF. FATF jobber for å fremme innføring av nasjonal lovgivning både i og utenfor medlemslandene. Målet er å bidra til å avdekke hvitvasking og inndra svarte penger samt å erstatte finansiell diskresjon med gjennomsiktighet. Rammeverket for FATFs føringer utgjøres av 40 anbefalinger og 9 spesialanbefalinger (Se appendix B og C). Etter terrorangrepene i USA 11. september 2001 utvidet FATF sitt mandat til også å omfatte finansiering av terrorisme (EFE:2010).

Kort oppsummert er budskapet i de 40 anbefalinger å:

- Kriminalisere hvitvasking og vedta lover for å inndra utbytte av straffbar handling.
- Opprette regler for kundeidentifisering og oppbevaring av opplysninger hos finansinstitusjoner, og rette spesiell oppmerksomhet mot ny teknologi som understøtter anonymitet.
- Kreve at mistenkelige transaksjoner rapporteres til myndighetene.
- Sørge for forsvarlig kontroll og tilsyn med finansinstitusjoner.
- Oppfordre alle lands regjeringer til å opprette finansielle etterretningsenheter (FIU) for å føre tilsyn med transaksjoner.
- Sette forhåndsbetingelser for å bidra til effektivt internasjonalt samarbeid.

(Se alle 40 anbefalinger i appendix B).

Anbefalingene er basert på et underliggende prinsipp om gjennomsiktighet. De er utformet for universell anvendelse, og er generelle prinsipper som skal tilpasses rettssystemet i hvert land. Implementering og overholdelse av anbefalingene sikres ved å føre tilsyn med landene og ved å tilby teknisk assistanse blant annet i form av rådgivning om lovverk, og evaluering av medlemslandenes tiltak mot hvitvasking og terrorfinansiering (EFE:2010).

FATF publiserer jevnlig rapporter som tar for seg nye utfordringer, modus, teknologi og bransjer som er sårbare i forbindelse med hvitvasking og finansiering av terrorisme. I løpet av 2009 publiserte de blant annet rapportene"Money laundering & terrorist financing in the securities sector","Risk based apporach: Guidance for the life insurance sector" og "Money laundering through the football sector" (EFE:2010).

2.4.4 EGMONT GROUP

Egmont group ble etter initiativ fra Belgia og USA opprettet i 1995 som et nettverk av FIU-er og er et uformelt samarbeid for myndighetsorganer som jobber mot hvitvasking. Kjernen i samarbeidet er tilgang på finansiell informasjon på tvers av landene og informasjon om nye hvitvaskingstrender og ny teknologi som er sårbar for hvitvasking, samt utveksling av erfaringer mellom FIU-ene. Per desember 2009 hadde egmont group 117 medlemmer (EFE:2010).

EFE er Norges FIU. FIU-en har som oppgave å motta og analysere rapporter om finansielle transaksjoner og videreformidle informasjonen i henhold til regelverket. Formålet er å sørge for effektiv utveksling av finansiell etterretning mellom rapporteringspliktige og politi- og påtalemyndigheter via FIU-en. EFEs samarbeid i Egmont Group består i informasjonsutveksling på tvers av de ulike FIU-ene, basert på rapporter om mistenkelige transaksjoner. Noen av disse sakene publiseres på hjemmesidene til Egmont Group i anonymisert form (EFE:2010).

Egmont Group har ulike arbeidsgrupper som jobber med sine respektive tema. Disse omfatter en IT-gruppe, en operasjonell gruppe, en gruppe som tar seg av rettslige spørsmål, en opplæringsgruppe og en bistandsgruppe. Norge deltar i opplæringsgruppen. En gang i året avholdes plenumsmøte for alle medlemmene (EFE:2010).

2.4.5 MER OM FATF

Siden oppstarten i 1989 har FATF jobbet for å forhindre at det finansielle systemet blir misbrukt av kriminelle organisasjoner. FATF utarbeidet en rekke anbefalinger i 1990, som ble revidert i 1996 og 2003 for å sikre at arbeidet er oppdatert i forhold til den konstante utviklingen av trusler i forhold til hvitvasking. Disse anbefalingene (se appendix B) er ment å danne en slags basis for et rammeverk for anti-hvitvaskingsarbeid og er ment å benyttes for universelle arbeider (www.fatf-gafi.org – B).

FATF driver konstant overvåking av sine medlemmer, for å følge med på hvordan de til enhver tid ligger an i anti-hvitvaskingsarbeidet. I dette arbeidet, samarbeider de med andre internasjonale organisasjoner. Dette arbeidet danner også grunnlaget for videreutvikling og revidering av de til enhver tid gjeldene anbefalinger. Arbeidet foregår ved at hvert medlemsland blir besøkt av en liten gruppe eksperter innen juss, finans og politimyndighet som går gjennom det enkelte lands hvitvaskingsarbeid. Formålet med besøket, er å avdekke innen hvilke områder det enkelte land har gjort fremskritt innen arbeidet, og hvilke området som krever mer arbeid. På denne måten blir FATFs anbefalinger hele tiden vurdert og oppdatert dersom det viser seg at det enkelte land har funnet metoder som er mer effektive enn andre. Dersom det enkelte land ikke følger opp, vil det også gjennom FATF legges press på landet slik at det til enhver tid er oppdatert i hvitvaskingsarbeidet (www.fatf-gafi.org – B).

FATF har ingen definerte grunnlov/grunnregler eller noe definert livsløp. I stedet blir FATF ved jevne mellomrom internrevidert for å se at de fortsatt har en misjon. FATF har eksistert siden 1989, og sittende mandat (2004-2012) gjennomførte i april 2008 sist en vurdering og ble godkjent og revidert for videre drift (www.fatf-gafi.org – B).

2.4.5.1 FATFS HISTORIE

FATF ble grunnlagt som et resultat av en voksende bekymring rundt hvitvaskingsproblematikken. Dette skjedde under G7 møtet i Paris i 1989. Som et svar på den stadig voksende trusselen i forhold til hvitvasking, ble FATF opprettet av Europakommisjonen, med medlemmer fra G7-landene, Europakommisjonen og 8 andre land (www.fatf-gafi.org – B).

FATF ble gitt som oppgave å undersøke hvitvaskingsteknikker og – trender, undersøke hva slags tiltak medlemslandene allerede hadde satt i gang mot hvitvasking på et nasjonalt og/eller internasjonalt nivå, og sette en standard for hva slags tiltak som gjensto å innføre i kampen mot hvitvasking. I april 1990, under ett år etter opprettelsen av FATF ga de ut et sett med 40 anbefalinger som var ment å være et omfangsrikt verktøy i denne kampen (www.fatf-gafi.org – B).

I 2001 ble utviklingen av kampen mot terrorfinansiering lagt til som et arbeidsområde for FATF. I oktober 2001 ga FATF ut 8 spesielle anbefalinger for å håndtere temaet terrorfinansiering. Den kontinuerlige utviklingen på dette området, gjorde at de måtte revidere dette arbeidet betraktelig i juni 2003. Dette igjen ledet til en ny utgivelse i oktober 2004, hvor de utga 9 spesielle anbefalinger i kampen mot terrorfinansiering. Dette betyr at det per i dag (april 2010) eksisterer 40+9 anbefalinger i arbeidet mot hvitvasking og terrorfinansiering (www.fatf-gafi.org – B).

I løpet av 2001-2002 utvidet FATF medlemskapet sitt fra 16-28 medlemmer. I 2002 utvidet de til 31 medlemmer, i 2003 til 33 medlemmer, og i 2007 til sine 35 medlemmer slik det er i dag (www.fatf-gafi.org – B).

2.4.6 LIGNENDE ORGANISASJONER

I tillegg til FATF finnes det en rekke organisasjoner med observatørstatur og enkelte av disse er også medlemmer av FATF. Under følger en oversikt over disse organisasjonene. På websiden www.fatf-gafi.org finnes en oversikt over disse organisasjoner dersom man er spesielt interessert i mer info om disse:

FATF Style Regional Bodies

- Eurasian Group (EAG)
- Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG)
- Intergovernmental Action Group against Money-Laundering in Africa (GIABA)

Other International Organisations

- African Development Bank
- Asian Development Bank
- Basel Committee on Banking Supervision (BCBS)
- Commonwealth Secretariat
- Egmont Group of Financial Intelligence Units
- European Bank for Reconstruction and Development (EBRD)
- European Central Bank (ECB)
- Eurojust
- Europol
- Inter-American Development Bank (IDB)
- International Association of Insurance Supervisors (IAIS)
- International Monetary Fund (IMF)
- International Organisation of Securities Commissions (IOSCO)
- Interpol
  Interpol/Money Laundering *[English]*
- Organization of American States / Inter-American Committee Against Terrorism (OAS/CICTE)
- Organization of American States / Inter-American Drug Abuse Control Commission (OAS/CICAD)

- Organisation for Economic Co-operation and Development (OECD)
- Offshore Group of Banking Supervisors (OGBS)
- United Nations -
  Office on Drugs and Crime (UNODC)
  Counter-Terrorism Committee of the Security Council (UNCTC)
  The Al-Qaida and Taliban Sanctions Committee (1267 Committee)
- World Bank
- World Customs Organization (WCO)

(www.fatf-gafi.org – A).

KAPITTEL 3 – HVITVASKINGSMETODER OG -TRENDER

3.1 BAKGRUNN

Hvitvasking av penger er et gammelt fenomen og strekker seg langt tilbake i tid. Hvor langt er vanskelig å anslå, men det er naturlig å tenke seg at det kan være helt siden man innførte valuta som betalingsform. Bekjempelse av hvitvasking derimot er et relativt nytt fenomen, og det spesielt i forbindelse med finansiering av terror at det har blitt et såpass prioritert område for styresmaktene i land verden rundt. De store tiltakene ble satt i gang for ca 20 år siden, i det en del initiativ mot hvitvasking og terrorfinansiering ble satt i gang, blant annet opprettelsen av FATF. Dette kapittelet ser på utvikling de siste år i forhold til økonomisk kriminalitet og hvitvasking av penger.

3.2 UTVIKLINGSTREKK INNEN HVITVASKING

Hvitvasking av utbytte fra kriminelle handling tar stadig nye former og baseres på de svært mange mulighetene som finnes til å skjule, transportere og deponere penger, samt skjule koblingene til de kriminelle handlingene og til de kriminelle aktørene. I utlandet er det et vell av tilbud om administrative, finansielle og juridiske tjenester knyttet til forvaltning av penger for kundene på diskré måter. Sannsynligvis skjer mye av hvitvaskingen ved sammenblanding av legale og illegale midler i selskaper og overføringer mellom selskaper til og fra utlandet. I tillegg er det sannsynligvis blitt mer valutasmugling for å unngå rapportering til politiet av mistenkelige transaksjoner(MT) (Finansdepartementet:2004 – A).

3.3 UTFORDRINGER FOR POLITIET

Dels fordi mye av den grove økonomiske kriminaliteten ikke fanges opp av kontrollmyndighetene og politiet, og dels fordi denne kriminaliteten i større grad blir internasjonal og skjer i organisert form, vil utfordringene for politiet i første rekke være å kunne:

- Gjennomføre helhetlig etterforskning i store sakskomplekser innenfor rendyrket økonomisk kriminalitet på en effektiv måte.
- Tilrettelegge for kontinuitet i arbeid med alvorlig saker innenfor rendyrket økonomisk kriminalitet og videre kompetanseutvikling på spesialiserte fagområder.
- Rekruttere spisskompetanse innenfor økonomi og næringsliv inn i stabile tverrfaglige miljøer i politiet.
- Identifisere kriminalitet innenfor kriminelle nettverk som driver komplisert og omfattende økonomisk kriminalitet
- Integrere finansiell etterforskningsmetodikk i etterforskning av organisert, vinningsmotivert kriminalitet.
  (Finansdepartementet:2004 – A).

3.4 HVITVASKINGSMETODER

Når det gjelder utviklingstrekk innen hvitvasking, har Økokrims hvitvaskingsenhet trukket frem følgende punkter i sin årsrapport for 2001;

De enkleste formene for hvitvasking skjer i de land der primærforbrytelsen ble begått. Hvis de i tillegg involverer mindre beløp og er mer sporadisk av karakter er disse teknikkene populære:

- Pengespill – kjøp av vinnerbonger er en klassiker. Disse blir kjøpt opp mot et sjenerøst vederlag. Man har også mistanke om at visse elementer kjøper opp vinnerbonger i stor stil, for så å selge disse videre til kriminelle.
- Aksjemarkedet – med den rette aksjemegleren kan de kriminelle eksempelvis kjøpe spot og selge forwards, eller motsatt. Den ene transaksjonen gir gevinst, den andre tap. Megleren makulerer den transaksjonen som ga tap, og

hvitvaskeren kan vise til en faktisk gevinst. Kostnaden er dobbel kommisjon samt eventuelt avtalt pris til megleren.

- Eiendomsmarkedet - man kan kjøpe en eiendom med legitime penger, pusse den opp med illegale svarte penger, og selge den til en mye høyere markedsverdi.
- Nisjeprodukter – livrente, leasing og leie gir mange muligheter innen hvitvasking.

(Finansdepartementet:2004 – A).

Om man sitter med en kontinuerlig illegal pengestrøm er det vanskelig å overbevise om at man har flaks hele tiden. I disse tilfellene ser man at de kriminelle ofte bruker kontantbaserte skalkeskjulvirksomheter som eksempelvis bruktbil, renseri, videoutleie, grønnsakhandel, bygg og anlegg, barer og restauranter. Prinsippet er enkelt. Man blander legal og illegal inntekt og rapporterer den akkumulerte summen som virksomhetens legale inntekt. Dette i kombinasjon med fiktive utgifter gir disse virksomhetene en ryddig bunnlinje og minimal skatt (Finansdepartementet:2004 – A).

Om dette blir for stort, og risikoen for å bli oppdaget for høy, ser man ofte at pengene forsvinner til utlandet. Dette kan enten skje gjennom det formelle registrerte banksystemet eller ved omgåelse av dette. Omgår man systemet er disse teknikkene populære (Finansdepartementet:2004 – A).

- Smugling av kontanter. Dette gjøres ved å redusere volumet. Man pakker mest mulig penger i størst mulig seddelverdi. Sveitsiske franc, euro og dollar er de mest populære valutaene. 25.000 sveitsiske franc, verdt ca 200.000 norske kroner, tilsvarer 25 sedler pålydende 1000 franc.
- Moneygram og postens verdibrev – man kan sende og motta penger nesten hvor som helst i verden uten bankkonto eller betalingskort.
- Alternative banksystemer også kalt Hawala – mange etniske grupperinger bruker disse systemene som er opprettet av legitime grunner, men sårbare for misbruk.

(Finansdepartementet:2004 – A).

Hvis de kriminelle bruker det formelle systemet, må vi regne med at de er klar over rapporteringsrutinene institusjonene har. Hvis de ikke bruker skalkeskjulvirksomheter, kan man regne med at de aktivt strukturerer innskudd, og overføringer for ikke å tiltrekke seg oppmerksomhet. Hva slags virksomheter brukes til dette? Her er noen tegn man kan se etter:

- Virksomheten driver internasjonal handel med varer og/eller tjenester.
- Overføringer er strukturert i forskjellige beløp og med forskjellige betalingsinstrumenter, alt for å tåkelegge.
- Handel med tjenester er best da det ikke er noen regler for å kontrollere prisene som benyttes.

(Finansdepartementet:2004 – A).

Den beste virksomheten for å plassere penger inn i det registrerte systemet er som nevnt en kontantbasert virksomhet. Den beste virksomheten for å sende penger utenlands er et selskap engasjert i handelsvirksomhet med utlandet. Det bør derfor stilles alvorlige spørsmål ved innenlandske virksomheter som sender store summer til utlandet, og tilsvarende spørsmål ved kontantinnskudd på innenlandske kontoer til virksomheter som driver handelsvirksomhet med utlandet (Finansdepartementet:2004 – A).

Når pengene er flyttet ut av landet, begynner tilsløringsfasen. Kriminelle unngår gjerne personlig oppmøte i en bank i eksempelvis Sveits. Under nevnes noen typiske trekk:

- Man besøker land som tilbyr "instant-corporations" slik som money transfer og Forex og kjøper seg en virksomhet av en eller annen form. British Virgin Islands, Liberia, og Panama er blant de som tilbyr denne tjenesten.
- Pengene overføres så til disse selskapene og ikke til individer, da det kan være store utfordringer knyttet til å finne ut hvem som faktisk eier selskapet.
- Man oppretter konto i valgfritt skatteparadis, eksempelvis Østerrike, Sveits eller Luxembourg, og overfører pengene dit.
- Man foretar internasjonale overføringer for å tilsløre opprinnelsen, og på den måten brytes kjeden ved å ta ut/sette inn pengene i forskjellige land

(Finansdepartementet:2004 – A).

Den siste utfordringen blir da å få pengene hjem, og integrere den i den registrerte økonomien. Her er noen eksempler på hvordan dette kan gjøres:

- Betalingskort – utstedt av en utenlandsk bank, enten direkte trekk fra utenlandsk konto, eller overføring fra utenlandsk konto til kortselskap.
- Regningsbetaling – egne utenlandske selskaper dekker alle regninger i hjemlandet, eller ved overføring til utenlandske selskaper som faktisk spesialiserer seg på slike tjenester.
- Internasjonal eiendomshandel – man kan selge eiendom. til justert pris, til egen utenlandsk virksomhet.
- Kjøp og salg av aksjer/opsjoner/varer mellom egne innenlandske og utenlandske virksomheter.
- Personlig inntekt – mitt eget selskap i utlandet kan betale meg lønn for fiktive konsulentoppdrag, frynsegoder som fri bil og leilighet er heller ikke vanskelig å arrangere.
- Virksomhetsinntekt – fakturering av fiktive handler med varer/tjenester.
- Forretningslån – jeg kan "låne" penger av mine egne utenlandske virksomheter. Da har jeg også god grunn til å overføre penger til utlandet, og kan i tillegg trekke rentene fra på skatten. På denne måten slutter jeg hvitvaskingssirkelen og kan faktisk øke omfanget av den.

(Finansdepartementet:2004 – A).

3.5 AKTUELLE SCENARIOER

3.5.1 FIKTIVE SCENARIOER

Økokrim har i sin årsrapport fra 2009 med 2 fiktive scenarioer for hvordan hvitvasking kan foregå i Norge. Disse er gjengitt i sin helhet her:

3.5.1.1 SCENARIO 1 – HVITVASKING GJENNOM KONTANTINNSKUDD

Kunden setter inn til dels betydelig summer med kontanter på egen lønnskonto – for tiden er det ingen annen inngang på denne kontoen. I tillegg har kunden vekslet om små sedler til 1000-lapper. Kunden har forsøkt å åpne konto i en annen bank i en annen landsdel slik at andre kan sette inn penger på konto der. Økokrim blir i den forbindelse

kontaktet av denne banken. Den 13. juli observeres kunden i banken i tett dialog med to personer som man vet tilhører det kriminelle miljøet i byen. I tillegg ser man av aktiviteten på kundens konto at han reiser mye rundt i Norge.

I denne MT-meldingen ser vi at det opplyses om store kontantinnskudd, vekslinger til større sedler, men for øvrig lite annen kontoaktivitet, faktorer som i utgangspunktet kan virke mistenkelige. Det redegjøres for opprettelse av annen konto i en annen bank et helt annet sted i landet, samt at den rapporterte er observert med personer som er kjente som kriminelle i lokalmiljøet. Slike opplysninger er opplagt interessante for EFE, og er et godt utgangspunkt for videre undersøkelser (EFE:2010).

3.5.1.2 SCENARIO 2 – HVITVASKING GJENNOM LEILIGHETSKJØP

Ved kjøp av en leilighet i Kirkevik utbetalte Peder Ås kr 700 000 i kontanter for leiligheten og ytterligere kr 48 000 i kontanter for arbeid utført av selger, byggefirma Berg og Dahl AS. Det skal i tillegg gjøres opp kr 400 000 kontant med kr 100 000 i måneden til leiligheten er fullstendig oppgjort. Mottaker har dokumentert kontantmottakene så godt det lar seg gjøre, satt kontantene på konto, ført dem via restkonto og inntektsført alt i henhold til gjeldene regelverk (EFE:2010).

Det mottatte kontantbeløp er betydelig over det som kan anses naturlig for Peder Ås. Sett i sammenheng med de offentlige opplysninger vi finner om ham, virker det underlig at han kan besitte slike kontantsummer. Vi har funnet at han driver flisleggervirksomhet i Kirkevik, nær all omsetning er kontant, og ordreboken har vært full, 10 timer hver dag, 5-6 dager i uke, til kr 450 pr. time. Dette gir betydelig større inntekter enn det vi kan se er oppgitt til skattemyndighetene. Økokrim mener derfor at transaksjonene er mistenkelige. Innskuddene på henholdsvis kr 475 000, 125 000, 200 000 og 48 000 er foretatt til Bygdebanken, kontonummer xxxx.xx.xxxxx og xxxx.xx.xxxxx. I tillegg ser det ut til at Peder Ås skal betale kr 100 000 pr. måned i 4 måneder for å gjøre opp en leilighet. Her finnes det dog ikke avtaler, men indikasjoner (EFE:2010).

I dette tilfellet ser vi at mistanken begrunnes gjennom sammenlikning av offentlige kilder om den rapportertes økonomi med den tilgjengelige informasjonen som foreligger på bakgrunn av den rapporteringspliktiges rolle. Begrunnelsen og dokumentasjonen gir EFE godt grunnlag for videre undersøkelser av forholdene som beskrives(EFE:2010).

3.5.2 SCENARIOER FRA VIRKELIGHETEN

3.5.2.1 SCENARIO 3 – HVITVASKING GJENNOM FALSK FAKTURERING

Oslo tingrett dømte en svensk statsborger til to år og fire måneder ubetinget fengsel for hvitvasking av utbytte fra kriminelle handlinger i bygg- og anleggsbransjen. Det ble også idømt inndragning på 100 000 kroner.

Heleriene foregikk ved at den dømte utstedte uriktige fakturaer og dermed kvitterte for mottak av til sammen 14,5 millioner kroner for arbeid som ikke ble utført. Pengene ble siden hevet kontant og tilbakeført til den opprinnelige betaleren. De uriktige fakturaene ble siden brukt som dokumentasjon for å skaffe urettmessige utbetalinger av merverdiavgift. Saken illustrerer hvordan selskaper og fiktiv fakturering effektivt kan brukes som hvitvaskingsverktøy. Dersom utstederfirma og mottakerfirma samarbeider om slike transaksjoner, kan utbytte fra kriminalitet enkelt kamufleres som tilsynelatende legitim omsetning (EFE:2010).

3.5.2.2 SCENARIO 4 – HVITVASKING GJENNOM FALSK FAKTURERING 2.

I en Økokrim-sak i januar 2009 dømte Hedmarken tingrett en mann til ubetinget fengsel i seks måneder for grovt heleri og momslovbrudd på totalt ca. 1,5 millioner kroner. Mannen ble også ilagt rettighetstap, bot på 5000 kroner og inndragning av utbyttet fra handlingene (EFE:2010).

Mannen skrev under på at han hadde mottatt til sammen ca 1,5 millioner kroner i kontanter i samsvar med fakturaer fra selskaper i bygg- og anleggsbransjen der han var registrert som daglig leder (Selskapene var registrert som såkalte NUF – Norsk avdeling av Utenlandsk Foretak). Den dømte hadde likevel ikke mottatt pengene. Kvitteringene og fakturaene ble brukt til merverdiavgiftsbedrageri og utroskap i selskapet som mottok fakturaene, mens den dømte mottok mindre beløp som godtgjøring for underskriftene sine. I tillegg ble han dømt for manglende innsending av omsetningsmelding for selskapene. Mannen tilsto forholdene, noe som det ble lagt stor vekt på ved straffeutmålingen (EFE:2010).

Denne dommen er én av flere dommer i Økokrim-saker med slik kriminalitet i bygg- og anleggsbransjen, der denne fremgangsmåten er velkjent: Entreprenører gir håndverkerne

"svart" lønn med kontante uttak fra banken og dekker lønna opp i regnskapet med kvitteringer og fakturaer (inklusive merverdiavgift) fra fiktive underleverandører. EFE mottok i løpet av 2007 flere MT-rapporter som gjaldt personer og selskaper knyttet til denne saken. Det ble åpnet straffesak som ble overført til et av straffesaksteamene ved Økokrim høsten 2007 (EFE:2010).

3.5.2.3 SCENARIO 5 – HVITVASKING AV UTBYTTE FRA UTLANDET

I en Økokrim-sak dømte Oslo tingrett en britisk statsborger bosatt i Norge til fengsel i ett år og tre måneder for hvitvasking av utbytte fra kriminelle handlinger i utlandet. Mannen måtte også tåle inndragning av 1,8 millioner kroner (EFE:2010).

Briten hjalp en koreansk forretningskontakt med å motta flere pengeoverføringer, og var på den måte behjelpelig med å sikre kriminelt utbytte. Den dømtes framgangsmåte hadde mange trekk som tydet på hvitvasking. Opprinnelig var ønsket å overføre pengene via konto til Sveits, men fordi det da ble krevd legitimasjon, endret de framgangsmåte. Deretter ble de 1,8 millionene forsøkt vekslet til euro eller britiske pund, valutaer med høy valør, som er en annen kjent hvitvaskingsmetode. I forkant av vekslingene så man også eksempler på "smurfing", dvs. at utbyttet ble stykket opp for å vekke mindre oppsikt, og det ble brukt fiktiv fakturering og stråpersoner uten noen reell forretningsmessig rolle (EFE:2010).

Saken er spesiell fordi den i meget stor grad er etterforsket og iretteført av EFE. Vanligvis er EFEs rolle å motta og formidle etterretningsinformasjon til øvrige team i Økokrim, politiets særorganer (blant annet PST, Kripos, og politiets utlendingsenhet), politidistriktene og forvaltningsorgan med kontrolloppgaver som NAV og skattemyndighetene (EFE:2010).

3.5.2.4 SCENARIO 6 – HVITVASKING AV UTBYTTE FRA UTLANDET 2.

Nettstedet www.hvitvasking.no hadde i 2007 denne saken publisert:

Skjerpet straff i Norgeshistoriens største Hawalasak

Økokrim, 27. juni 2007: Borgarting lagmannsrett skjerpet straffen for en av hovedmennene i en Hawala-sak. Begge tiltalte ble i tillegg dømt til inndragning av utbytte for Hawalavirksomhet. De to ble av tingretten i november 2006 dømt for blant annet ulovlig bankvirksomhet. I tidsrommet 2001-2005 ble ca. 225 millioner kroner

overført fra Norge til diverse selskaper rundt omkring i Europa (www.hvitvasking.no – G).

Ankesaken endte med at den ene hovedmannen fikk skjerpet fengselsstraffen fra seks måneders betinget og seks måneders ubetinget fengsel til totalt ett og et halvt års ubetinget fengsel (www.hvitvasking.no – G).

De to domfelte drev betalingsformidling til utlandet mot vederlag (Hawalavirksomhet) uten tillatelse fra Norges Bank eller Kredittilsynet. "Hawala" er et system som benyttes for å overføre penger til utlandet utenom det ordinære bankvesenet. Til sammen ble det overført nærmere 225 millioner kroner fra en rekke personer i Norge til ulike personer/foretak i utlandet. Virksomheten opererte nesten uten noen form for dokumentasjon (www.hvitvasking.no – G).

Enheten for finansiell etterretning ved Økokrim mottok i perioden fra 2002 til 2004 flere MT-rapporter som gjaldt hyppige og relativt store pengeoverføringer til utlandet gjennom bankkontoene til flere norske selskaper hvor innehaverne var en nordmann og en irakisk statsborger (www.hvitvasking.no – G).

Pengene som gikk inn på konto var både kontante innbetalinger og overførsler, som stammet fra et stort antall ulike personer, før de ble sendt videre ut av landet. Pengestrømmen gikk som til ulike land, men ofte gikk pengene til Irak via Tyrkia. Enheten fikk i analyseprosessen mistanke om innsamlingsvirksomhet og såkalt hawalavirksomhet, og det ble opprettet samarbeid med lokale skattemyndigheter. På grunn av sakens kompleksitet ble det opprettet straffesak ved Økokrims utbytteteam i 2004 (www.hvitvasking.no – G).

Etterforskingen viste at det til sammen hadde blitt sendt over NOK 224 millioner ut av landet i den aktuelle perioden. Nordmannen hadde særlig en medhjelper, som igjen hadde en forgrening av underagenter, som samlet inn penger på den ovenfor beskrevne måten. De mistenkte hadde drevet betalingsformidling med utlandet mot vederlag, uten tillatelse, og uten å føre regnskap. Omfanget av virksomheten var økende (www.hvitvasking.no – G).

Det ble tatt ut tiltale for brudd på finansieringsvirksomhetsloven, hvitvaskingsloven, regnskapsloven, bokføringsloven, ligningsloven, merverdiavgiftsloven,

skattebetalingsloven og regnskapsførerloven. I tillegg ble den irakiske borgeren tiltalt for trygdebedrageri, herved brudd på Straffelovens § 270, og for heleri, herved brudd på straffelovens § 317. 24. november 2006 falt det dom i Oslo tingrett. Begge ble dømt i henhold til tiltalen (www.hvitvasking.no – G).

Den norske borgeren ble i tillegg til å drive ulovlig bankvirksomhet domfelt for skattesvik, merverdiavgiftsbedrageri, brudd på skattebetalingsloven og regnskapsførerloven. Han ble også fradømt retten til å drive selvstendig virksomhet, være daglig leder eller inneha ledende stilling i noe selskap for et tidsrom av fem år. I tillegg må han tilbakebetale 1.2 millioner kroner (www.hvitvasking.no – G).

Den andre ble i tillegg til å drive ulovlig bankvirksomhet også domfelt for skattesvik, hvitvasking og trygdebedrageri, og må tåle inndragning på 750 000 kroner (www.hvitvasking.no – G).

3.5.2.5 SCENARIO 7 – SKATTEUNNDRAGELSE.

EFE mottar ved hvert årsskifte et relativt høyt antall MT-rapporter som gjelder skatteunndragelse. En spesiell type av disse rapportene er de såkalte 31.12 – meldingene. Modus er at det foretas et uttak av kontanter i form av sjekk eller bankremisse fra bankkonto rett før årsskiftet og at pengene settes inn igjen på nyåret. Siktemålet med dette er å gi inntrykk av at formuen er lavere enn den faktisk er, og dermed unngå formuesbeskatning på hele formuen. 31.12 – meldingene kan imidlertid også være en inngang for å avdekke annen økonomisk kriminalitet (EFE:2010)

31.12 – meldingene blir analysert ved EFE og resulterer som regel i rapporter til skattemyndighetene, som gjerne reagerer med tilleggsskatt. Antallet slike meldinger har holdt seg ganske konstant de senere år, til tross for stadige advarsler mot fremgangsmåten i media (EFE:2010).

EFE mottok melding om en kvinne som tok ut penger like før årsskiftet, og som satte dem inn igjen like etter. Nærmere undersøkelser viste at kvinnen hadde brukt samme fremgangsmåte de siste ti årene. En etterretningsrapport ble oversendt skattemyndighetene. Totalt viste det seg å være en skatteunndragelse på 24,5 millioner kroner. Etter gjeldende regler hadde kvinnen måttet betale ca. 16 000 kroner i formueskatt årlig. Unndragelsen førte imidlertid til at hun ble ilagt 60 % straffeskatt

samt betaling av renter på det unndratt beløpet. Hennes totale skatteregning ble til slutt på ca. 500 000 kroner (EFE:2010).

3.5.2.6 SCENARIO 8 – SKATTEUNNDRAGELSE 2.

Nettstedet www.abcnyheter.no publiserte følgende artikkel 30.04.10:

190 skjulte millioner på Østlandet avslørt

59 personer på Østlandet har forsøkt å skjule 190 millioner kroner i bankinnskudd. Nå er alle avslørt av Skatt øst (www.abcnyheter.no).

Det er bankene selv som har gjort Økokrim oppmerksom på jukset, og som har sendt hvitvaskingsmeldinger om det som har foregått (www.abcnyheter.no).

De 59 har tatt ut pengene fra banken like før årsskiftet og satt dem inn igjen rett etter årsskiftet. Hensikten har vært å unngå at beløpene ble innrapportert til skattemyndighetene som formue (www.abcnyheter.no).

I en pressemelding opplyser Skatt øst at 44 av de 59 har gjort det samme gjennom mange år, slik at det samlede innrapporterte beløpet er 190 millioner kroner (www.abcnyheter.no).

Enkelt å avsløre
– Jeg er overrasket over at noen fortsatt tror at de kan slippe unna med denne metoden for å unndra formuesskatt, når det er så enkelt å avsløre slike unndragelser, sier skattekrimsjef i Skatt øst, Jan-Egil Kristiansen (www.abcnyheter.no).

Han sier at skattemyndighetene systematisk kontrollerer slike saker. Den som prøver seg vil få en baksmell, for det må betales skatt ti år tilbake i tid og 60 prosent straffeskatt i tillegg for det som er forsøkt unndratt (www.abcnyheter.no).

Om noen har forsøkt seg i år, er det fortsatt mulig å føre riktig formue opp i selvangivelsen. Fristen for å levere selvangivelsen for vanlige lønnsmottakere er 30. april (www.abcnyheter.no).

Oversikten viser at 42 av dem som forsøkte å jukse med formuen på denne måten bor i Oslo og ti i Akershus. Resten er fordelt på Østfold, Hedmark og Oppland (www.abcnyheter.no).

25 prosent av alle som forsøkte seg med denne metoden var pensjonister over 67 år. Største beløp er på 15 millioner kroner (for ti år) og gjelder en 67-åring fra Oslo (www.abcnyheter.no).

3.5.3 STRATEGISK ANALYSE – PROSTITUSJON OG PENGER

EFE utarbeidet i 2009 en strategisk analyse av finansielle transaksjoner foretatt av nigerianske statsborgere før og etter forbudet mot kjøp av seksuelle tjenester. Formålet var å se om det oppsto endringer i transaksjonsmønsteret etter at forbudet mot sexkjøp ble innført 01.01.09. Målgruppen for analysen var primært politi som jobber mot prostitusjon, men analysen ble også gjort åpent tilgjengelig. Hypotesen som lå til grunn for analysen, var at store deler av pengeoverføringene og vekslingene foretatt av nigerianske borgere, var generert gjennom prostitusjon. I analysen ble det hentet ut informasjon om overføringer fra Norge til Nigeria samt vekslinger foretatt av nigerianske statsborgere i Norge. Tallene i denne analysen omfatter følgelig alle transaksjoner til Nigeria og vekslinger foretatt av personer som har oppgitt å være nigerianske statsborgere (EFE:2010).

Analysen viste at overføringene sank med 40 % fra november 2008 til januar 2009. Fra januar 2008 til januar 2009 var imidlertid nedgangen på 25 %. Slik ser man et tydelig sammenfall mellom sexkjøpsforbudet og antall overføringer til Nigeria (EFE:2010).

Når det gjaldt vekslinger foretatt av nigerianere i Norge, viste imidlertid uttrekket fra valutaregisteret små endringer i den totale summen som ble vekslet før og etter forbudet. Antall aktører som vekslet. gikk imidlertid en del ned, noe som innebar at det gjennomsnittlige beløpet per veksling økte. Dette kan indikere at prostitusjonspenger utgjorde en liten andel av den totale summen som ble vekslet av nigerianere. På den annen side viste informasjonen fra Pro-senteret at en relativt stor andel av nigerianske prostituerte fortsatt oppholdt seg i landet, og det faktum at det ble vekslet noenlunde like mye penger som før forbudet, kan også indikere at de prostituerte organiserte virksomheten sin på en annen måte etter årsskiftet. (EFE:2010).

3.6 INDIKASJONER PÅ MISTENKELIGE TRANSAKSJONER (MT)

I følge undersøkelses- og rapporteringsplikten, er det en rekke indikasjoner på mistenkelige transaksjoner. Listen under gjelder spesifikt for eiendomshandel, men kan også være aktuell for en del andre bransjer også:

- Kontante transaksjoner
- Bruk av bankremisser
- Uvanlig bruk av klientkonto (eks. for høyt innbetalt forskudd)
- Betaling overføres fra et land kjøper ikke har noen opplyst tilknytning til.
- Uvanlig stor egenkapital i forhold til inntekt
- Selger aksepterer tap
- Kort tid mellom erverv og videresalg
- Bruk av stråmenn
- Eiendommen kjøpes usett
- Kjøp/salg til betydelig overpris/underpris
- Unormalt transaksjonsmønster i forhold til oppdragets art, for eksempel
    - At selger ikke skal være mottaker av oppgjøret
    - At kjøper ikke skal betale selv
    - At oppgjøret deles opp i unødig mange transaksjoner
- Misforhold mellom en klients dårlige økonomiske stilling og betalingsevne i aktuell transaksjon
- Etterspørsel etter andre tjenester enn det som er normalt, for eksempel bekreftelser på oppgjør, ekstraordinære avtalepunkter, ny verditakst når annen takst foreligger.

(Eiendomsmegleren:2009)

Undersøkelses- og rapporteringsplikten inntrer selv om transaksjonen ikke gjennomføres. For eksempel vil en kundes forsøk og påfølgende avvisning fra meglerforetakets side på å betale kjøpesummen med kontante midler kunne innebære en rapporteringsplikt for meglerforetaket (Finanstilsynet:2009).

KAPITTEL 4 – OMFANG AV HVITVASKING

4.1 OMFANG AV HVITVASKING I NORGE

Den illegale økonomien i Norge omfatter store summer, og økonomisk kriminalitet utgjør "motoren" i de fleste kriminelle nettverk. Kriminelle nettverk som genererer mye kontanter, for eksempel ved salg av narkotika, varesmugling eller grove ran, hvitvasker disse i det legale markedet eller reinvesterer i ny kriminell virksomhet (www.regjeringen.no – B).

På landsbasis utgjør økonomisk kriminalitet gjennomgående omkring 2 % av samtlige anmeldte lovbrudd. I 2005 ble det anmeldt 8097 lovbrudd som omfattet økonomisk kriminalitet. Antallet anmeldte lovbrudd i denne kategorien har vært stabil de siste årene. Unntaket er 2003 hvor 15 951 lovbrudd ble anmeldt i denne kategorien. Dette skyldes én bestemt sak som førte til en rekke anmeldelser. 1 696 straffereaksjoner ble gitt for økonomisk kriminalitet i 2003 (www.regjeringen.no – B).

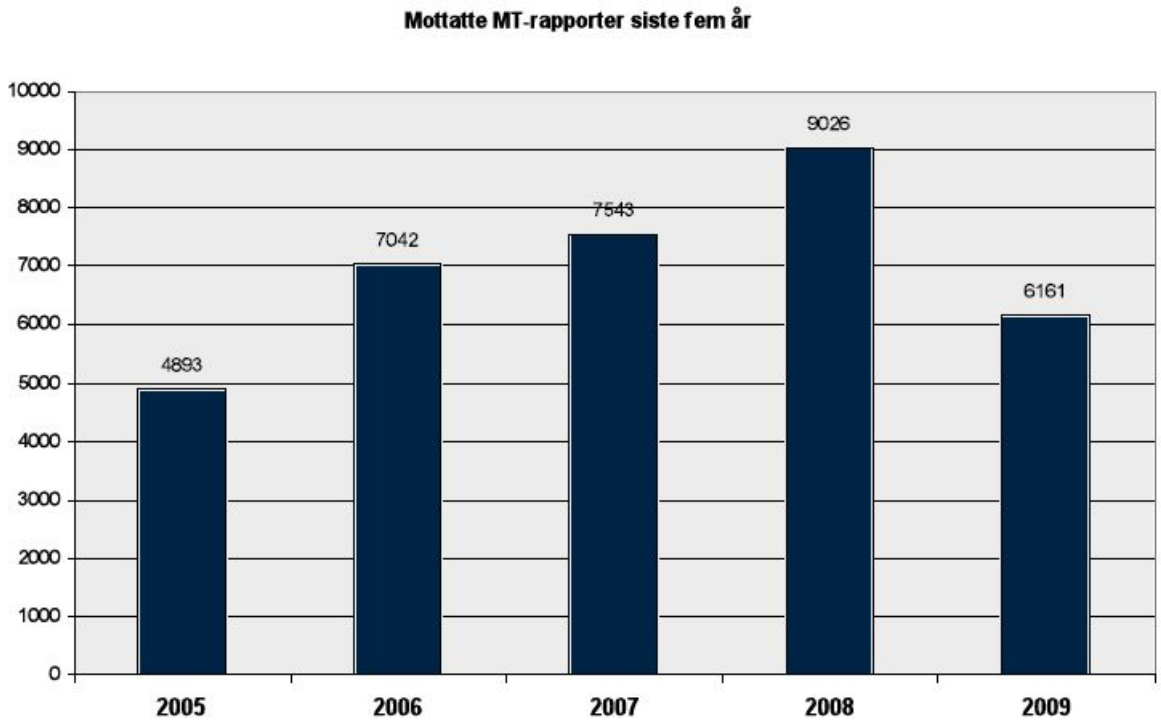
En undersøkelse blant 2000 virksomheter foretatt av SSB, viser at ca. hver femte virksomhet var offer for økonomisk kriminalitet i 2003. Mange av disse bedriftene har vært ute for flere, og enkelte for svært mange, økonomiske lovbrudd (www.regjeringen.no - B).

EFE har aldri videreformidlet mer etterretningsinformasjon til politiet og kontrollmyndighetene enn i 2009. EFE produserte 352 etterretningsrapporter i 2009, mot 243 i 2008. Økningen i antall etterretningsrapporter skyldes at bruken av systemet Ask har kommet ordentlig i gang, og at EFE derfor benytter informasjonen fra MT-rapportene på en mer effektiv måte. Antallet registrerte MT-rapporter sank med ca. 30 % i 2009. Denne nedgangen skyldes at EFE var opptatt av å få en riktigere struktur på rapporteringen. Dette medførte blant annet at enkeltstående transaksjoner som tidligere ble registrert som MT-rapporter, nå går inn som vedlegg og informasjon til den aktuelle transaksjonen eller objektet som rapporteres. Selv om antallet registrerte MT-rapporter har gått noe ned, har EFE reelt sett mottatt minst like mye informasjon i 2009 i som i 2008 (EFE:2010).

Skattebetalerforeningen gjennomførte en holdningsundersøkelse i 2008, som viser at svart arbeid i stor grad aksepteres blant det norske folk. Undersøkelsen viser at

40 prosent av de spurte synes det er greit å betale svart for mindre arbeid på hus/hytte. Like mange rapporterte også at de har betalt svart for små oppdrag. Det svenske skatteverket har gjennomført en analyse der de estimerer at manglende innbetalt skatt i Sverige utgjør ca. 5 prosent av svensk BNP. Det er ikke gjennomført en tilsvarende beregning i Norge, men det svenske estimatet kan sannsynligvis også gi et bilde av forholdene i Norge (EFE:2010).

4.2 STATISTIKK



Figur 4.2 – Mottatte MT-rapporter siste 5 år (EFE:2010).

4.2.1 UTVIKLING I ANTALL MT-RAPPORTER

I 2009 registrerte EFE 6166 MT-rapporter. Det er en nedgang på 32 % fra 2008. Nedgangen kan nesten utelukkende forklares med en lavere rapportering fra betalingsformidlingsvirksomheter. Der EFE tidligere registrerte én melding per transaksjon, registrerer de nå i større grad at flere mistenkelige transaksjoner på én person registreres i én og samme MT-rapport, noe som påvirker antallet registrerte MT-rapporter. Selv om færre rapporter registreres, er EFE av den oppfatning at de mottar mer informasjon enn tidligere, noe økningen i antallet formidlede

etterretningsrapporter kan tyde på. EFE er glade for at bankene har opprettholdt sitt rapporteringsnivå, til tross for at mange av deres ressurser har gått med til utvikling av nye fagsystemer og informasjonsarbeid om den nye hvitvaskingsloven. EFE ser det også som positivt at antallet rapporter fra revisorer og regnskapsførere fortsetter å øke. Disse rapporteringspliktige sender ofte detaljerte rapporter som gir godt grunnlag for videre undersøkelser. Forsikringsselskapene har doblet sin rapportering fra 2008, og befinner seg nå på omtrent samme rapporteringsnivå som i 2007 og 2006. Advokater rapporterte nesten dobbelt så ofte i 2009 som i 2008. EFE anser likevel antallet for å være lavt i forhold til det totale volumet av transaksjoner som går gjennom advokatvirksomheter. Rapporteringer fra bilforhandlere og øvrige selgere av verdifulle gjenstander har sunket. Kvaliteten på disse rapportene i 2009 var gjerne svak, og i verste fall feilaktig. Ofte gir denne rapporteringen lite ekstra informasjon å bygge en analyse på, og EFE må ofte kontakte den rapporteringspliktige ved behov for ytterligere opplysninger (EFE:2010).

Mottatte MT-rapporter fra de ulike virksomhetsområdene fordeler seg som følger:

	2006	2007	2008	2009
Banker	1481	2556	2073	2176
Virksomheter for betalingsformidling	5380	4656	6680	3681
Forsikringsselskaper	31	34	15	31
Verdipapirforetak	10	4	1	1
E-pengeforetak	-	2	1	0
Meglere	5	19	11	21
Revisorer	46	75	78	97
Regnskapsførere	12	15	44	58
Advokater	10	13	7	12
Forhandlere av gjenstander	27	119	109	82
Andre	7	16	7	2
Antall rapporter per år	7042	7543	9026	6161

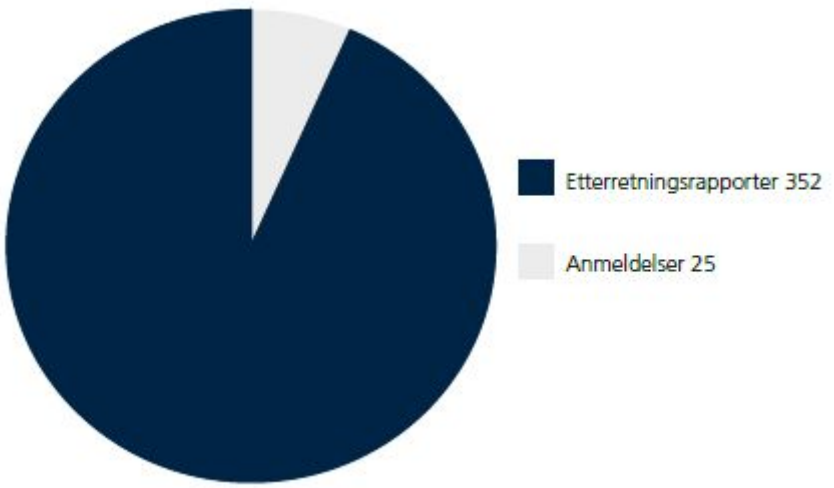
Figur 4.2.1 – MT-rapporter i forhold til virksomhet (EFE:2010).

De fleste MT-rapportene kommer fra virksomheter for betalingsformidling og banker, men det er ikke naturlig å sammenlikne antallet med antallet rapporter fra andre grupper rapporteringspliktige. Det høye antallet rapporter fra førstnevnte grupper kan ses i sammenheng med stor oppmerksomhet rundt rapporteringsplikten, i kombinasjon med erkjennelsen av at denne typen virksomhet blir brukt av kriminelle.

Bankene har også de klart største kundekretsene blant de rapporteringspliktige, og har dessuten vært omfattet av rapporteringsplikten lengst (EFE:2010).

Omfanget og innholdet i MT-rapportene varierer mellom de ulike gruppene rapporteringspliktige. En MT-rapport fra en virksomhet for betalingsformidling omhandler ofte ikke mer enn én person og én transaksjon, men disse rapporteres ofte. På den annen side er en MT-rapport fra en revisor i de fleste tilfeller mye mer omfattende og inneholder gjerne informasjon om flere personer og mange transaksjoner. Det er derfor naturlig med stor forskjell på antall mottatte MT-rapporter fra enkelte virksomhetsområder fortsatt er lavt, til tross for at det er brukt mye ressurser på foredragsvirksomhet. Årsaken er neppe mangel på transaksjoner som burde vært rapportert (EFE:2010).

4.2.2 FORHOLDET MELLOM ANTALL ETTERRETNINGSRAPPORTER OG ANMELDELSER

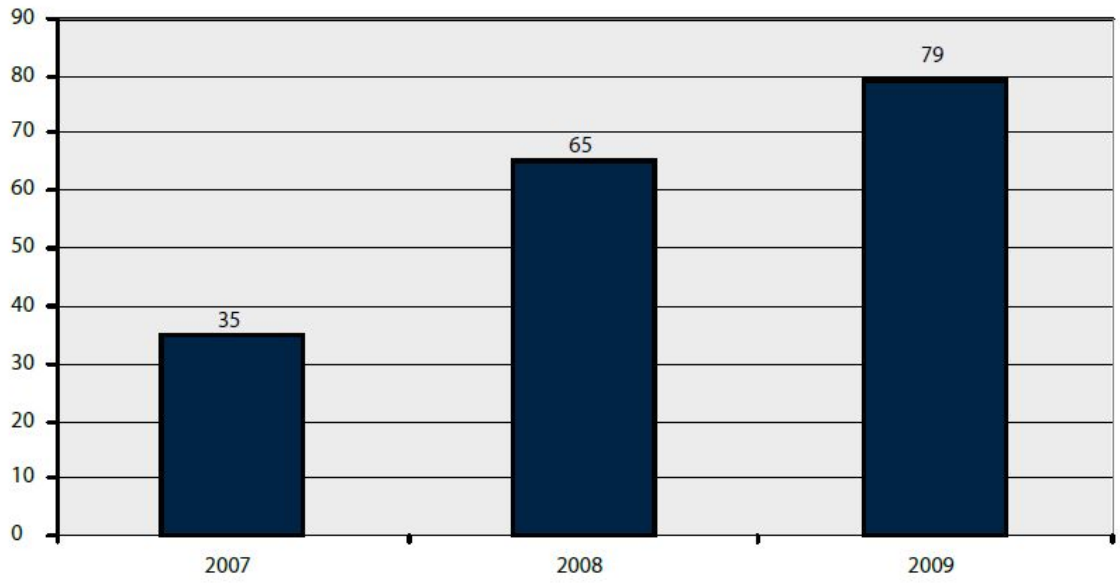


Figur 4.2.2 – Forhold mellom rapporter og anmeldelser (EFE:2010).

I 2009 utarbeidet EFE 352 etterretningsrapporter, mot 243 i 2008. Dette skyldes i stor grad at systemet Ask er blitt ordentlig etablert, og at man derfor har kunnet bruke flere ressurser på det praktiske etterretningsarbeidet. EFE leverte inn 25 anmeldelser og egenrapporter i straffesaker i 2009, mot 27 i 2008 (EFE:2010).

4.2.3 UTVIKLING I ANTALL FORESPØRSLER FRA ANDRE FIU-ER.

I 2009 så EFE at økningen i antall forespørsler fra utenlandske FIU-er fortsatte. Det ble behandlet 79 forespørsler, mot 65 i 2008 og 35 i 2007. Dette vitner om at man i større grad enn tidligere ser mulighetene for å spore objekter og pengestrømmer på tvers av landegrensene (EFE:2010).



Figur 4.2.3-2 – Utvikling i forespørsler fra andre lands FIU (EFE:2010).

4.3 HISTORIKK OVER ØKONOMISK KRIMINALITET

Statistisk sentralbyrå
Statistics Norway

1 Lovbrudd anmeldt, etter lovbruddsgruppe. 1993-2006. Absolutte tall og per 1 000 innbyggere

	I alt	Forbrytelse	Forseelse	Lovbruddsgruppe									
				Økonomisk kriminalitet	Annen vinnings-kriminalitet	Volds-kriminalitet	Seksual-kriminalitet	Narkotika-kriminalitet	Skadeverk	Miljø-kriminalitet	Arbeidsmiljø-kriminalitet	Trafikk-kriminalitet	Annen kriminalitet
				Absolutte tall									
1993	327 466	230 180	97 286	6 680	187 422	16 096	2 173	12 714	16 208	3 355	766	49 750	32 302
1994	332 771	234 941	97 830	6 375	190 686	16 865	2 102	13 550	17 084	3 686	872	47 226	34 325
1995	377 478	267 925	109 553	7 872	207 242	18 076	2 244	21 435	24 258	3 867	1 017	53 945	37 522
1996	385 446	271 205	114 241	6 698	208 813	19 299	3 518	25 009	24 665	3 711	998	52 805	39 930
1997	402 252	284 695	117 557	6 968	214 865	19 288	3 372	31 217	27 592	3 866	1 206	55 657	38 221
1998	415 472	293 799	121 673	7 502	219 949	19 839	2 945	35 144	30 470	3 813	1 260	57 370	37 180
1999	407 277	291 924	115 353	7 545	213 183	20 371	2 804	37 426	30 171	3 607	985	54 268	36 917
2000	424 918	306 526	118 392	8 280	221 577	23 572	2 772	40 730	28 828	3 383	963	56 391	38 422
2001	417 166	299 714	117 452	8 014	207 041	24 180	3 058	46 251	25 396	3 454	945	57 202	41 625
2002	437 250	319 523	117 727	7 950	226 285	25 289	3 142	45 092	22 809	2 900	887	59 339	43 557
2003	420 762	303 824	116 938	15 951	214 973	24 478	3 322	36 657	21 618	2 391	793	59 537	41 042
2004	407 377	287 821	119 556	7 915	206 250	24 874	3 608	37 259	20 345	2 399	801	62 606	41 320
2005	394 301	275 684	118 617	8 097	192 369	25 064	3 311	37 597	20 908	2 647	862	61 825	41 621
2006	400 322	277 016	123 306	7 392	187 296	25 623	3 586	41 698	22 305	2 763	831	64 874	43 954

						Per 1 000 innbyggere						
1993	76,2	53,5	22,6	1,6	43,6	3,7	0,5	3,0	3,8	0,8	0,2	11,6	7,5
1994	76,9	54,3	22,6	1,5	44,1	3,9	0,5	3,1	4,0	0,9	0,2	10,9	7,9
1995	86,8	61,6	25,2	1,8	47,7	4,2	0,5	4,9	5,6	0,9	0,2	12,4	8,6
1996	88,2	62,1	26,1	1,5	47,8	4,4	0,8	5,7	5,6	0,8	0,2	12,1	9,1
1997	91,6	64,8	26,8	1,6	48,9	4,4	0,8	7,1	6,3	0,9	0,3	12,7	8,7
1998	94,0	66,5	27,5	1,7	49,8	4,5	0,7	8,0	6,9	0,9	0,3	13,0	8,4
1999	91,6	65,7	25,9	1,7	48,0	4,6	0,6	8,4	6,8	0,8	0,2	12,2	8,3
2000	94,9	68,4	26,4	1,8	49,5	5,3	0,6	9,1	6,4	0,8	0,2	12,6	8,6
2001	92,6	66,6	26,1	1,8	46,0	5,4	0,7	10,3	5,6	0,8	0,2	12,7	9,2
2002	96,6	70,6	26,0	1,8	50,0	5,6	0,7	10,0	5,0	0,6	0,2	13,1	9,6
2003	92,4	66,7	25,7	3,5	47,2	5,4	0,7	8,1	4,7	0,5	0,2	13,1	9,0
2004	89,0	62,9	26,1	1,7	45,1	5,4	0,8	8,1	4,4	0,5	0,2	13,7	9,0
2005	85,6	59,8	25,8	1,8	41,8	5,4	0,7	8,2	4,5	0,6	0,2	13,4	9,0
2006	86,3	59,7	26,6	1,6	40,4	5,5	0,8	9,0	4,8	0,6	0,2	14,0	9,5

Figur 4.3 – Tabell over utvikling av kriminalitet fra 1993 til 2006 (www.ssb.no).

Over sees en historikk av utvikling av økonomisk kriminalitet fra 1993 til 2006. Kolonnen økonomisk kriminalitet er den som er interessant her. Denne kategorien inneholder flere faktorer enn hvitvasking, men gir allikevel et bilde av situasjonen. Økonomisk kriminalitet har holdt seg mer eller mindre stabilt de siste 15-20 år i forhold til antall saker. Dette viser seg i forhold til statistikk i Norge, men også i utlandet. Men man ser en utvikling i forhold til større saker, og man har rettet fokuset mer mot terrorfinansiering. Angrepet i New York i 2001 er det største terrorangrepet i nyere historie, og dette ble en vekker for bekjempelse av økonomisk kriminalitet og hvitvasking.

4.4 FORVENTET UTVIKLING I FREMTIDEN

I utgangspunktet var en målsetning for denne oppgaven å kartlegge prognoser for hvordan hvitvasking kan komme til å bli i fremtiden. Det viste seg at slik informasjon var veldig vanskelig å få tak i, da det ikke var mulig å finne kilder på internett eller annen litteratur om dette. Planen var da å få ta i noen personer i eksempelvis Finanstilsynet eller Økokrim som kunne uttale seg om dette.

Finanstilsynet og Økokrim var skeptiske i forhold til å komme med noen prognoser. Økokrim var speisielt vanskelige å få i tale, og grunnen til dette er at hvitvaskingssaker ofte er kompliserte. Politiet som påtalemyndighet ønsker også å holde kortene tett til brystet, og gi så lite info om slike saker som mulig. Under følger utdrag fra en epost som ble mottatt fra Økokrim i denne forbindelse:

"Statistikk over hvitvasking er et svært problematisk område, siden det ligger i sakens natur at denne økonomien forsøkes holdes skjult. Ulike myndigheter i ulike land har laget estimater over størrelsen på den svarte økonomien, men dette er selvfølgelig bare estimater og langt fra sikre

tall. Vi besitter ingen slike tall som vi går gode for. Den statistikken vi har er antall MT-rapporter, som sannsynligvis bare utgjør en liten del av det totale omfanget av hvitvasking. Det er selvfølgelig også vanskelig å spå om utviklingen framover, men det er lov å håpe at økt kjennskap til hvitvaskingsregimet og bedre rutiner hos de rapporteringspliktige fører til avdekking av mer hvitvasking enn tidligere. "

Når man ser på utviklingen de siste år, så har den vært ganske stabil. Det er derfor nærliggende å anta, at fremtiden også vil forholde seg slik. Det kan jo være at det nye regelverket og et tettere internasjonalt samarbeid, vil føre til færre hvitvaskingssaker. Men som man ofte ser når nye lover blir innført, så blir de kriminelle enda flinkere til å skjule sin virksomhet. Det kan også være at de kriminelle finner andre veier for å få hvitvasket pengene. Skatte- og avgiftskriminalitet har også holdt seg konstant de sist år på tross av gjentatt advarsler i media, og det er liten grunn til å anta at fremtiden vil bringe noe annet på den fronten.

KAPITTEL 5 – KONSEKVENSER OG INFLUERENDE FAKTORER

5.1 BAKGRUNN

Årsakssammenhenger og influerende faktorer (risikodrivere) knyttet til oprisk finner vi i:

- interne prosesser
- menneskene i organisasjonen
- selskapets systemer
- eksterne hendelser

(kilde: forelesningsnotater i operasjonell risiko).

Dette kapittelet tar for seg hva slags faktorer som spiller inn i forhold til hvitvasking. For å visualisere dette, benyttes et bayesiansk nettverk. Dette er benyttet for å gjøre illustrasjonen av både influerende faktorer og konsekvenser bedre.

Et bayesiansk nettverk er en probabilistisk grafisk modell for å modellere fenomener/situasjoner hvor vi må håndtere usikkerhet kvalitativt og kvantitativt. Bayesianske nettverk er et rammeverk for å resonnere kvantitativt om usikkerhet gitt observasjoner, og bygger på representasjon av reelle årsakssammenhenger. I denne oppgaven benyttes kun nettverket til å fremstille grafisk årsakssammenhengene. Hensikten med nettverket i denne oppgaven er at man lettere skal kunne se sammenhenger og konsekvenser mellom de ulike faktorene.

5.1.1 SAMFUNNSFAKTORER

Økokrim har i sin trendrapport 2008-2009 listet opp en rekke faktorer som er kriminalitetshemmende og en rekke faktorer som er kriminalitetsfremmende. Disse faktorene er interresante da de sier en del om hva som motiverer folk til å bedrive kriminalitet.

5.1.1.1 KRIMINALITETSFREMMENDE SAMFUNNSFAKTORER

- Teknologi og Internett gjør kommunikasjon mellom mennesker raskere og enklere. Denne utviklingen kommer også aktører som begår kriminalitet til gode. Lovbruddene er i mange tilfeller ikke nye, men de foregår på en ny arena. Ved hjelp av

teknologi kan lovbrudd gjennomføres på svært kort tid og mot mange på samme tid, samtidig som spor raskt kan slettes. Etterforsking av slike lovbrudd er ofte tids- og ressurskrevende fordi lovbruddene foregår på en global elektronisk arena – der gjerningspersonen gjerne kan være i utlandet. Etterforskingen innebærer ofte internasjonalt politisamarbeid (Økokrim:2010).

- Globaliseringen og utvidelsen av EUs indre marked innebærer at landegrenser blir et stadig mindre hinder for å flytte personer, varer, kapital og tjenester. Opprettelsen av det indre markedet er uttrykk for et ønske om blant annet å tilrettelegge for økt og enklere handel og flere transaksjoner mellom medlemsstatene. Denne utviklingen drar også aktører som begår kriminalitet nytte av. Den grensekryssende kriminaliteten blir lettere å gjennomføre, noe som gjør bekjempelsen av den vanskeligere (Økokrim:2010).

- Det norske samfunnets politiske struktur, med demokratisk styre, et godt utviklet velferdssystem og grunnleggende prinsipper om rettssikkerhet, åpner for at kriminelle aktører/nettverk fra stater med mindre velfungerende strukturer kan fristes til å etablere seg her for å drive kriminell virksomhet (Økokrim:2010).

- Det finnes ulike strukturer og fenomen – som for eksempel skatteparadis, norskregistrerte utenlandske foretak (NUF) og uformelle verdioverføringssystemer til utlandet (Hawala virksomhet) – som gir mulighet for diskresjon/tilsløring av faktiske forhold rundt blant annet identitet og eierskapsforhold. Slike forhold kan bidra til at det lettere kan begås økonomisk kriminalitet (Økokrim:2010).

- En økende sentralisering innebærer at flere flytter til sentrale strøk. Den sosiale kontrollen her er langt svakere enn på mindre steder. Dette kan igjen føre til mer kriminalitet. Sannsynligvis er dette mest aktuelt i forbindelse med tradisjonell kriminalitet, men anonymiteten som større byer gir, er også en fordel når økonomisk kriminalitet begås (Økokrim:2010).

- Mange vil hevde at dagens samfunn er preget av en hardere konkurranse enn tidligere. Særlig regnes den internasjonale konkurransen for å ha blitt hardere. En grunn kan være at det innen flere sektorer blir stadig færre og tyngre aktører, og at spillerommene for de industrielle aktørene blir mindre. Samtidig er vi også vitne til økt konkurranse mellom individer i deres kamp om posisjoner. Konkurransen kan på

begge plan bidra til å gjøre det fristende å ta i bruk ulovlige eller tvilsomme metoder (Økokrim:2010).

- Revisors rolle og posisjon er særdeles viktig i kampen mot økonomisk kriminalitet. Etter revisorloven kan revisor, uten hinder av taushetsplikten, underrette politiet dersom det i forbindelse med revisjonsoppdrag eller andre tjenester fremkommer forhold som gir grunn til mistanke om at det er foretatt en straffbar handling. Revisorer er også rapporteringspliktige etter hvitvaskingsloven. Ved mistanke om at en transaksjon har tilknytning til utbytte av en straffbar handling eller terrorfinansiering, skal rapporteringspliktige foreta en nærmere undersøkelse. Dersom undersøkelsene ikke avkrefter mistanken, skal opplysningene oversendes Økokrim. Slik rapportering finner i dag sted i kun begrenset omfang, selv om Økokrim registrerer økning i antall rapporter om mistenkelige transaksjoner fra denne virksomhetsgruppen (Økokrim:2010).

- Næringslivet benytter i stor grad fageksperter for å maksimere selskapets utbytte. Dette fører til at muligheter og smutthull utnyttes, samtidig som det utvikles kompliserte forretningsstrukturer og avtaler. Det er ressurskrevende for kontrollmyndighetene å følge opp dette, noe som kan gi rom for større grad av økonomisk kriminalitet og miljøkriminalitet (Økokrim:2010).

- Mobiliteten i arbeidslivet er stor, og én tendens er at folk skifter jobb oftere. Hvis ansatte i større grad opplever seg som tjenesteleverandører i stedet for ansatte, kan lojaliteten til arbeidsgiver bli svekket. Et utslag av dette kan bli flere tilfeller av underslag, korrupsjon eller annen illojal atferd (Økokrim:2010).

- Den private rikdommen øker, og den blir stadig mer synlig fordi mange i større grad har et ønske om å eksponere den. Å framstå som fremgangsrik blir viktigere både for bedrifter og privatpersoner. Økonomisk kriminalitet kan være en velegnet metode for å oppnå rask rikdom og status (Økokrim:2010).

- De gjeldende verdier og holdninger i et samfunn påvirker borgernes tilbøyelighet til å begå lovbrudd. En "grådighetskultur" som tidvis kommer til syne, viser handlingsmønstre der målet er å tilegne seg så store verdier som mulig, uten å vurdere om dette er fortjent eller anstendig. Det at slike handlinger blir akseptert, og til og med i noen grad blir et mål på vellykkethet, fører til liberalisering av de kulturelle

normene for hva som er akseptabelt. Jo mer allmenngyldige slike mål blir, desto sterkere vil de påvirke de kulturelle normene over tid (Økokrim:2010).

- Stigmatiseringen i forbindelse med enkelte økonomiske lovbrudd eller miljøkriminalitet er svak, særlig når det sammenlignes med mer tradisjonell kriminalitet. I enkelte sammenhenger vil det å innrømme simple tyverier av fysiske gjenstander kunne føre til sosial eksklusjon og stigmatisering, mens for eksempel skatteunndragelser eller skader på naturen/miljøet kan møtes med et skuldertrekk eller til og med positiv oppmerksomhet (Økokrim:2010).

5.1.1.2 KRIMINALITETSHEMMENDE SAMFUNNSFAKTORER

- Flere mediekanaler og mediebedrifter har ført til større offentlighet. Mediene fokuserer ofte sterkt på kriminalitet, siden dette stort sett blir betraktet som "godt stoff". Dette fører igjen til at flere er med å avdekke kriminalitet (Økokrim:2010).

- Bedrifter er mer opptatt av omdømmet sitt enn tidligere. Bevisstheten rundt lovbrudd er også voksende – både hva gjelder lovbrudd som bedriftene kan rammes av, men også hva de/deres ansatte kan gjøre seg skyldig i. Som en følge av dette styrkes rutiner for intern- og ekstern kontroll, samtidig som fokuset på etikk blir større. Dette kan føre til økt forebygging og avdekking av kriminalitet (Økokrim:2010).

- Lovreguleringen rundt økonomisk kriminalitet og miljøkriminalitet er styrket. Det samme er kontrollapparatene for å avdekke og iretteføre slike lovbrudd. Det internasjonale samarbeidet er også blitt bedre. Økt fokus og håndtering av avdekkede saker som virker forståelig og rettferdig for allmennheten, kan føre til økt forståelse og skjerpet moral (Økokrim:2010).

5.2 SLIK FOREGÅR HVITVASKING

5.2.1 HVITVASKINGENS TRE FASER

Figur 5.2.1 – hvitvaskingens 3 faser (Egenprodusert).

Utfordringen for banker og finansieringsinstitusjoner er å fange opp hvitvaskingen i de forskjellige fasene.

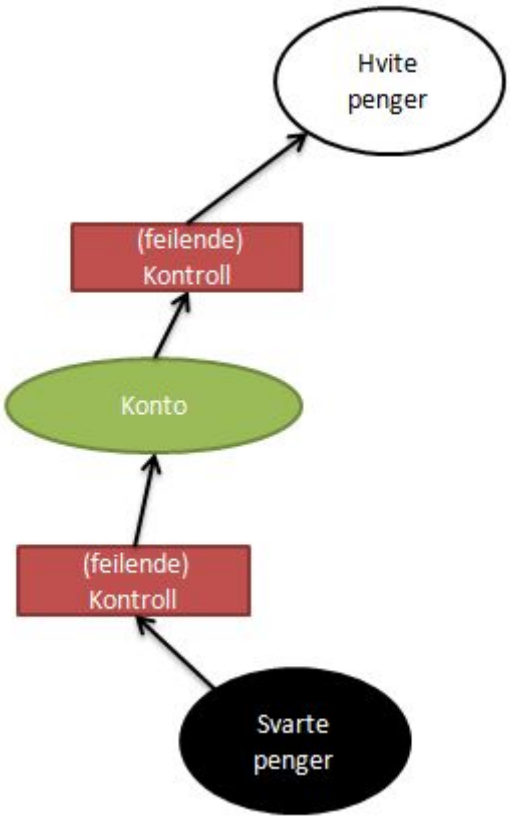
Den viktigste fasen er plasseringsfasen, da det er her pengene kommer inn i systemet. Viktige barrierer her, er identitetskontrollen og "kjenn din kunde" prinsippet. Det er viktig at bankene kjenner sin rapporteringsplikt, og melder fra om man mistenker at transaksjonen kan være midler fra kriminelt utbytte. Store kontantbeløp er det verste å bli kvitt. En mye brukt metode, er oppkjøp av vinnerbonger fra pengespill (jmf. punkt 3.4) Problemet for hvitvaskeren blir i dette tilfellet å overbevise om at man har flaks hele tiden. Dette er noe de rapporteringspliktige (spillkommisjonær i dette tilfelle) bør være klar over, og melde fra om dersom man mistenker noe kriminelt. En annen form for hvitvasking er å gjøre dette gjennom et vanlig firma. En vanlig måte å gjøre dette på, er å blande legal og illegal virksomhet. For eksempel gjennom den lokale kebabkiosken eller grønnsaksforhandlere el. virksomheter (jmf. punkt 3.4). Det finnes også eksempler på at regnskapsfører i en bedrift har samarbeidet med kriminelle ved å

skrive under for varer/tjenester som ikke er mottatt(eksempel i punkt 3.5.2.1). Spesielt tjenester er det vanlig å jukse med tjenester da det er mindre kontroll og regler for prissetting på dette, enn det er på fysiske varer (jmf. punkt 3.4).

Ved tilsløringsfasen er det viktig at man har samarbeid på tvers av institusjoner og landegrenser. Det er viktig at man overvåker konti og transaksjoner. Er det for eksempel en konto med få og store overføringer, gjerne på tvers av landegrenser, eller på forskjellige kanter av landet, bør det ringe en bjelle for den rapporteringspliktige. Selskaper med kompliserte eierstrukturer og/eller selskaper som handler med utlandet bør overvåkes og oppfølges nøye. Det er viktig for den rapporteringspliktige å rapportere dersom man har en mistanke. Siden en MT-rapport ikke er det samme som en anmeldelse, bør terskelen for å rapportere være lav. I de fleste saker har det vært mange rapporter over lengre tid, det er derfor viktig å rapportere en gang for mye slik at viktig info ikke går tapt.

I integreringsfasen er hvitvaskingen utført og pengene er disponible for den kriminelle til lovlig bruk. For mange kriminelle er det status i å ha dyre gjenstander, for eksempel luksusbiler, hus/leiligheter, smykker osv. Det er viktig at de som selger slike produkter, rapporterer dersom de mistenker at midlene kommer fra en illegal opprinnelse. Selv om hvitvaskingen på dette stadiet er ferdig utført, er det fullt mulig å spore tilbake midlene via tilsløringsfasen og plasseringsfasen. Her er det også naturlig å tenke seg at de kriminelle kan ha medsammensvorne hos f.eks. bilselgeren som får et vederlag for ikke å rapportere inn MT-rapporten.

5.2.2 HVITVASKING VED FINANSINSTITUSJONER (BANKKONTO)



Figur 5.2.2 – slik foregår hvitvasking (Egenprodusert).

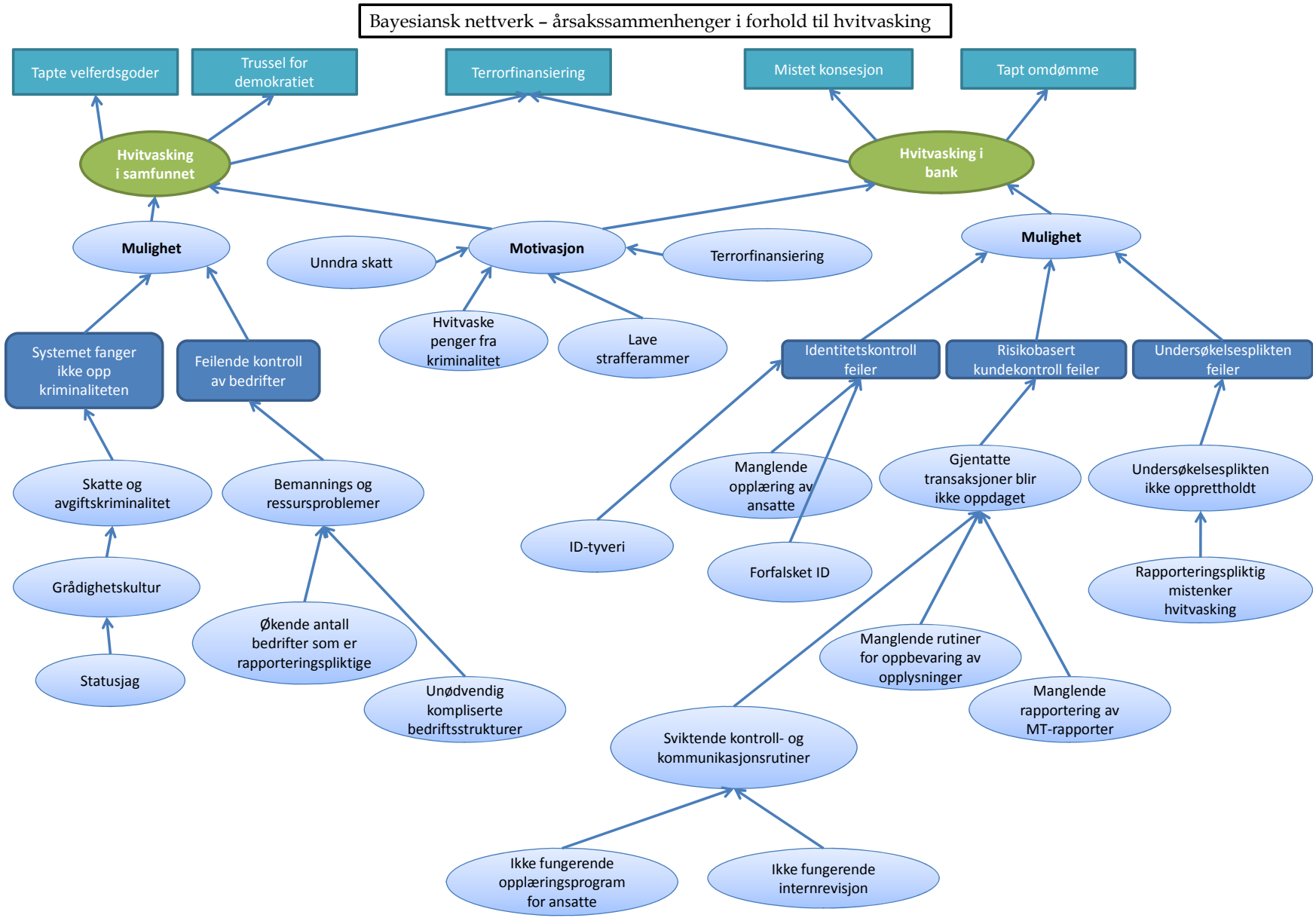
Hensikten med å hvitvaske penger, er som regel å få illegale midler lovlig inn i den legale økonomien. Den enkleste formen for hvitvasking er illustrert over. Man kan tenke seg at Hansen har et stort utbytte i kontanter han vil ha gjort hvite. Rapporteringsplikten til finansinstitusjonen ilegger en rekke plikter ved transaksjoner og opprettelse av konto. Dersom denne kontrollen feiler, vil Hansen ikke ha noen problemer med å få disse pengene inn på konto, og første fase av hvitvaskingen er unnagjort. Det neste som gjelder nå, er å tilsløre opprinnelsen og ikke skape mistanke når man skal ta i bruk pengene. En metode her kan være å dele pengene opp i mindre beløp, og gjerne overføre til flere forskjeligge konti, ofte også til utlandet.

En viktig del av det nye hvitvaskingsregelverket er identitetskontroll. Dette skal være en barriere ved opprettelse av nye kontoer. Dette er også en del av "Kjenn din kunde prinsippet" som både FATF og Basel-komiteen er veldig opptatt av (Basel:2001). Dersom det blir avkrevd en grundig sjekk av identitet ved opprettelse av konto, skal dette virke avskrekkende for å opprette konto for kriminelt bruk (slik som eksempel

3.5.2.3). De fleste er redd for å sette sitt personlige omdømme på spill. Et stadig økende problem her, er identitetstyveri. Ved å opprette konto ved bruk av falsk identitet, vil man kunne omgå denne sperren, og i verste fall skape store problemer for vedkommende som har fått sin identitet stjålet til å renvaske seg.

5.3 ÅRSAKSSAMMENHENGER

Årsakssammenhengene i den norske banknæringen og samfunnet for øvrig er organisert i et bayesiansk nettverk. En nærmere forklaring på de ulike faktorer i nettverket er gitt etter nettverket.



Figur 5.3 – bayesiansk nettverk

5.4 DISKUSJON AV BAYESIANSK NETTVERK

Det bayesianske nettverket er organisert med topphendelser som tapshendelser og videre årsakssammenhenger som fører til disse hendelsene. Topphendelsen er avhengig av ytelsen til kontrolltiltakene. De 5 tapshendelsene i nettverket er:

- Tapte velferdsgoder
- Trussel for demokratiet
- Mistet konsesjon
- Tapt omdømme
- Terrorfinansiering

5.4.1 TAPTE VELFERDSGODER

Penger som hvitvaskes stammer enten fra kriminelle handlinger, fra svart arbeid, eller fra skjulte midler hos eksempelvis skatteparadis, eller skatte/avgiftssvindel. En felles egenskap her, er at dette er penger det ellers ville blitt betalt skatt for. Disse pengene vil da ikke komme fellesskapet til gode, og samfunnet taper midler. Det er også sagt at slik svindel kan virke konkurransevridende da firmaer som snyter skatt og avgifter vil kunne tilby bedre priser siden de har lavere utgifter. Dersom pengene kommer fra vinningskriminalitet er det også noen som lider et tap, enten det er en privatperson eller en bedrift som er ranet. Dette vil på en eller annen måte føre til et tap for samfunnet. Dersom noen blir ranet, vil det ofte føre til en utbetaling av forsikring, som da vil føre til en høyere premie for alle andre.

5.4.2 TRUSSEL FOR DEMOKRATIET

Ved skatte- og avgiftskriminalitet underminerer man hele velferdssystemet og også som ytterste konsekvens demokratiet(ref. Økokrim:2008). Vårt samfunn er basert på at velferden er finansiert gjennom skatter og avgifter. Dersom tilstrekkelig mange velger å snyte dette systemet for å fremme personlig rikdom, kan hele demokratiet til slutt stå i fare. I det siste ser man mer og mer en grådighetskultur, og mange velger å gå nye veier for å tilegne seg rikdom. Dette kan føre til at folk aksepterer kriminelle handlinger på en annen måte enn tidligere, og det kan føre til en svekket rettsoppfatning(jmf. punkt 1.1). Finanskrisen vi nå er inne i, er et resultat av denne

grådighetskulturen. Folk har levd over evne over lang tid, og til slutt kollapset hele økonomien.

5.4.3 TAPT OMDØMME

En finansieringsinstitusjon er som bedrifter flest, avhengig av kunder for å overleve. Dersom rapporteringsplikten ikke overholdes, kan den ansatte straffes med bøter, eller i særlig skjerpende omstendigheter kan fengsel inntil 1 år anvendes, jfr. hvitvaskingsloven § 28. Dette gir et tap for banken, både omdømmemessig og verdimessig. Dersom det komme frem i media at en institusjon gjentatte ganger har vært offer for hvitvasking kan dette skape et tapt omdømme for bedriften. Dette kan i verste fall føre til en kundeflukt og at bedriften går konkurs.

5.4.4 MISTET KONSESJON

En finansieringsinstitusjon som blir benyttet til hvitvasking og det viser seg at rapporteringsplikten ikke er overholdt gjentatte ganger, kan i verste fall miste konsesjonen til å drive virksomhet. En insitusjon som ikke følger loven i forhold til rutiner og utstyr som kreves for å utføre tilstrekkelig anti-hvitvaskingsarbeid, straffes med dagbøter og kan også i siste instant miste konsesjonen. Det er Finanstilsynet som håndhever dette.

5.4.5 TERRORFINANSIERING

Hvitvasking av penger kan og blir brukt til finansiering av terror. Mye av årsaken til det internasjonale samarbeidet mot hvitvasking er nettopp bekjempelse av terrorfinansiering. Ved å hindre finansene håper man også å få bukt med terror på lengre sikt. I banknæringen hvitvaskes penger gjennom innskudd og transaksjoner, mens i samfunnet skjer det gjerne gjennom bedrifter, og da gjerne bedrifter med unødvendig komplisert struktur, og ofte bedrifter som handler med utlandet(se punkt 3.4). Ofte ser man en blanding av svart og hvit økonomi i de aktuelle bedriftene, noe som gjør midlene ekstra vanskelig å spore.

5.4.6 MOTIVASJON OG MULIGHET

Nettverket deles her inn i to deler, den ene delen er hvitvasking i samfunnet, og den andre i banknæringen. Med samfunnet menes her privatpersoner og bedrifter som ikke er finansinstitusjoner. Deretter deles det inn i nodene mulighet og motivasjon. For å spare plass, og fordi motivasjonen ofte er den samme i bank og samfunn, ble disse slått sammen til en. Bakgrunnen for å dele det opp på denne måten, er at man skal kunne se hvilke faktorer som spiller inn på motivasjonen man har for å bedrive hvitvasking og hvilke muligheter man har til å bedrive hvitvasking. Hensikten er videre at dette nettverket skal visualisere sammenhengene som fører til motivasjon og mulighet. Ved bekjempelse av hvitvasking kan man deretter se på mulighet og motivasjon for seg. Om man klarer å kutte motivasjonen, vil man kunne forhindre og begrense hvitvaskingen, og likeledes om man kutter muligheten vil også hvitvaskingen begrenses eller forhindres.

5.4.7 MOTIVASJONSFAKTORER

Følgende motivasjonsfaktorer er identifisert i nettverket:

- Unndra skatt

  Her menes å unndra skatt eller avgifter. Måter å gjøre dette på kan være ved å oppgi lavere inntekt enn man har, eller å skjule formuer i skatteparadis eller såkalte NUF (Norskregistrert utenlandsk selskap). Det finnes også eksempler på de som tar ut formuen i kontanter rett før nyttår, for å sette dem inn igjen etter nyttår. For å fange opp dette, finnes det egne MT-rapporter som heter 31.12 rapporter. Motivasjonen er profitt som følge av å snyte systemet for skatt og/eller avgifter. Se kapittel 3 for mer info om dette. Spesielt punkt 3.5.2.5.

- Hvitvaske penger fra kriminalitet

  Etter en kriminell handling sitter man gjerne med et utbytte. For å kunne ta disse i bruk, må pengene inn i den legale økonomien. Det er knyttet en del utfordringer til å få disse inn i økonomien uten å vekke mistanke. Kapittel 3 tar for seg mange av disse metodene. Motivasjonen her er å kunne ta i bruk midler som stammer fra kriminelle handlinger.

- Lave strafferammer

  Norge opererer med lave strafferammer i forhold til mange andre land i verden. Det er derfor naturlig at en del kriminelle og kriminelle nettverk velger å etablere seg i Norge fremfor andre land, da risikoen er lavere for å få lang straff er lavere her. Motivasjonen i dette tilfelle blir en ren kost/nytte kalkulasjon i forhold til straff dersom man blir tatt.

- Terrorfinansiering

  Terrorfinansiering er tidligere nevnt som en tapshendelse, men det vil også være en motivasjon. Dersom man ønsker å bedrive terror, trenger man å finansiere dette på et vis. For å finansiere gjør man gjerne kriminelle handlinger, og for å kunne ta i bruk midlene, må disse hvitvaskes. Motivasjonen i dette tilfelle blir da å skaffe penger til terrorhandlinger, og da gjør man kriminelle handlinger som fører til et utbytte som må hvitvaskes.

5.4.8 MULIGHET FOR HVITVASKING I SAMFUNNET

Nettverket tar her for seg punktene

- Feilende kontroll av bedrifter
  - Unødvendig kompliserte bedriftsstrukturer

    Som en følge av at regelverket og oppfølgingen i forhold til hvitvasking har blitt såpass mye strengere i senere tid, er det blitt vanligere for kriminelle aktører som ønsker å hvitvaske penger gjennom legale bedrifter å organisere bedrifter med kompliserte strukturer uten at det er noen grunn til det. På den måten er det lettere å skjule midler og midlenes opprinnelse. Dette gjør bedriftene også vanskeligere å kontrollere, og også mer ressurskrevende. Dette fører indirekte til bemannings- og ressursproblemer. Punkt 3.4 har mer om dette

  - Økende antall bedrifter som er rapporteringspliktige

    Det blir stadig flere bedrifter som omfattes av rapporteringsplikten. Det nye lovverket mot hvitvasking, omfatter flere bedrifter enn tidligere

uten at kontrollmyndighetene har fått tildelt flere ressurser (ref EFE:2010). I tillegg har det nye regelverket ført til omstrukturering av MT-rapporter, samt innført nye rutiner som må implementeres (ref EFE:2010). Denne omstruktureringen krever opplæring av rapporteringspliktige og kontrollmyndigheter. Dette fører til bemanningsproblemer som igjen fører til at man ikke får kontrollert bedriftene grundig nok, og dermed har man mulighet for hvitvasking uten at det fanges opp av myndighetene.

- Bemannings og ressursproblemer

  Bemannings- og ressursproblemer fører til at bedriftene ikke kontrolleres ofte og grundig nok i forhold til kravene i regelverket.

- Systemet fanger ikke opp kriminaliteten

  Et stadig jag etter status og eksponering av personlig rikdom, fører til at mange ønsker dette uten å tenke over om det er fortjent eller passende. Dette leder da til en grådighetskultur hvor man gjør hva som helst for å skaffe seg rikdommen. Dette leder da til at man jukser på skatt og avgifter for å tilegne seg denne rikdommen. En manglende stigmatisering i samfunnet generelt til denne typen kriminalitet er også en pådriver for dette (jmf. punkt 5.1.1.1).

5.4.9 MULIGHETER FOR HVITVASKING I BANKNÆRINGEN

Nettverket tar her for seg punktene:

- Identitetskontrollen feiler

  Den lovbaserte identitetskontrollen feiler. Årsakene til dette kan være:

  - ID tyveri

    Et økende problem er ID-tyveri og det kan få store konsekvenser for de som er utsatt for dette. I forhold til hvitvasking kan det være at de som får stjålet identiteten sin, får opprettet en konto i sitt navn som brukes til

hvitvaskingsformål. Mange som har fått frastjålet sin identitet, bruker langt tid, ofte mange år på å renvaske seg.

- Manglende opplæring av ansatte

  Hvitvaskingsregelverket er komplisert, og mange ansatte er kanskje ikke klar over gjeldende regler. Dette kan føre til at identitetskontrollen feiler, og særlig i forhold til bedrifter og reelle rettighetshavere, eller kontrollen med fysisk ID for fysiske personer. Kapittel 2 har mer om dette.

- Forfalsket ID

  Forfalsket ID kan benyttes til å opprette konto i falsk ID til å benyttes til hvitvaskingsformål.

- Risikobasert kundekontroll feiler

Den risikobaserte kundekontrollen kan feile. Årsaker til dette kan være:

- Gjentatte transaksjoner blir ikke oppdaget

  Økokrim er ofte avhengig av at det foretas mange transaksjoner før en sak oppdages. Dette er også vanlig i forhold til hvitvasking da man gjerne deler opp beløp for ikke å tiltrekke for mye mistanke.

  - Manglende rapportering av MT rapporter

    Dersom en MT rapport ikke blir sendt inn pga. svikt hos den rapporteringspliktige, forsvinner også noe av grunnlaget for at Økokrim skal kunne etterforske saken. Dersom hvitvaskingssaker skal kunne oppdages er det svært viktig at disse rapportene sendes inn. Det er viktig at den rapporteringspliktige er klar over at han ikke risikerer noe ved å sende en slik rapport, da den ikke gjelder som anmeldelse. I følge hvitvaskingsloven § 28 kan også den rapporteringspliktige selv risikere straff dersom han lar være å rapportere.

- Manglende rutiner for oppbevaring av opplysninger

  Dersom opplysninger ikke blir oppbevart og benyttet slik som foreskrevet i regelverket, kan det føre til at viktig informasjon går tapt, og man mister grunnlag for å kunne følge opp en mistenkelig kunde.

- Sviktende kontroll- og kommunikasjonsrutiner

  Kontroll og kommunikasjonsrutiner er viktig for å avdekke hvitvaskingen. Årsakene til at dette svikter kan være:

  - Ikke fungerende opplæringsprogram for ansatte

    Dersom de ansatte i institusjonen ikke har gode nok kunnskaper om rutinene kan dette føre til svikt.

  - Ikke fungerende internrevisjon

    Dersom internrevisjonen i institusjonen ikke fungerer skikkelig, kan dette kanskje ikke avdekke rutiner som ikke er gode nok.

- Undersøkelsesplikten feiler
  - Undersøkelsesplikten ikke opprettholdt
    - Rapporteringspliktig mistenker hvitvasking

Dette punktet er for å understreke viktigheten av undersøkelses- og rapporteringsplikten. Dersom en rapporteringspliktig mistenker at transaksjonen er fra kriminelle kilder har han en plikt til å undersøke videre for å bekrefte eller avkrefte mistanken. Dersom han oppdager noe mistenkelig har han da en plikt til å rapportere forholdet til Økokrim. Kapittel 2 gjør nærmere rede for rapporteringsplikten.

5.5 BARRIERER OG KONTROLLFUNKSJONER MOT HVITVASKING I NORGE

Når man snakker om risikostyring og risikohåndtering, snakker man ofte om hva man kan gjøre for å forhindre uønskede utfall. Disse kalles for barrierer og kontrollfunksjoner i litteraturen. Dette kapittelet gjør rede for hva slags barrierer og kontrollfunksjoner den norske banknæringen opererer med i forhold til hvitvasking.

Ny hvitvaskingslov trådte i kraft 15.04.2009. Formålet med loven er å bekjempe hvitvasking av utbytte fra straffbare handlinger. Loven medfører en rekke forpliktelser som rapporteringspliktige er pålagt å etterleve. Under følger en kort oppsummering av sentrale plikter i henhold til loven

- Identitetskontroll
- Registrering og oppbevaring av opplysninger
- Undersøkelses- og rapporteringsplikt
- Interne kontroll- og kommunikasjonsrutiner

Hvitvaskingsloven innebærer også forpliktelser for Økokrim, herunder

- Sletting av opplysninger
- Utlevering av opplysninger til Kontrollutvalget

(www.hvitvasking.no - H).

5.5.1 IDENTITETSKONTROLL

Ved etablering av kundeforhold skal rapporteringspliktige kreve gyldig legitimasjon av kunden. Kundeforhold anses i følge forskriften etablert når kunden kan bruke den rapporteringspliktiges tjenester.

5.5.1.2 NYE PRIVATKUNDER

Nye privatkunder må opplyse om navn, fødselsnummer eller D-nummer, fast adresse og fremvise legitimasjon. I tillegg må man opplyse om:

- Kundeforholdets formål og tilsiktede art
- Hvorfor du ønsker å gjennomføre større transaksjoner
- Hvor pengene kommer fra eller hva de skal brukes til
- Du eller noen nærstående har et høytstående verv eller stilling i utlandet

5.5.1.3 NYE BEDRIFTSKUNDER

Bedriftskunder må i tillegg opplyse om foretaksnavn, organisasjonsnummer og eierforhold. Du vil bli spurt om privatpersoner har direkte eller indirekte eierandeler på mer enn 25 prosent, eller om noen på annen måte kontrollerer virksomheten.

Representanter for bedriften eller personer med disposisjonsrett over bedriftens midler, må legitimere seg samt dokumentere sin rett til å opptre på vegne av bedriften.

5.5.1.4 EKSISTERENDE KUNDER

Alle må være forberedt på å svare på spørsmål og fremlegge gyldig legitimasjon. Dette vil typisk kunne skje dersom det fremkommer nye opplysninger om ditt kundeforhold eller dine transaksjoner. Finansnæringen må kunne dokumentere overfor tilsynsmyndighetene at næringen oppfyller lovens krav til kundekontroll av alle (www.hvitvasking.no – K).

Kundekontrollen er den viktigste kontrollen for hvitvasking sin del. Og spesielt er dette viktig ved opprettelse av kundeforhold. Dette er første instans i hvitvasking sin del, og det er her viktig å undersøke alle detaljer skikkelig. Identitetstyveri er et stadig økende problem, og å opprette konto i en falsk identitet er et nyttig verktøy for hvitvaskere. Ved å opptre med falsk identitet slipper man å risikere sitt eget navn og rennome, og også risiko for bøter eller fengsel.

Dersom denne kontrollen feiler, kan de kriminelle fritt opprette en konto, og første del av hvitvaskingen kan begynne. Som nevnt i tidligere eksempel (punkt 3.5.2.3), er det

nettopp denne kundekontrollen som kan skremme vekk kriminelle fra å hvitvaske gjennom en bank.

5.5.2 REGISTRERING OG OPPBEVARING AV OPPLYSNINGER

Ved opprettelse av kundeforhold skal rapporteringspliktige registrere kundeopplysninger og oppbevare disse opplysningene forsvarlig i fem år. Dette er viktig da hvitvaskingssaker ofte er kompliserte og ofte blir tilfellene avslørt gjennom flere MT-rapporter over lengre tid. Dersom man ikke har et godt og oversiktlig system for registrering og oppbevaring kan mye verdifull data gå tapt, og man risikerer at sakene ikke blir oppdaget. Iht. personvernloven skal opplysningene slettes etter 5 år.

5.5.3 UNDERSØKELSE OG RAPPORTERING

Etter hvitvaskingsloven § 7 første ledd skal den rapporteringspliktige gjøre selvstendige undersøkelser når det oppstår mistanke om at en transaksjon har tilknytning til utbytte av straffbar handling.

Disse kontrollene er kritiske for å oppdage hvitvaskingen. Rapporteringsplikten er særdeles viktig å overholde da det er disse rapportene som skaper grunnlaget

Hva er en mistenkelig transaksjon?

Etter hvitvaskingsloven § 7 er det tilstrekkelig at man har en "vag mistanke" for at undersøkelsesplikten skal inntre. Hensikten med undersøkelsene er å få bekreftet eller avkreftet mistanken. Det er derfor ikke grunn til å stille strenge krav til mistanke før undersøkelsesplikten inntrer (www.hvitvasking.no – I).

Mistanken trenger heller ikke være knyttet til formening om hvilken straffbar handling som eventuelt skulle være begått for at det skal oppstå undersøkelsesplikt (www.hvitvasking.no – I).

Mistanken kan også helt eller delvis være begrunnet i forhold som ikke er knyttet til den konkrete transaksjonen. En transaksjon er i mange tilfeller i seg selv ikke mistenkelig, men kjennskap til kundens økonomiske stilling kan gjøre at man skjønner

at pengene som transaksjonen gjelder ikke kan ha en lovlig kilde. Det mistenkelige forhold kan også være knyttet til en tredjepart (www.hvitvasking.no – I).

Kredittilsynets rundskriv 9/2004 punkt 2.10 gir eksempler på "mistenkelige transaksjoner" som kan medføre en plikt til å foreta nærmere undersøkelser. Forskriften til hvitvaskingsloven inneholder ikke noen definisjon på hva som er en "mistenkelig transaksjon". I forskriftens § 10 første ledd er det gitt anvisning på diverse forhold som kan utløse plikten til å foreta nærmere undersøkelser (www.hvitvasking.no – I).

• **Transaksjonen synes å mangle et legitimt formål.**

Det kan eksempelvis være et oppdrag hvor pengesummen skal gå frem og tilbake mellom ulike konti innen en gitt tidsramme, at samme beløp går frem og tilbake mellom ulike institusjoner iht. et gitt oppdrag, og at en større sum splittes i flere mindre summer, men samles igjen på en ny konto (www.hvitvasking.no – I).

• **Transaksjonen er usedvanlig stor eller kompleks, eller er uvanlig i forhold til kundens kjente forretningsmessige eller personlige transaksjoner.**

Det blir her snakk om skjønn. En transaksjon kan være stor i forhold til én kunde, mens den er helt normal i forhold til en annen. Institusjonene må her nytte sine kunnskaper om den enkelte kunde. "Kjenn-din-kunde"-prinsippet inngår her som helt sentralt (www.hvitvasking.no – I).

• **Transaksjonen foretas til eller fra en kunde i et land eller område som ikke har tilfredsstillende tiltak mot hvitvasking eller terrorfinansiering.**

Her må særlig aktsomhet vises i forhold til transaksjoner utenfor FATF-området. Det er grunn til å være særlig observante overfor transaksjoner med kunder eller institusjoner i land med strenge sekresjonsbestemmelser, som tilbyr høy avkastning og skattefritak. På www.fatf-gafi.org finnes en oversikt med informasjon om tiltak mot land og områder, som ikke samarbeider i kampen mot hvitvasking og terrorfinansiering ("NCCT Initiative") (www.hvitvasking.no – I).

• **Transaksjonen på annen måte har en uvanlig karakter**

Det blir her snakk om skjønn. Som eksempler nevnes:

- Rask og ekstraordinær nedbetaling av lån med kontanter
- Dersom det er et vesentlig misforhold mellom dokumentert betjeningsevne (inntekter, formue mv.) og lånebeløpet samt avtalte nedbetalingsbetingelser (ekstraordinær nedbetaling), kan det være en indikasjon på hvitvasking.
- Bruk av bankremisser som stadig blir fornyet
- Større vekslingsoperasjoner når gamle pengesedler blir ugyldige
- Bruk av ukurante betalingsmidler i forhold til den underliggende operasjon
- Store kontanttransaksjoner
- Bruk av betalingskort, hvor uvanlig mange store transaksjoner finner sted over et kort tidsrom

(www.hvitvasking.no – I).

Et område som er særlig utsatt for hvitvasking og terrorfinansiering, er valutavirksomhet. Slik virksomhet omfatter valutaveksling og betalingsformidling mot utlandet (www.hvitvasking.no – I).

Det er også grunn til å ha særskilt årvåkenhet rettet mot forretningsområder der det er lite eller ingen personkontakt med kunden (www.hvitvasking.no – I).

De ovennevnte "signalene" på mulig hvitvasking er ment som eksempler. Det er høyst sannsynlig flere eksempler. Dette er et område i stadig utvikling, og rapporteringspliktige må følge med på nye trender og metoder og innlemme disse i sine opplæringsprogrammer. FATF publiserer mange rapporter med informasjon om nye hvitvaskingsmetoder (www.hvitvasking.no – I).

5.5.4 KONTROLL OG KOMMUNIKASJONSRUTINER

Rapporteringspliktige skal etablere forsvarlige interne kontroll- og komunikasjonsrutiner som sikrer oppfyllelse av pliktene og bestemmelsene i henhold til loven. Loven sier videre at:

- Rutinene skal være skriftlige og fastsatt på øverste nivå hos den rapporteringspliktige.
- En utpekt person i ledelsen skal ha et særskilt ansvar for oppfølging av rutinene.
- Det skal gjennomføres opplæringsprogrammer og oppfølging for ansatte og andre personer som utfører oppgaver til oppfyllelse av plikter etter loven

(www.hvitvasking.no – J)

5.5.5 ØKOKRIMS PLIKTER OG KONTROLLUTVALGET FOR TILTAK MOT HVITVASKING

Hvitvaskingsloven medfører også plikter for ØKOKRIM. Dette gjelder i forhold til sletting av opplysninger og utlevering av opplysninger til Kontrollutvalget for tiltak mot hvitvasking av utbytte fra straffbare handlinger mv (www.regjeringen.no – C).

Kontrollutvalget for tiltak mot hvitvasking av utbytte fra straffbare handlinger mv. har eksistert siden 1995, og medlemmene er nå oppnevnt av Kongen med hjemmel i lov om tiltak mot hvitvasking og terrorfinansiering mv. (hvitvaskingsloven § 31). Bestemmelsene i hvitvaskingsloven utfylles av forskrift om kontrollutvalget for tiltak mot hvitvasking av utbytte fra straffbare handlinger (www.regjeringen.no – C).

Kontrollutvalgets hovedoppgave er å påse at rettssikkerhets- og personvernhensyn ivaretas i forbindelse med Økokrims behandling av opplysninger de mottar i medhold av hvitvaskingsloven (www.regjeringen.no – C).

Innenfor dette området har Kontrollutvalget tre hovedoppgaver:

- Kontrollutvalget skal føre kontroll med Økokrims behandling av opplysninger om mistenkelige transaksjoner (MT-rapporter) banker og andre rapporteringspliktige sender inn til Økokrim (hvitvaskingsloven § 18)

- Kontrollutvalget skal føre kontroll med Økokrims pålegg overfor en bank eller en annen rapporteringspliktig om ikke å gjennomføre en transaksjon som utløser undersøkelsesplikt (hvitvaskingsloven § 19)

- Kontrollutvalget skal føre kontroll med at Økokrim oppfyller plikten til å slette opplysninger de mottar i MT-rapporter senest fem år etter opplysningene ble registrert hos Økokrim med mindre det i løpet av denne tiden er registrert nye opplysninger, eller det er foretatt etterforsknings- eller rettergangsskritt mot den opplysningene gjelder (hvitvaskingsloven § 29).

(www.regjeringen.no – C).

Kontrollutvalget gjennomfører meldte og uanmeldte kontrollbesøk hos Økokrim. Utvalget blir i møtene med Økokrim løpende orientert om status for antall registrerte meldinger (MT-rapporter) i hvitvaskingsdatabasen og mottar informasjon om andre forhold knyttet til enhetens løpende virksomhet. (www.regjeringen.no – C).

Kontrollutvalget skal også undersøke klager fra enkeltpersoner eller organisasjoner vedrørende Økokrims behandling av mottatte opplysninger (forskrift om kontrollutvalget for tiltak mot hvitvasking § 4). Utvalget kan i tillegg til dette, av eget tiltak, ta opp enhver sak eller ethvert forhold i tilknytning til Økokrims bruk av mottatte opplysninger (www.regjeringen.no – C).

Kontrollutvalget skal hvert år gi Finansdepartementet en rapport om sin virksomhet, og denne rapporten er offentlig. Utvalget kan gi særskilt rapport eller melding til departementet i enkeltsaker. Dersom utvalget finner kritikkverdige forhold, skal disse rapporteres særskilt til departementet (www.regjeringen.no – C).

5.6 HVITVASKING – EN TRUSSEL FOR NORSK BANKNÆRING?

Hvitvasking er en trussel for den norske banknæringen. De største konsekvensene for banknæringen er tap av penger, renommé og i verste fall mistet konsesjon. Dersom det kommer ut at en institusjon har blitt benyttet til hvitvasking gjentatte ganger, vil det kunne føre til en kundeflukt og tapte inntekter for institusjonen. I verste fall vil det kunne føre til en tapt konsesjon for bedriften og en avvikling av selskapet. Alle finansinstitusjoner har derfor en egeninteresse i å forhindre hvitvasking og en plikt gjennom hvitvaskingsregelverket.

Trusselen er stor for den norske banknæringen, og også internasjonalt. Dette ser man ved at det stadig kommer nye lovverk for å forhindre hvitvasking. De siste 20 år har

det også blitt et stadig større internasjonal samarbeid for å få bukt med problemet. Med den teknologiske utviklingen vi ser i dag, er det stadig enklere å flytte penger med få klikk. Dette gjør det enkelt å flytte store summer med få tastetrykk hvor som helst i verden. En stor utfordring, er såkalte skatteparadis (se punkt 3.4) hvor det er enkelt å skjule penger. Disse finnes det fortsatt mange av, men de får stadig større press på seg gjennom det internasjonale samarbeidet. Ved å bli kvitt disse, vil også trusselen for næringen lette.

5.7 HVITVASKING – EN TRUSSEL FOR SAMFUNNET?

Hvitvasking er en trussel for samfunnet. Hvitvasking i form av skatteunndragelser gjør at demokratiet og velferdssystemet står i fare. Hvitvasking som kommer fra vinningskriminalitet påfører samfunnet et direkte tap i form av kroner og øre fra kriminalitetshandlingen, og det faktum at disse midlene blir det heller ikke betalt skatt av. Hvitvasking som ender med terrorfinansiering bidrar til at samfunnet blir utrygt, og vil i verste fall ende med krig og dødsfall.

En stor trussel for samfunnet er en stadig økende grådighetskultur. Grådighetskulturen fører med seg en generell aksept av økonomisk kriminalitet. De færreste blir stigmatisert av å snyte på skatten, og i mange miljøer er dette til og med sett på som positivt, og blir møtt med en klapp på skulderen. Mange glemmer at de pengene vi betaler gjennom skatter og avgifter blir brukt på subsidier av goder, og til helseordninger. Ved å snyte staten på denne måten vil staten få mindre penger tilgjengelig til dette, og kan i verste fall ende med å få en stor statsgjeld fordi folk benytter seg av svarte tjenester, unnlater å oppgi formue, og generell annen skatte- og avgiftssvindel.

KONKLUSJON / VIDERE ARBEID

Denne oppgaven har tatt for seg hvitvasking som problem i samfunnet og banknæringen. Oppgaven har tatt for seg lovverk, omfang, og årsakssammenhenger i forhold til hvitvasking med hovedfokus på Norge, og også hvordan det internasjonale arbeidet fungerer.

Kampen mot hvitvasking er en vanskelig kamp. Som all annen kriminalitet klarer alltid de kriminelle å finne nye metoder når nye regler dukker opp. Kampen mot hvitvasking er derfor avhengig at man har et strengt lovverk, at man har et sterkt fokus på dette i banknæringen og andre næringer. Det er viktig at de ansatte i banknæringen og andre rapporteringspliktige næringer kjenner sin undersøkelses- og rapporteringsplikt og følger opp dette med gode rapporter slik at det blir mulig å få denne kriminaliteten til livs.

Den nye rapporteringsplikten som ble innført av det nye hvitvaskingsregelverket er i ferd med å implementeres. Men kunnskapen om, holdningen til og oppfølgingen av undersøkelses- og rapporteringsplikten varierer sterkt blant de rapporteringspliktige. Man ser en økning av rapportering blant regnskapsførere og revisorer, og det er en positiv trend. Utviklingen er også positiv for enkelte andre grupper, men jevnt over er det et betydelig forbedringspotensial her. Kvaliteten på rapportene er meget varierende, og i en del tilfeller kan den karakteriseres som svak og/eller feilaktig. Her har både EFE, tilsynsmyndigheter og de rapporteringspliktige utfordringer for å oppnå bedre etterlevelse av regelverket. Et satsingsområde for EFE blir å få de rapporteringspliktige til å sende inn kvalitativt bedre MT-rapporter.

Videre arbeid kan være å fokusere mer på det internasjonale arbeidet. Denne oppgaven tar for seg noe, men den har mest fokus på Norge og norges arbeid. Et annet punkt er videre oppfølging av hvordan lovverket endrer seg i fremtiden, og hvordan utviklingen blir i forhold til rapportering av MT-rapporter og kvaliteten på disse. Slik det er nå, er kvaliteten som tidligere nevnt veldig varierende. Man er helt nødvendig av gode rapporter for at kampen mot hvitvasking skal være effektiv, og derfor kan det være interresant å se hvordan dette vil endre seg dersom kvaliteten på rapportene blir bedre.

REFERANSER / KILDER

Basel:2001	Basel Committee on Banking Supervision, Customer due diligence for banks.
EFE:2010	Økokrims (EFE) årsrapport 2009
Eiendomsmegleren:2009	Eiendomsmegleren 4/2009
Finansdepartementet:2004 - A	Finansdepartementets proposisjon nr. 72 2002-2003
Finansdepartementet:2004 - B	Finansdepartementets proposisjon nr. 81 2002-2003
Finansdepartementet:2009	Finansdepartementets proposisjon nr. 3 2008-2009
Finanskomiteen:2009	Innstilling O. nr. 42(2008–2009) - Innstilling til Odelstinget fra finanskomiteen
Finanstilsynet:2009	Finanstilsynets (Kredittilsynets) rundskriv 8/2009
NOU:2007	Norges offentlige utredninger 2007:10 – Innføring av EUs tredje hvitvaskingsdirektiv.
Økokrim:2008	Økokrims trendapport 2007
Økokrim:2010	Økokrims trendrapport 2008-2009
www.abcnyheter.no	http://www.abcnyheter.no/abc-penger/nyheter/100430/190-skjulte-millioner-pa-ostlandet-avslort
www.fatf-gafi.org - A	http://www.fatf-gafi.org/document/52/0,3343,en_32250379_32236869_34027188_1_1_1_1,00.html
www.fatf-gafi.org - B	http://www.fatf-gafi.org/pages/0,3417,en_32250379_32236836_1_1_1_1_1,00.html

www.hvitvasking.no - A	http://www.hvitvasking.no/Hvitvasking/Hva-er-hvitvasking/
www.hvitvasking.no - B	http://www.hvitvasking.no/Hvitvasking/Hvorfor-bekjempe-hvitvasking/
www.hvitvasking.no - C	http://www.hvitvasking.no/Internasjonalt-samarbeid/De-forste-initiativene/
www.hvitvasking.no – D	http://www.hvitvasking.no/Rapportering-til-Okokrim/Hvem-har-rapporteringsplikt/
www.hvitvasking.no – E	http://www.hvitvasking.no/Rapportering-til-Okokrim/Nar-skal-det-rapporteres/
www.hvitvasking.no – F	http://www.hvitvasking.no/Rapportering-til-Okokrim/Straff-for-manglende-rapportering/
www.hvitvasking.no – G	http://www.hvitvasking.no/Nyhetsarkiv/Rettsavgjorelser/Skjerpet-straff-i-Norgeshistoriens-storste-Hawalasak/
www.hvitvasking.no - H	http://www.hvitvasking.no/Lov-og-forskrift/
www.hvitvasking.no - I	http://www.hvitvasking.no/Begrepsavklaring/Hva-er-en-mistenkelig-transaksjon/
www.hvitvasking.no - J	http://www.hvitvasking.no/Lov-og-forskrift/Hvitvaskingsloven/Kontroll-og-kommunikasjonsrutiner/
www.hvitvasking.no - K	http://www.hvitvasking.no/Lov-og-forskrift/Hvitvaskingsloven/Identitetskontroll/
www.lovdata.no	http://www.lovdata.no/all/tl-19020522-010-018.html
www.regjeringen.no - A	http://www.regjeringen.no/nb/dep/fin/dok/nouer/2002/nou-2002-14/10.html?id=117934

www.regjeringen.no - B	http://www.regjeringen.no/nb/dep/jd/tema/korrupsjon_og_hvitvasking/omfang-av-okonomisk-kriminalitet.html?id=418107
www.regjeringen.no - C	http://www.regjeringen.no/nb/dep/fin/tema/Finansmarkedene/kontrollutvalget-for-tiltak-mot-hvitvask.html?id=544546

FIGURLISTE

Universitetet i Stavanger

Appendix A – Hvitvaskingsloven

LOV 2009-03-06 nr 11: Lov om tiltak mot hvitvasking og terrorfinansiering mv. (hvitvaskingsloven)

DATO:	LOV-2009-03-06-11
DEPARTEMENT:	FIN (Finansdepartementet)
PUBLISERT:	I 2009 hefte 3
IKRAFTTREDELSE:	2009-04-15
SIST-ENDRET:	LOV-2009-06-19-48 fra 2009-12-21
SIST-ENDRET:	LOV-2009-12-11-127
ENDRER:	LOV-1985-05-24-28 , LOV-2003-06-20-41
SYS-KODE:	BG20a, BG26j, D02
NÆRINGSKODE:	81, 810, 9121
KUNNGJORT:	06.03.2009 kl. 13.45
KORTTITTEL:	Hvitvaskingsloven - hvvl.

INNHOLD

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

Jf. EØS-avtalen vedlegg IX nr. 23b (direktiv 2005/60/EF). - Jf. *tidligere* lov 20 juni 2003 nr. 41.

Kapittel 1. Innledende bestemmelser

§ 1. *Lovens formål*

Lovens formål er å forebygge og avdekke transaksjoner med tilknytning til utbytte av straffbare handlinger eller med tilknytning til terrorhandlinger.

§ 2. *Definisjoner*

I denne lov forstås med:

1. rapporteringspliktige: personer som nevnt i § 4,
2. transaksjon: enhver overføring, formidling, ombytting eller plassering av formuesgoder,
3. reelle rettighetshavere: fysiske personer som i siste instans eier eller kontrollerer en kunde eller som en transaksjon gjennomføres på vegne av. En fysisk person skal i alle tilfelle regnes som reell rettighetshaver dersom vedkommende:
   a) direkte eller indirekte eier eller kontrollerer mer enn 25 prosent av eierandelene eller stemmene i et selskap, unntatt selskap som har finansielle instrumenter opptatt til notering på et regulert marked i EØS-stat eller er underlagt informasjonsplikt tilsvarende det som gjelder ved notering på et regulert marked i EØS-stat,
   b) utøver kontroll over ledelsen av en juridisk person på annen måte enn nevnt i bokstav a,
   c) ifølge vedtekter eller på annet grunnlag skal motta 25 prosent eller mer av formuesgodene i en stiftelse, et fond eller en tilsvarende juridisk person eller formuesmasse,
   d) har hovedinteressen av opprettelsen eller forvaltningen av en stiftelse, et fond eller en tilsvarende juridisk person eller formuesmasse, eller
   e) utøver kontroll over mer enn 25 prosent av formuesgodene i en stiftelse, et fond eller en lignende juridisk person eller formuesmasse.
4. tilbydere av virksomhetstjenester: fysiske og juridiske personer som tilbyr en eller flere av følgende tjenester:

a) oppretter selskaper og andre juridiske personer,

b) opptrer som tillitsvalgte eller ledende ansatte i selskap, deltaker i ansvarlig selskap eller kommandittselskap, eller lignende posisjoner i andre typer juridiske personer,

c) besørger forretningsadresser, administrative adresser eller postadresser og dertil knyttede tjenester for juridiske personer,

d) administrerer eller forvalter fond eller tilsvarende formuesmasser,

e) opptrer som aksjeeiere for tredjeperson, med mindre denne er et selskap som har finansielle instrumenter opptatt til notering på et regulert marked i EØS-stat eller er underlagt informasjonsplikt tilsvarende det som gjelder ved notering på et regulert marked i EØS-stat, eller

f) sørger for at andre personer opptrer i posisjoner som nevnt i bokstav b, d og e.

§ 3. *Geografisk virkeområde*

Loven gjelder for rapporteringspliktige som er etablert i Norge, herunder filialer av utenlandske foretak.

Loven gjelder for Svalbard og Jan Mayen. Departementet kan i forskrift fastsette at deler av loven ikke skal gjelde på Svalbard og Jan Mayen og fastsette særlige regler for disse områdene for fremme av lovens formål.

§ 4. *Rapporteringspliktige*

Loven gjelder for følgende juridiske personer:

1. finansinstitusjoner,
2. Norges Bank,
3. e-pengeforetak,
4. foretak som driver virksomhet som består i overføring av penger eller pengefordringer,
5. verdipapirforetak,
6. forvaltningsselskaper for verdipapirfond,
7. forsikringsselskaper,
8. foretak som driver forsikringsformidling som ikke er gjenforsikringsmegling,
9. postoperatører ved formidling av verdisendinger,
10. verdipapirregistre, og
11. foretak som driver depotvirksomhet.

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

1. statsautoriserte og registrerte revisorer,
2. autoriserte regnskapsførere,
3. advokater og andre som ervervsmessig eller stadig yter selvstendig juridisk bistand, når de bistår eller opptrer på vegne av klienter ved planlegging eller utføring av finansielle transaksjoner eller transaksjoner som gjelder fast eiendom eller gjenstander med verdi over 40 000 kroner,
4. eiendomsmeglere og boligbyggelag når det drives eiendomsmegling,
5. foretak som mot vederlag tilbyr tilsvarende tjenester som nevnt i nr. 1 til 4,
6. tilbydere av virksomhetstjenester, og
7. forhandlere av gjenstander, herunder auksjonsforretninger, kommisjonærer og lignende, ved transaksjoner i kontanter på 40 000 norske kroner eller mer eller et tilsvarende beløp i utenlandsk

valuta.

Loven gjelder også for foretak og personer som utfører tjenester på vegne av eller for personer som nevnt i første og annet ledd.

Når advokater opptrer som bostyrere, gjelder bestemmelsene i §§ 17, 18, 20, 21, 27 og 28.

Departementet kan i forskrift fastsette unntak fra enkelte eller flere av bestemmelsene i loven for visse rapporteringspliktige. Departementet kan i forskrift la enkelte eller flere av bestemmelsene i loven få anvendelse for forhandlere av gjenstander ved transaksjoner over bestemte beløpsgrenser ved bruk av nærmere angitte typer betalingsmiddel.

Departementet kan i forskrift fastsette regler som nærmere angir hvem som er omfattet av § 4 første og annet ledd og regler som gir loven anvendelse for foretak som driver spillvirksomhet, inkassoforetak, pensjonskasser og formidlere av andeler i ansvarlige selskaper og kommandittselskaper.

Kapittel 2. Kundekontroll og løpende oppfølging

§ 5. *Risikobasert kundekontroll og løpende oppfølging*

Rapporteringspliktige skal foreta kundekontroll etter §§ 6 til 13 og løpende oppfølging etter § 14. Kundekontroll og løpende oppfølging skal foretas på grunnlag av en vurdering av risiko for transaksjoner med tilknytning til utbytte av straffbare handlinger eller forhold som rammes av straffeloven §§ 147 a, 147 b eller 147 c, der risikoen vurderes ut fra type kunde, kundeforhold, produkt eller transaksjon.

Rapporteringspliktige skal kunne påvise at omfanget av utførte tiltak er tilpasset den aktuelle risiko.

§ 6. *Plikt til å foreta kundekontroll*

Rapporteringspliktige skal foreta kundekontroll ved

1. etablering av kundeforhold,
2. transaksjon som gjelder 100 000 norske kroner eller mer, for kunde som den rapporteringspliktige ikke har et etablert kundeforhold til,
3. mistanke om at en transaksjon har tilknytning til utbytte av straffbar handling eller forhold som rammes av straffeloven §§ 147 a, 147 b eller 147 c, eller
4. tvil om hvorvidt tidligere innhentede opplysninger om kunden er korrekte eller tilstrekkelige.

Beløpsgrensene i første ledd nr. 2 beregnes samlet for transaksjoner som gjennomføres i flere operasjoner som ser ut til å kunne ha sammenheng med hverandre. Dersom beløpet ikke er kjent når transaksjonen gjennomføres, skal kundekontrollen foretas så snart den rapporteringspliktige blir kjent med at beløpsgrensen er oversteget.

Departementet kan i forskrift fastsette nærmere regler om når kundeforhold skal anses etablert.

§ 7. *Gjennomføring av kundekontroll*

Kundekontroll som nevnt i § 6 skal omfatte

1. registrering av opplysninger som nevnt i § 8,
2. bekreftelse av kundens identitet på grunnlag av gyldig legitimasjon,
3. bekreftelse av identiteten til reelle rettighetshavere på grunnlag av egnede tiltak, og
4. innhenting av opplysninger om kundeforholdets formål og tilsiktede art.

Dersom kunden er en juridisk person, skal identiteten til den som handler på vegne av kunden bekreftes på grunnlag av gyldig legitimasjon. Videre skal det dokumenteres, ved firmaattest, stiftelsesdokument, skriftlig fullmakt eller lignende, at vedkommende er berettiget til å representere kunden utad.

Dersom andre enn kunden er gitt disposisjonsrett over en konto eller et depot, eller er gitt rett til å gjennomføre transaksjonen, skal vedkommendes identitet bekreftes på grunnlag av gyldig legitimasjon.

Dersom bekreftelse av en fysisk persons identitet skal skje på grunnlag av fysisk legitimasjon uten vedkommendes personlige fremmøte, skal det fremlegges ytterligere dokumentasjon som bekrefter vedkommendes identitet.

Bekreftelse av fysiske personers identitet etter første ledd nr. 2, annet ledd og tredje ledd kan foretas på annet grunnlag enn gyldig legitimasjon dersom den rapporteringspliktige er sikker på vedkommendes identitet.

Departementet kan i forskrift fastsette nærmere regler om gjennomføring av kundekontroll, herunder hva som anses som gyldig legitimasjon.

§ 8. *Registrering av opplysninger*

Rapporteringspliktige skal registrere følgende opplysninger om kunder:

1. fullt navn eller foretaksnavn,
2. fødselsnummer, organisasjonsnummer, D-nummer eller, dersom kunden ikke har slikt nummer, annen entydig identitetskode,
3. fast adresse, og
4. referanse til legitimasjon som er brukt for å bekrefte kundens identitet.

Plikten til å registrere kundens faste adresse etter første ledd nr. 3 gjelder ikke dersom folkeregisteret har vedtatt at kundens adresse skal være fortrolig eller strengt fortrolig.

For fysiske personer som ikke har fått tildelt norsk fødselsnummer eller D-nummer, skal det registreres fødselsdato, fødested, kjønn og statsborgerskap. Dersom den rapporteringspliktige er kjent med at kunden har to statsborgerskap, skal dette registreres.

For juridiske personer som ikke er registrert i offentlig register, skal det i tillegg registreres opplysninger om organisasjonsform, stiftelsestidspunkt samt daglig leder, forretningsfører, innehaver eller tilsvarende kontaktperson. Dersom kontaktperson er en juridisk person, skal det også oppgis en fysisk person som kontaktperson og registreres opplysninger som nevnt i første ledd om vedkommende.

Rapporteringspliktige skal registrere opplysninger som entydig identifiserer reelle rettighetshavere.

§ 9. *Tidspunkt for kundekontroll*

Kundekontroll skal gjennomføres før etablering av kundeforhold eller utføring av transaksjon.

Fra første ledd gjelder følgende unntak:

1. Bekreftelse av identiteten til kunder og reelle rettighetshavere skal kunne foretas under etablering av kundeforhold, dersom etableringen av kundeforholdet er nødvendig for ikke å hindre den alminnelige forretningsdrift og det er liten risiko for transaksjoner med tilknytning til en straffbar handling eller forhold som rammes av straffeloven §§ 147 a, 147 b eller 147 c.
2. Bekreftelse av identiteten til den begunstigede etter en livsforsikringspolise kan foretas etter tegning av polisen, forutsatt at bekreftelse av identiteten foretas før utbetalingstidspunktet eller det tidspunkt

den begunstigede utøver sine rettigheter etter polisen.

3. Bekreftelse av identiteten til kunden og reelle rettighetshavere kan foretas etter åpning av bankkonto, forutsatt at det finnes foranstaltninger som sikrer at transaksjoner knyttet til kontoen ikke kan utføres av kunden eller på dennes vegne før bekreftelse av identiteten er foretatt.

§ 10. *Følger av at kundekontroll ikke kan gjennomføres*

Dersom kundekontroll ikke kan gjennomføres, skal rapporteringspliktige ikke etablere kundeforhold eller utføre transaksjonen. Et etablert kundeforhold skal avvikles hvis fortsettelse av kundeforholdet medfører risiko for transaksjoner med tilknytning til utbytte av straffbare handlinger eller forhold som rammes av straffeloven §§ 147 a, 147 b eller 147 c.

Første ledd gjelder ikke når advokater og andre som ervervsmessig eller stadig yter selvstendig juridisk bistand er i ferd med å fastslå en klients rettsstilling eller bistår klienten i forbindelse med rettergang.

§ 11. *Kundekontroll utført av tredjeparter*

For gjennomføring av kundekontrolltiltak som nevnt i § 7 nr. 2 til 4 kan rapporteringspliktige legge til grunn tiltak som er utført av følgende tredjeparter:

1. finansinstitusjoner,
2. verdipapirforetak,
3. forvaltningsselskaper for verdipapirfond,
4. forsikringsselskaper,
5. foretak som driver forsikringsformidling som ikke er gjenforsikringsmegling,
6. verdipapirregistre,
7. statsautoriserte og registrerte revisorer,
8. autoriserte regnskapsførere,
9. advokater og andre som ervervsmessig eller stadig yter selvstendig juridisk bistand, når de bistår eller opptrer på vegne av klienter ved planlegging eller utføring av finansielle transaksjoner, transaksjoner som gjelder fast eiendom eller transaksjoner som gjelder gjenstander med verdi over 40 000 kroner,
10. eiendomsmeglere og boligbyggelag når det drives eiendomsmegling, eller
11. tilsvarende juridiske og fysiske personer som nevnt i nr. 1 til 4 og 6 til 10 fra annen stat, såfremt disse er underlagt lovmessig registreringsplikt og regler om kundekontroll, oppbevaring og tilsyn som svarer til reglene i denne lov.

Adgangen til å legge til grunn kundekontrolltiltak utført av tredjeparter i medhold av første ledd, medfører ikke unntak fra den rapporteringspliktiges

1. plikt til å registrere opplysninger som nevnt i § 8 og oppbevare opplysninger og dokumenter som nevnt i § 22, eller
2. ansvar for at kundekontroll gjennomføres i samsvar med denne lov og forskrifter gitt med hjemmel i denne lov.

Rapporteringspliktige kan legge til grunn kundekontroll foretatt av tredjeparter som ikke er etablert i Norge, selv om bekreftelse av kundens identitet, jf. § 7 første ledd nr. 2, er foretatt på annet grunnlag enn gyldig legitimasjon.

Tredjepart skal stille de opplysninger vedkommende har samlet inn for gjennomføring av tiltak som nevnt i § 7 nr. 2 til 4, til rådighet for den rapporteringspliktige som kunden henvises til. Tredjepart skal etter anmodning, omgående videresende kopier av identifikasjons- og kontrollopplysninger og annen

relevant dokumentasjon om kundens eller den reelle rettighetshavers identitet, til den rapporteringspliktige. Utlevering av opplysninger og dokumenter som er nødvendige for at den rapporteringspliktige skal kunne oppfylle sine plikter etter §§ 5 annet ledd, 8 eller 22, medfører ikke brudd på lovmessig taushetsplikt når kunden informeres om at opplysningene utleveres.

Departementet kan i forskrift fastsette unntak fra adgangen til å legge til grunn kundekontroll utført av tredjeparter.

§ 12. *Utkontraktering av gjennomføring av kundekontroll*

Rapporteringspliktige kan inngå skriftlige avtaler med oppdragstakere om utkontraktering av gjennomføring av kundekontroll.

Følgende juridiske og fysiske personer kan fungere som oppdragstakere etter første ledd:

1. rapporteringspliktige, med unntak av tilbydere av virksomhetstjenester som nevnt i § 4 annet ledd nr. 6 og forhandlere av gjenstander som nevnt i § 4 annet ledd nr. 7, og
2. postoperatører med konsesjon.

Den rapporteringspliktige har ansvar for at kundekontroll gjennomføres i samsvar med gjeldende lov og forskrifter og at det etableres forsvarlige rutiner og treffes nødvendige tiltak etter § 23.

Utlevering av opplysninger og dokumenter, som oppdragstaker har innhentet på grunnlag av utkontraktering av gjennomføring av kundekontroll, som er nødvendig for at den rapporteringspliktige skal kunne oppfylle sine plikter etter §§ 5 annet ledd, 8 og 22 medfører ikke brudd på lovmessig taushetsplikt.

Departementet kan i forskrift fastsette at andre enn de som er omfattet av annet ledd kan fungere som oppdragstakere.

§ 13. *Forenklet kundekontroll*

Departementet kan i forskrift fastsette unntak fra plikt til å foreta kundekontroll etter § 6 første ledd nr. 1, 2 og 4 og annet ledd. Rapporteringspliktige skal før anvendelse av unntak innhente tilstrekkelige opplysninger til å fastslå at forholdet dekkes av den aktuelle unntaksbestemmelse.

Første ledd medfører ikke unntak fra plikt til å registrere opplysninger etter § 8 første til tredje ledd ved opprettelse av konto.

§ 14. *Løpende oppfølging*

Rapporteringspliktige skal løpende følge opp eksisterende kundeforhold, herunder påse at transaksjoner som den rapporteringspliktige blir kjent med er i samsvar med den rapporteringspliktiges kjennskap til kunden og dens virksomhet. Rapporteringspliktige skal oppdatere dokumentasjon og opplysninger om kunder.

§ 15. *Forsterkede kontrolltiltak*

I situasjoner som etter sin art innebærer høy risiko for transaksjoner med tilknytning til utbytte av straffbare handlinger eller forhold som rammes av straffeloven §§ 147 a, 147 b eller 147 c, skal rapporteringspliktige ut fra en risikovurdering anvende andre kontrolltiltak i tillegg til de tiltak som følger av §§ 5 til 14.

Rapporteringspliktige skal ha til rådighet egnede kontrolltiltak for å fastslå om kunden er en politisk eksponert person. Rapporteringspliktige skal, ved kundeforhold til eller transaksjoner for slike personer

1. påse at beslutningstaker innhenter samtykke fra overordnet før etablering av kundeforhold,

2. treffe egnede tiltak for å fastslå opprinnelsen til kundens formue og den kapital som inngår i kundeforholdet eller transaksjonen, og
3. føre forsterket løpende oppfølging med kundeforholdet.

Med politisk eksponert person som nevnt i annet ledd menes fysisk person som

1. innehar eller i løpet av det siste året har innehatt høytstående offentlig verv eller stilling i en annen stat enn Norge,
2. er nært familiemedlem til person som nevnt i nr. 1, eller
3. er kjent medarbeider til person som nevnt i nr. 1.

Rapporteringspliktige skal vie særlig oppmerksomhet til produkter og transaksjoner som fremmer anonymitet, og om nødvendig iverksette tiltak for å forebygge transaksjoner med tilknytning til utbytte av straffbare handlinger eller forhold som rammes av straffeloven §§ 147 a, 147 b eller 147 c.

Departementet kan i forskrift fastsette nærmere regler om hvilke situasjoner som skal omfattes av første ledd og hvilke kontrolltiltak som i slike tilfeller skal anvendes. Departementet kan i forskrift fastsette nærmere regler om hvem som skal anses som politisk eksponerte personer.

§ 16. *Korrespondentbankforbindelser*

Ved bruk av en institusjon fra stat utenfor EØS som korrespondentbank, skal kredittinstitusjoner

1. innhente tilstrekkelige opplysninger om korrespondentinstitusjonen til fullt ut å forstå arten av dens virksomhet og på grunnlag av offentlig tilgjengelige opplysninger fastslå institusjonens omdømme og tilsynets kvalitet,
2. vurdere korrespondentinstitusjonens kontrolltiltak for forebyggelse og bekjempelse av handlinger som beskrevet i straffeloven §§ 317 og 147 b,
3. påse at beslutningstaker innhenter samtykke fra overordnet før etablering av nye korrespondentbankforbindelser,
4. dokumentere den enkelte institusjons ansvar, og
5. i forbindelse med oppgjørskonti, forsikre seg om at korrespondentinstitusjonen
   a) har verifisert identiteten til, og fører løpende oppfølging av, kunder som har direkte adgang til konti hos kredittinstitusjonen, og
   b) på anmodning kan fremlegge relevante opplysninger fra kundekontrollen til kredittinstitusjonen.

Kredittinstitusjoner skal ikke inngå eller opprettholde korrespondentbankforbindelse til tomme bankselskaper. Kredittinstitusjoner skal treffe egnede tiltak for å sikre at de ikke inngår eller opprettholder korrespondentbankforbindelser med kredittinstitusjoner som er kjent for å tillate at deres konti brukes av tomme bankselskaper.

Med tomt bankselskap som nevnt i annet ledd menes en kredittinstitusjon som er opprettet i en stat der institusjonen ikke er fysisk til stede med en reell ledelse og administrasjon, og som ikke er tilknyttet et regulert finanskonsern.

Kapittel 3. Undersøkelse og rapportering

§ 17. *Undersøkelsesplikt*

Dersom rapporteringspliktige har mistanke om at en transaksjon har tilknytning til utbytte av en straffbar handling eller forhold som rammes av straffeloven §§ 147 a, 147 b eller 147 c, skal det foretas nærmere undersøkelser for å få bekreftet eller avkreftet mistanken.

Rapporteringspliktige skal skriftlig eller elektronisk registrere resultatene av undersøkelsene.

Departementet kan i forskrift fastsette nærmere regler om undersøkelsesplikt.

§ 18. *Rapporteringsplikt*

Dersom undersøkelser som nevnt i § 17 ikke avkrefter mistanken, skal den rapporteringspliktige av eget tiltak oversende opplysninger til Økokrim om den aktuelle transaksjonen og om de forhold som har medført mistanke. Den rapporteringspliktige skal på forespørsel gi Økokrim alle nødvendige opplysninger om transaksjonen og mistanken.

Advokater og andre som ervervsmessig eller stadig yter rettshjelpvirksomhet har ikke plikt til å rapportere om forhold som de har fått kjennskap til gjennom arbeidet med å fastslå klientens rettsstilling, eller om forhold som de har fått kjennskap til før, under eller etter en rettssak, når de forhold opplysningene omhandler har direkte tilknytning til rettstvisten. Tilsvarende gjelder for revisorer og andre rapporteringspliktige når de bistår advokater eller andre som ervervsmessig eller stadig yter rettshjelpvirksomhet i arbeid som nevnt i første punktum.

Departementet kan i forskrift pålegge rapporteringspliktige å overføre opplysninger til Økokrim elektronisk. Departementet kan i forskrift fastsette nærmere regler om rapporteringsplikten.

§ 19. *Gjennomføring av mistenkelige transaksjoner*

Rapporteringspliktige skal ikke gjennomføre transaksjoner som medfører rapporteringsplikt som nevnt i § 18 før Økokrim er underrettet. Økokrim kan i særlige tilfeller gi pålegg om ikke å gjennomføre transaksjoner.

En transaksjon kan likevel gjennomføres før opplysninger er oversendt Økokrim, dersom unnlatelse av å gjennomføre transaksjonen kan vanskeliggjøre Økokrims undersøkelser eller eventuell etterforskning eller det ikke er mulig å la være å gjennomføre transaksjonen. Opplysninger skal i så fall oversendes Økokrim umiddelbart etter at transaksjonen er gjennomført.

§ 20. *Forholdet til taushetsplikt*

Meddelelse av opplysninger til Økokrim i god tro etter § 18 medfører ikke brudd på taushetsplikt og gir ikke grunnlag for erstatningsansvar eller straffansvar.

Finansinstitusjoner og forsikringsselskaper kan uten hinder av taushetsplikt utveksle nødvendige kundeopplysninger seg imellom når det anses nødvendig som ledd i undersøkelser som nevnt i § 17.

§ 21. *Forbud mot å avsløre undersøkelser, rapportering eller etterforskning*

Kunder eller tredjepersoner skal ikke gjøres kjent med at det foretas undersøkelser som nevnt i § 17, at det er gitt opplysninger som nevnt i § 18 eller at det er iverksatt etterforskning.

Første ledd er ikke til hinder for utveksling av opplysninger som nevnt i § 20 annet ledd.

Første ledd er ikke til hinder for at rapporteringspliktige som nevnt i § 4 annet ledd nr. 1 til 3 forsøker å få en klient til å avstå fra å begå en ulovlig handling.

Departementet kan i forskrift fastsette unntak fra første ledd.

Kapittel 4. Oppbevaring

§ 22. *Oppbevaring av opplysninger og dokumenter*

Rapporteringspliktige skal oppbevare kopier av dokumenter benyttet i forbindelse med kundekontroll

som nevnt i § 7, samt registrerte opplysninger som nevnt i § 8, i fem år etter at kundeforholdet er avsluttet eller transaksjonen er gjennomført, med mindre lengre frister følger av annen lov eller forskrift. Dersom det er benyttet kvalifisert sertifikat, skal sertifikatets identifikasjonskode og opplysninger om sertifikatutstederens identitet oppbevares. Det skal ved bruk av kontonummer eller på annen måte registreres en entydig forbindelse mellom kundeforhold og registrerte opplysninger som nevnt i § 8.

Rapporteringspliktige skal oppbevare dokumenter i tilknytning til transaksjoner som nevnt i § 17 i minst fem år etter at transaksjonen er gjennomført.

Dokumenter og opplysninger som nevnt i første og annet ledd skal oppbevares på en betryggende måte, beskyttes mot uautorisert tilgang fra uvedkommende og slettes innen ett år etter at oppbevaringsplikten opphører. Personopplysningsloven gjelder for rapporteringspliktiges oppbevaring av personopplysninger.

Departementet kan i forskrift fastsette nærmere regler om oppbevaringsmåte og sletting av opplysninger.

Kapittel 5. Interne rutiner og systemer mv.

§ 23. *Kontroll- og kommunikasjonsrutiner*

Rapporteringspliktige skal ha forsvarlige interne kontroll- og kommunikasjonsrutiner som sikrer oppfyllelse av plikter etter denne lov.

Rutinene skal være fastsatt på øverste nivå hos den rapporteringspliktige. Det skal utpekes en person i ledelsen som skal ha et særskilt ansvar for å følge opp rutinene.

Rapporteringspliktige skal treffe nødvendige tiltak for å sikre at ansatte og andre personer som utfører oppgaver på vegne av den rapporteringspliktige

1. er kjent med de plikter som påligger den rapporteringspliktige etter denne lov,
2. lærer å kjenne igjen transaksjoner som nevnt i § 17, og
3. er kjent med den rapporteringspliktiges interne rutiner for håndtering av slike transaksjoner.

§ 24. *Elektroniske overvåkningssystemer*

Finansinstitusjoner skal etablere elektroniske overvåkningssystemer.

Departementet kan i forskrift pålegge andre rapporteringspliktige å etablere elektroniske overvåkningssystemer og fastsette nærmere regler om slike systemer.

§ 25. *Systemer for oversikt over kundeforhold*

Rapporteringspliktige som nevnt i § 4 første ledd skal ha systemer som muliggjør raske og fullstendige svar på forespørsler fra Økokrim eller tilsynsmyndighet om hvorvidt de har eller i løpet av de siste fem år har hatt kundeforhold til konkrete personer og om kundeforholdets art.

§ 26. *Filialer og datterselskaper i stater utenfor EØS*

Rapporteringspliktige som nevnt i § 4 første ledd skal påse at filialer og datterselskaper etablert i stater utenfor EØS

1. er kjent med kontroll- og kommunikasjonsrutiner som beskrevet i § 23, og
2. anvender tilsvarende tiltak for kundekontroll, løpende oppfølging og oppbevaring som beskrevet i kapittel 2 og 4.

Dersom lovgivningen i vedkommende stat ikke tillater anvendelse av tiltak som nevnt i første ledd nr. 2, skal den rapporteringspliktige

1. informere tilsynsmyndigheten om dette, og
2. iverksette andre tiltak som er egnet til å motvirke risikoen for transaksjoner med tilknytning til utbytte av straffbare handlinger eller forhold som beskrevet i straffeloven §§ 147 a, 147 b eller 147 c.

Kapittel 6. Avsluttende bestemmelser

§ 27. *Pålegg og tvangstiltak*

Tilsynsorgan kan gi den rapporteringspliktige pålegg om at forhold i strid med denne lov eller bestemmelser gitt i medhold av loven, skal opphøre. Tilsynsorgan kan sette en frist for at forholdene bringes i samsvar med pålegget.

Dersom den rapporteringspliktige ikke etterkommer pålegg etter første ledd, kan tilsynsorgan ilegge tvangsmulkt. Tvangsmulkten kan ilegges i form av engangsmulkt eller løpende mulkt. Ilagt mulkt er tvangsgrunnlag for utlegg.

Departementet kan i forskrift fastsette nærmere regler om fastsettelse av tvangsmulkt, herunder mulktens størrelse.

§ 28. *Straff*

Med bøter straffes den som forsettlig eller grovt uaktsomt overtrer eller medvirker til overtredelse av denne lovs §§ 5, 6, 7, 8, 15, 17, 18 eller 22, eller forskrifter gitt i medhold av disse bestemmelsene.

Ved særlig skjerpende omstendigheter kan fengsel inntil 1 år anvendes.

§ 29. *Økokrims håndtering av opplysninger*

Opplysninger som Økokrim mottar etter § 18 skal slettes senest fem år etter at opplysningene ble registrert, med mindre det i dette tidsrommet er registrert nye opplysninger eller det er foretatt etterforsknings- eller rettergangsskritt mot den registrerte.

Dersom Økokrims undersøkelser viser at det ikke foreligger en straffbar handling, skal opplysningene slettes snarest mulig.

Departementet kan i forskrift fastsette nærmere regler om Økokrims og politiets saksbehandling i tilknytning til mottatte rapporter, herunder sletting av opplysninger.

§ 30. *Utveksling av opplysninger for bekjempelse av terrorhandlinger mv.*

Økokrim kan gi opplysninger som Økokrim mottar etter § 18 til andre offentlige myndigheter enn politiet som har oppgaver knyttet til forebygging av forhold som rammes av straffeloven §§ 147 a, 147 b eller 147 c.

Opplysninger som Økokrim mottar etter bestemmelsene i denne lov, kan Økokrim gi videre til skatteetaten og toll- og avgiftsetaten til bruk i deres arbeid med skatt, avgift og toll.

Endret ved lov 11 des 2009 nr. 127.

§ 31. *Kontrollutvalget for tiltak mot hvitvasking*

Kontrollutvalget for tiltak mot hvitvasking (Kontrollutvalget) skal føre kontroll med:

1. Økokrims behandling av opplysninger mottatt etter § 18,
2. Økokrims pålegg og godkjenninger etter § 19 første ledd, og
3. Økokrims håndtering av opplysninger etter § 29.

Kontrollutvalget skal bestå av minst tre medlemmer som oppnevnes av Kongen. Dessuten oppnevnes ett eller flere varamedlemmer. Lederen for utvalget skal oppfylle de krav som stilles til høyesterettsdommere. Kontrollutvalgets medlemmer har taushetsplikt om det de får vite i utøvelsen av sitt verv.

Økokrim skal gi Kontrollutvalget de opplysninger, dokumenter mv. som Kontrollutvalget finner nødvendig for sin kontroll. Når Kontrollutvalget krever det, har Økokrims tjenestemenn plikt til å forklare seg overfor Kontrollutvalget uten hensyn til taushetsplikt.

Departementet kan i forskrift fastsette nærmere regler om oppgavene og saksbehandlingen til Kontrollutvalget.

§ 32. *Opplysninger som skal følge en transaksjon i betalingskjeden mv.*

Departementet kan i forskrift fastsette regler om hvilke opplysninger om avsender som skal følge en transaksjon i betalingskjeden, samt regler om betalingsformidleres opplysnings- og kontrollplikter i forbindelse med slike transaksjoner.

§ 33. *Personer eller foretak med tilknytning til land eller områder som ikke har gjennomført tilfredsstillende tiltak*

Departementet kan i forskrift fastsette

1. særskilte regler om rapportering av transaksjoner med eller for personer eller foretak som har tilknytning til land eller områder som ikke har gjennomført tilfredsstillende tiltak mot handlinger som beskrevet i straffeloven §§ 317 og 147 b, og
2. forbud mot eller restriksjoner i rapporteringspliktiges adgang til å etablere kundeforhold med eller foreta transaksjoner med eller for personer eller foretak som har tilknytning til land eller områder som ikke har gjennomført tilfredsstillende tiltak mot handlinger som beskrevet i straffeloven §§ 317 og 147 b.

Kapittel 7. Ikrafttredelse og endringer i andre lover

§ 34. *Ikrafttredelse*

Loven trer i kraft fra den tid Kongen bestemmer.[1]

Plikt til avvikling av kundeforhold etter § 10 første ledd gjelder kun for kundeforhold som er etablert etter lovens ikrafttredelse.

1 Fra 15 april 2009 iflg. res. 6 mars 2009 nr. 269.

§ 35. *Endringer i andre lover*

Fra den tid loven trer i kraft, gjøres følgende endringer i andre lover: - - -

Databasen sist oppdatert 4. juni 2010

Universitetet i Stavanger

Appendix B – FATFs 40 anbefalinger

Financial Action Task Force Groupe d'action financière

FATF Standards

FATF 40 Recommendations

20 June 2003
(incorporating the amendments of 22 October 2004)

INTRODUCTION

Money laundering methods and techniques change in response to developing counter-measures. In recent years, the Financial Action Task Force (FATF) [1] has noted increasingly sophisticated combinations of techniques, such as the increased use of legal persons to disguise the true ownership and control of illegal proceeds, and an increased use of professionals to provide advice and assistance in laundering criminal funds. These factors, combined with the experience gained through the FATF's Non-Cooperative Countries and Territories process, and a number of national and international initiatives, led the FATF to review and revise the Forty Recommendations into a new comprehensive framework for combating money laundering and terrorist financing. The FATF now calls upon all countries to take the necessary steps to bring their national systems for combating money laundering and terrorist financing into compliance with the new FATF Recommendations, and to effectively implement these measures.

The review process for revising the Forty Recommendations was an extensive one, open to FATF members, non-members, observers, financial and other affected sectors and interested parties. This consultation process provided a wide range of input, all of which was considered in the review process.

The revised Forty Recommendations now apply not only to money laundering but also to terrorist financing, and when combined with the Eight Special Recommendations on Terrorist Financing provide an enhanced, comprehensive and consistent framework of measures for combating money laundering and terrorist financing. The FATF recognises that countries have diverse legal and financial systems and so all cannot take identical measures to achieve the common objective, especially over matters of detail. The Recommendations therefore set minimum standards for action for countries to implement the detail according to their particular circumstances and constitutional frameworks. The Recommendations cover all the measures that national systems should have in place within their criminal justice and regulatory systems; the preventive measures to be taken by financial institutions and certain other businesses and professions; and international co-operation.

The original FATF Forty Recommendations were drawn up in 1990 as an initiative to combat the misuse of financial systems by persons laundering drug money. In 1996 the Recommendations were revised for the first time to reflect evolving money laundering typologies. The 1996 Forty Recommendations have been endorsed by more than 130 countries and are the international anti-money laundering standard.

In October 2001 the FATF expanded its mandate to deal with the issue of the financing of terrorism, and took the important step of creating the Eight Special Recommendations on Terrorist Financing. These Recommendations contain a set of measures aimed at combating the funding of terrorist acts and terrorist organisations, and are complementary to the Forty Recommendations[2].

A key element in the fight against money laundering and the financing of terrorism is the need for countries systems to be monitored and evaluated, with respect to these international standards. The mutual evaluations conducted by the FATF and FATF-style regional bodies, as well as the assessments conducted by the IMF and World Bank, are a vital mechanism for ensuring that the FATF Recommendations are effectively implemented by all countries.

---

[1] The FATF is an inter-governmental body which sets standards, and develops and promotes policies to combat money laundering and terrorist financing. It currently has 33 members: 31 countries and governments and two international organisations; and more than 20 observers: five FATF-style regional bodies and more than 15 other international organisations or bodies. A list of all members and observers can be found on the FATF website at http://www.fatf-gafi.org/Members_en.htm

[2] The FATF Forty and Eight Special Recommendations have been recognised by the International Monetary Fund and the World Bank as the international standards for combating money laundering and the financing of terrorism.

THE FORTY RECOMMENDATIONS

A. LEGAL SYSTEMS

Scope of the criminal offence of money laundering

1. Countries should criminalise money laundering on the basis of the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988 (the Vienna Convention) and the United Nations Convention against Transnational Organized Crime, 2000 (the Palermo Convention).

Countries should apply the crime of money laundering to all serious offences, with a view to including the widest range of predicate offences. Predicate offences may be described by reference to all offences, or to a threshold linked either to a category of serious offences or to the penalty of imprisonment applicable to the predicate offence (threshold approach), or to a list of predicate offences, or a combination of these approaches.

Where countries apply a threshold approach, predicate offences should at a minimum comprise all offences that fall within the category of serious offences under their national law or should include offences which are punishable by a maximum penalty of more than one year's imprisonment or for those countries that have a minimum threshold for offences in their legal system, predicate offences should comprise all offences, which are punished by a minimum penalty of more than six months imprisonment.

Whichever approach is adopted, each country should at a minimum include a range of offences within each of the designated categories of offences[3].

Predicate offences for money laundering should extend to conduct that occurred in another country, which constitutes an offence in that country, and which would have constituted a predicate offence had it occurred domestically. Countries may provide that the only prerequisite is that the conduct would have constituted a predicate offence had it occurred domestically.

Countries may provide that the offence of money laundering does not apply to persons who committed the predicate offence, where this is required by fundamental principles of their domestic law.

2. Countries should ensure that:

a) The intent and knowledge required to prove the offence of money laundering is consistent with the standards set forth in the Vienna and Palermo Conventions, including the concept that such mental state may be inferred from objective factual circumstances.

b) Criminal liability, and, where that is not possible, civil or administrative liability, should apply to legal persons. This should not preclude parallel criminal, civil or administrative proceedings with respect to legal persons in countries in which such forms of liability

[3] See the definition of "designated categories of offences" in the Glossary.

are available. Legal persons should be subject to effective, proportionate and dissuasive sanctions. Such measures should be without prejudice to the criminal liability of individuals.

Provisonal measures and confiscation

3. Countries should adopt measures similar to those set forth in the Vienna and Palermo Conventions, including legislative measures, to enable their competent authorities to confiscate property laundered, proceeds from money laundering or predicate offences, instrumentalities used in or intended for use in the commission of these offences, or property of corresponding value, without prejudicing the rights of bona fide third parties.

Such measures should include the authority to: (a) identify, trace and evaluate property which is subject to confiscation; (b) carry out provisional measures, such as freezing and seizing, to prevent any dealing, transfer or disposal of such property; (c) take steps that will prevent or void actions that prejudice the State's ability to recover property that is subject to confiscation; and (d) take any appropriate investigative measures.

Countries may consider adopting measures that allow such proceeds or instrumentalities to be confiscated without requiring a criminal conviction, or which require an offender to demonstrate the lawful origin of the property alleged to be liable to confiscation, to the extent that such a requirement is consistent with the principles of their domestic law.

B. MEASURES TO BE TAKEN BY FINANCIAL INSTITUTIONS AND NON-FINANCIAL BUSINESSES AND PROFESSIONS TO PREVENT MONEY LAUNDERING AND TERRORIST FINANCING

4. Countries should ensure that financial institution secrecy laws do not inhibit implementation of the FATF Recommendations.

Customer due diligence and record-keeping

5.* Financial institutions should not keep anonymous accounts or accounts in obviously fictitious names.

Financial institutions should undertake customer due diligence measures, including identifying and verifying the identity of their customers, when:

- establishing business relations;
- carrying out occasional transactions: (i) above the applicable designated threshold; or (ii) that are wire transfers in the circumstances covered by the Interpretative Note to Special Recommendation VII;
- there is a suspicion of money laundering or terrorist financing; or
- the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.

The customer due diligence (CDD) measures to be taken are as follows:

a) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information[4].

b) Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include financial institutions taking reasonable measures to understand the ownership and control structure of the customer.

c) Obtaining information on the purpose and intended nature of the business relationship.

d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

Financial institutions should apply each of the CDD measures under (a) to (d) above, but may determine the extent of such measures on a risk sensitive basis depending on the type of customer, business relationship or transaction. The measures that are taken should be consistent with any guidelines issued by competent authorities. For higher risk categories, financial institutions should perform enhanced due diligence. In certain circumstances, where there are lower risks, countries may decide that financial institutions can apply reduced or simplified measures.

Financial institutions should verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers. Countries may permit financial institutions to complete the verification as soon as reasonably practicable following the establishment of the relationship, where the money laundering risks are effectively managed and where this is essential not to interrupt the normal conduct of business.

Where the financial institution is unable to comply with paragraphs (a) to (c) above, it should not open the account, commence business relations or perform the transaction; or should terminate the business relationship; and should consider making a suspicious transactions report in relation to the customer.

These requirements should apply to all new customers, though financial institutions should also apply this Recommendation to existing customers on the basis of materiality and risk, and should conduct due diligence on such existing relationships at appropriate times.

6.* Financial institutions should, in relation to politically exposed persons, in addition to performing normal due diligence measures:

a) Have appropriate risk management systems to determine whether the customer is a politically exposed person.
b) Obtain senior management approval for establishing business relationships with such customers.

[4] Reliable, independent source documents, data or information will hereafter be referred to as "identification data".

* Recommendations marked with an asterisk should be read in conjunction with their Interpretative Note.

c) Take reasonable measures to establish the source of wealth and source of funds.
d) Conduct enhanced ongoing monitoring of the business relationship.

7. Financial institutions should, in relation to cross-border correspondent banking and other similar relationships, in addition to performing normal due diligence measures:

a) Gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action.
b) Assess the respondent institution's anti-money laundering and terrorist financing controls.
c) Obtain approval from senior management before establishing new correspondent relationships.
d) Document the respective responsibilities of each institution.
e) With respect to "pay able-through accounts", be satisfied that the respondent bank has verified the identity of and performed on-going due diligence on the customers having direct access to accounts of the correspondent and that it is able to provide relevant customer identification data upon request to the correspondent bank.

8. Financial institutions should pay special attention to any money laundering threats that may arise from new or developing technologies that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes. In particular, financial institutions should have policies and procedures in place to address any specific risks associated with non-face to face business relationships or transactions.

9.* Countries may permit financial institutions to rely on intermediaries or other third parties to perform elements (a) – (c) of the CDD process or to introduce business, provided that the criteria set out below are met. Where such reliance is permitted, the ultimate responsibility for customer identification and verification remains with the financial institution relying on the third party.

The criteria that should be met are as follows:

a) A financial institution relying upon a third party should immediately obtain the necessary information concerning elements (a) – (c) of the CDD process. Financial institutions should take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay.

b) The financial institution should satisfy itself that the third party is regulated and supervised for, and has measures in place to comply with CDD requirements in line with Recommendations 5 and 10.

It is left to each country to determine in which countries the third party that meets the conditions can be based, having regard to information available on countries that do not or do not adequately apply the FATF Recommendations.

10.* Financial institutions should maintain, for at least five years, all necessary records on transactions, both domestic or international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit

reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of criminal activity.

Financial institutions should keep records on the identification data obtained through the customer due diligence process (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence for at least five years after the business relationship is ended.

The identification data and transaction records should be available to domestic competent authorities upon appropriate authority.

11.* Financial institutions should pay special attention to all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The background and purpose of such transactions should, as far as possible, be examined, the findings established in writing, and be available to help competent authorities and auditors.

12.* The customer due diligence and record-keeping requirements set out in Recommendations 5, 6, and 8 to 11 apply to designated non-financial businesses and professions in the following situations:

a) Casinos – when customers engage in financial transactions equal to or above the applicable designated threshold.

b) Real estate agents - when they are involved in transactions for their client concerning the buying and selling of real estate.

c) Dealers in precious metals and dealers in precious stones - when they engage in any cash transaction with a customer equal to or above the applicable designated threshold.

d) Lawyers, notaries, other independent legal professionals and accountants when they prepare for or carry out transactions for their client concerning the following activities:

- buying and selling of real estate;
- managing of client money, securities or other assets;
- management of bank, savings or securities accounts;
- organisation of contributions for the creation, operation or management of companies;
- creation, operation or management of legal persons or arrangements, and buying and selling of business entities.

e) Trust and company service providers when they prepare for or carry out transactions for a client concerning the activities listed in the definition in the Glossary.

Reporting of suspicious transactions and compliance

13.* If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, directly by law or regulation, to report promptly its suspicions to the financial intelligence unit (FIU).

14.* Financial institutions, their directors, officers and employees should be:

a) Protected by legal provisions from criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the FIU, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred.

b) Prohibited by law from disclosing the fact that a suspicious transaction report (STR) or related information is being reported to the FIU.

15.* Financial institutions should develop programmes against money laundering and terrorist financing. These programmes should include:

a) The development of internal policies, procedures and controls, including appropriate compliance management arrangements, and adequate screening procedures to ensure high standards when hiring employees.
b) An ongoing employee training programme.
c) An audit function to test the system.

16.* The requirements set out in Recommendations 13 to 15, and 21 apply to all designated non-financial businesses and professions, subject to the following qualifications:

a) Lawyers, notaries, other independent legal professionals and accountants should be required to report suspicious transactions when, on behalf of or for a client, they engage in a financial transaction in relation to the activities described in Recommendation 12(d). Countries are strongly encouraged to extend the reporting requirement to the rest of the professional activities of accountants, including auditing.

b) Dealers in precious metals and dealers in precious stones should be required to report suspicious transactions when they engage in any cash transaction with a customer equal to or above the applicable designated threshold.

c) Trust and company service providers should be required to report suspicious transactions for a client when, on behalf of or for a client, they engage in a transaction in relation to the activities referred to Recommendation 12(e).

Lawyers, notaries, other independent legal professionals, and accountants acting as independent legal professionals, are not required to report their suspicions if the relevant information was obtained in circumstances where they are subject to professional secrecy or legal professional privilege.

Other measures to deter money laundering and terrorist financing

17. Countries should ensure that effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, are available to deal with natural or legal persons covered by these Recommendations that fail to comply with anti-money laundering or terrorist financing requirements.

18. Countries should not approve the establishment or accept the continued operation of shell banks. Financial institutions should refuse to enter into, or continue, a correspondent banking relationship with shell banks. Financial institutions should also guard against establishing relations with respondent foreign financial institutions that permit their accounts to be used by shell banks.

19. Countries should consider the feasibility and utility of a system where banks and other financial institutions and intermediaries would report all domestic and international currency transactions above a fixed amount, to a national central agency with a computerised data base, available to competent authorities for use in money laundering or terrorist financing cases, subject to strict safeguards to ensure proper use of the information.

20. Countries should consider applying the FATF Recommendations to businesses and professions, other than designated non-financial businesses and professions, that pose a money laundering or terrorist financing risk.

Countries should further encourage the development of modern and secure techniques of money management that are less vulnerable to money laundering.

Measures to be taken with respect to countries that do not or insufficiently comply with the FATF Recommendations

21. Financial institutions should give special attention to business relationships and transactions with persons, including companies and financial institutions, from countries which do not or insufficiently apply the FATF Recommendations. Whenever these transactions have no apparent economic or visible lawful purpose, their background and purpose should, as far as possible, be examined, the findings established in writing, and be available to help competent authorities. Where such a country continues not to apply or insufficiently applies the FATF Recommendations, countries should be able to apply appropriate countermeasures.

22. Financial institutions should ensure that the principles applicable to financial institutions, which are mentioned above are also applied to branches and majority owned subsidiaries located abroad, especially in countries which do not or insufficiently apply the FATF Recommendations, to the extent that local applicable laws and regulations permit. When local applicable laws and regulations prohibit this implementation, competent authorities in the country of the parent institution should be informed by the financial institutions that they cannot apply the FATF Recommendations.

Regulation and supervision

23.* Countries should ensure that financial institutions are subject to adequate regulation and supervision and are effectively implementing the FATF Recommendations. Competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding or being the beneficial owner of a significant or controlling interest or holding a management function in a financial institution.

For financial institutions subject to the Core Principles, the regulatory and supervisory measures that apply for prudential purposes and which are also relevant to money laundering, should apply in a similar manner for anti-money laundering and terrorist financing purposes.

Other financial institutions should be licensed or registered and appropriately regulated, and subject to supervision or oversight for anti-money laundering purposes, having regard to the risk of money laundering or terrorist financing in that sector. At a minimum, businesses providing a service of money or value transfer, or of money or currency changing should be licensed or registered, and subject to effective systems for monitoring and ensuring compliance with national requirements to combat money laundering and terrorist financing.

24. Designated non-financial businesses and professions should be subject to regulatory and supervisory measures as set out below.

a) Casinos should be subject to a comprehensive regulatory and supervisory regime that ensures that they have effectively implemented the necessary anti-money laundering and terrorist-financing measures. At a minimum:

- casinos should be licensed;
- competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding or being the beneficial owner of a significant or controlling interest, holding a management function in, or being an operator of a casino
- competent authorities should ensure that casinos are effectively supervised for compliance with requirements to combat money laundering and terrorist financing.

b) Countries should ensure that the other categories of designated non-financial businesses and professions are subject to effective systems for monitoring and ensuring their compliance with requirements to combat money laundering and terrorist financing. This should be performed on a risk-sensitive basis. This may be performed by a government authority or by an appropriate self-regulatory organisation, provided that such an organisation can ensure that its members comply with their obligations to combat money laundering and terrorist financing.

25.* The competent authorities should establish guidelines, and provide feedback which will assist financial institutions and designated non-financial businesses and professions in applying national measures to combat money laundering and terrorist financing, and in particular, in detecting and reporting suspicious transactions.

C. INSTITUTIONAL AND OTHER MEASURES NECESSARY IN SYSTEMS FOR COMBATING MONEY LAUNDERING AND TERRORIST FINANCING

Competent authorities, their powers and resources

26.* Countries should establish a FIU that serves as a national centre for the receiving (and, as permitted, requesting), analysis and dissemination of STR and other information regarding potential money laundering or terrorist financing. The FIU should have access, directly or indirectly, on a timely basis to the financial, administrative and law enforcement information that it requires to properly undertake its functions, including the analysis of STR.

27.* Countries should ensure that designated law enforcement authorities have responsibility for money laundering and terrorist financing investigations. Countries are encouraged to support and develop, as far as possible, special investigative techniques suitable for the investigation of money laundering, such as controlled delivery, undercover operations and other relevant techniques. Countries are also encouraged to use other effective mechanisms such as the use of permanent or temporary groups specialised in asset investigation, and co-operative investigations with appropriate competent authorities in other countries.

28. When conducting investigations of money laundering and underlying predicate offences, competent authorities should be able to obtain documents and information for use in those investigations, and in prosecutions and related actions. This should include powers to use compulsory measures for the production of records held by financial institutions and other persons, for the search of persons and premises, and for the seizure and obtaining of evidence.

29. Supervisors should have adequate powers to monitor and ensure compliance by financial institutions with requirements to combat money laundering and terrorist financing, including the authority to conduct inspections. They should be authorised to compel production of any information from financial institutions that is relevant to monitoring such compliance, and to impose adequate administrative sanctions for failure to comply with such requirements.

30. Countries should provide their competent authorities involved in combating money laundering and terrorist financing with adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of those authorities are of high integrity.

31. Countries should ensure that policy makers, the FIU, law enforcement and supervisors have effective mechanisms in place which enable them to co-operate, and where appropriate co-ordinate domestically with each other concerning the development and implementation of policies and activities to combat money laundering and terrorist financing.

32. Countries should ensure that their competent authorities can review the effectiveness of their systems to combat money laundering and terrorist financing systems by maintaining comprehensive statistics on matters relevant to the effectiveness and efficiency of such systems. This should include statistics on the STR received and disseminated; on money laundering and terrorist financing investigations, prosecutions and convictions; on property frozen, seized and confiscated; and on mutual legal assistance or other international requests for co-operation.

Transparency of legal persons and arrangements

33. Countries should take measures to prevent the unlawful use of legal persons by money launderers. Countries should ensure that there is adequate, accurate and timely information on the beneficial ownership and control of legal persons that can be obtained or accessed in a timely fashion by competent authorities. In particular, countries that have legal persons that are able to issue bearer shares should take appropriate measures to ensure that they are not misused for money laundering and be able to demonstrate the adequacy of those measures. Countries could consider measures to facilitate access to beneficial ownership and control information to financial institutions undertaking the requirements set out in Recommendation 5.

34. Countries should take measures to prevent the unlawful use of legal arrangements by money launderers. In particular, countries should ensure that there is adequate, accurate and timely information on express trusts, including information on the settlor, trustee and beneficiaries, that can be obtained or accessed in a timely fashion by competent authorities. Countries could consider measures to facilitate access to beneficial ownership and control information to financial institutions undertaking the requirements set out in Recommendation 5.

D. INTERNATIONAL CO-OPERATION

35. Countries should take immediate steps to become party to and implement fully the Vienna Convention, the Palermo Convention, and the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism. Countries are also encouraged to ratify and implement other relevant international conventions, such as the 1990 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and the 2002 Inter-American Convention against Terrorism.

Mutual legal assistance and extradition

36. Countries should rapidly , cons tructively and effectiv ely provide the widest possible rang e of mutual legal assistance in relation to m oney la undering and terrorist financing inv estigations, prosecutions, and related proceedings. In particular, countries should:

a) Not prohibit or place unreasona ble or unduly restrictive conditions on the prov ision of mutual legal assistance.

b) Ensure that they hav e clear and efficient processes for the execution of m utual leg al assistance requests.

c) Not refuse to execute a request for mutual leg al assistance on the sole g round that the offence is also considered to involve fiscal matters.

d) Not refuse to execute a request for m utual legal assistance on the g rounds that laws require financial institutions to maintain secrecy or confidentiality.

Countries should ensure that the pow ers of their com petent authorities required under Recommendation 28 are also av ailable for use in response to requests for mutual legal assistance, and if consistent with their dom estic framework, in response to direct requests from foreign judicial or law enforcement authorities to domestic counterparts.

To avoid conflicts of j urisdiction, considerati on should be g iven to dev ising and apply ing mechanisms for determ ining the best v enue for prosecution of defendants in the interests of justice in cases that are subject to prosecution in more than one country.

37. Countries should, to the greatest extent possible, render m utual leg al assistance notwithstanding the absence of dual criminality.

Where dual criminality is required for m utual legal assistance or extradition, that requirem ent should be deemed to be satisfied regardless of whether both countries place the offence within the same category of offence or denominate the offence by the same terminology, provided that both countries criminalise the conduct underlying the offence.

38.* There should be authority to tak e expeditious action in response to requests by foreig n countries to identify, freeze, seize and confiscate property laundered, proceeds from m oney laundering or predicate offences, instrumentalities used in or intended for use in the commission of these offences, or property of corresponding v alue. T here should also be arrangements for co- ordinating seiz ure and c onfiscation proceedings, which m ay include the sharing of confiscated assets.

39. Countries should recog nise money laundering as an extraditable offence. Each country should either extradite its own nationals, or where a country does not do so solely on the g rounds of nationality, that country should, at the request of the country seek ing extradition, subm it the case w ithout undue delay to its com petent aut horities for the purpose of prosecution of the offences set forth in the request. Those authorities should take their decision and conduct their proceedings in the sam e manner as in the case of any other offence of a serious nature under the domestic law of that country. The countries concerned should cooperate with each other, in particular on procedural and evidentiary aspects, to ensure the efficiency of such prosecutions.

Subject to their leg al frameworks, countries m ay consider sim plifying extradition by allowing direct transmission of extraditi on requests betw een appropriate m inistries, extraditing persons based only on w arrants of arrests or j udgements, and/or introducing a simplified extradition of consenting persons who waive formal extradition proceedings.

Other forms of co-operation

40.* Countries should ensure that their competent authorities provide the widest possible range of international co-operation to their foreign counterparts. There should be clear and effective gateways to facilitate the prompt and constructive exchange directly between counterparts, either spontaneously or upon request, of information relating to both money laundering and the underlying predicate offences. Exchanges should be permitted without unduly restrictive conditions. In particular:

a) Competent authorities should not refuse a request for assistance on the sole ground that the request is also considered to involve fiscal matters.

b) Countries should not invoke laws that require financial institutions to maintain secrecy or confidentiality as a ground for refusing to provide co-operation.

c) Competent authorities should be able to conduct inquiries; and where possible, investigations; on behalf of foreign counterparts.

Where the ability to obtain information sought by a foreign competent authority is not within the mandate of its counterpart, countries are also encouraged to permit a prompt and constructive exchange of information with non-counterparts. Co-operation with foreign authorities other than counterparts could occur directly or indirectly. When uncertain about the appropriate avenue to follow, competent authorities should first contact their foreign counterparts for assistance.

Countries should establish controls and safeguards to ensure that information exchanged by competent authorities is used only in an authorised manner, consistent with their obligations concerning privacy and data protection.

GLOSSARY

In these Recommendations the following abbreviations and references are used:

"**Beneficial owner**" refers to the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.

"**Core Principles**" refers to the Core Principles for Effective Banking Supervision issued by the Basel Committee on Banking Supervision, the Objectives and Principles for Securities Regulation issued by the International Organization of Securities Commissions, and the Insurance Supervisory Principles issued by the International Association of Insurance Supervisors.

"**Designated categories of offences**" means:

- participation in an organised criminal group and racketeering;
- terrorism, including terrorist financing;
- trafficking in human beings and migrant smuggling;
- sexual exploitation, including sexual exploitation of children;
- illicit trafficking in narcotic drugs and psychotropic substances;
- illicit arms trafficking;
- illicit trafficking in stolen and other goods;
- corruption and bribery;
- fraud;
- counterfeiting currency;
- counterfeiting and piracy of products;
- environmental crime;
- murder, grievous bodily injury;
- kidnapping, illegal restraint and hostage-taking;
- robbery or theft;
- smuggling;
- extortion;
- forgery;
- piracy; and
- insider trading and market manipulation.

When deciding on the range of offences to be covered as predicate offences under each of the categories listed above, each country may decide, in accordance with its domestic law, how it will define those offences and the nature of any particular elements of those offences that make them serious offences.

"**Designated non-financial businesses and professions**" means:

a) Casinos (which also includes internet casinos).
b) Real estate agents.
c) Dealers in precious metals.
d) Dealers in precious stones.
e) Lawyers, notaries, other independent legal professionals and accountants – this refers to sole practitioners, partners or employed professionals within professional firms. It is not meant to refer to 'internal' professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to measures that would combat money laundering.

f) Trust and Company Service Providers refers to all persons or businesses that are not covered elsewhere under these Recommendations, and which as a business, provide any of the following services to third parties:

- acting as a formation agent of legal persons;
- acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
- providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;
- acting as (or arranging for another person to act as) a trustee of an express trust;
- acting as (or arranging for another person to act as) a nominee shareholder for another person.

"**Designated threshold**" refers to the amount set out in the Interpretative Notes.

"Financial institutions" means any person or entity who conducts as a business one or more of the following activities or operations for or on behalf of a customer:

1. Acceptance of deposits and other repayable funds from the public.[5]
2. Lending.[6]
3. Financial leasing.[7]
4. The transfer of money or value.[8]
5. Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money).
6. Financial guarantees and commitments.
7. Trading in:
   (a) money market instruments (cheques, bills, CDs, derivatives etc.);
   (b) foreign exchange;
   (c) exchange, interest rate and index instruments;
   (d) transferable securities;
   (e) commodity futures trading.
8. Participation in securities issues and the provision of financial services related to such issues.
9. Individual and collective portfolio management.
10. Safekeeping and administration of cash or liquid securities on behalf of other persons.
11. Otherwise investing, administering or managing funds or money on behalf of other persons.
12. Underwriting and placement of life insurance and other investment related insurance[9].
13. Money and currency changing.

---

[5] This also captures private banking.

[6] This includes inter alia: consumer credit; mortgage credit; factoring, with or without recourse; and finance of commercial transactions (including forfaiting).

[7] This does not extend to financial leasing arrangements in relation to consumer products.

[8] This applies to financial activity in both the formal or informal sector e.g. alternative remittance activity. See the Interpretative Note to Special Recommendation VI. It does not apply to any natural or legal person that provides financial institutions solely with message or other support systems for transmitting funds. See the Interpretative Note to Special Recommendation VII.

[9] This applies both to insurance undertakings and to insurance intermediaries (agents and brokers).

When a financial activity is carried out by a person or entity on an occasional or very limited basis (having reg ard to quantitativ e a nd absolute criteria) such that there is little risk of money laundering activity occurring, a country may decide that the application of anti- money laundering measures is not necessary, either fully or partially.

In strictly lim ited and j ustified circum stances, and based on a prov en low risk of m oney laundering, a country may decide not to apply some or all of the Forty Recommendations to some of the financial activities stated above.

"**FIU**" means financial intelligence unit.

"**Legal arrangements**" refers to express trusts or other similar legal arrangements.

"**Legal persons**" refers to bodies corporate, foundations, anstalt, partnerships, or associations, or any similar bodies that can establish a perm anent cust omer relationship w ith a financial institution or otherwise own property.

"**Payable-through accounts**" refers to correspondent accounts that are used directly by third parties to transact business on their own behalf.

"**Politically Exposed Persons**" (PEPs) are indiv iduals who are or hav e been entrusted with prominent public functions in a foreign country, for example Heads of State or of government, senior politicians, senior government, j udicial or m ilitary officials, senior executiv es of state ow ned corporations, important political party officials. Business relationships with family members or close associates of PEPs involve reputational risks similar to those with PEPs themselves. The definition is not intended to cover middle ranking or more junior individuals in the foregoing categories.

"**Shell bank**" means a bank incorporated in a jurisdiction in which it has no phy sical presence and which is unaffiliated with a regulated financial group.

"**STR**" refers to suspicious transaction reports.

"**Supervisors**" refers to the designated competent authorities responsible for ensuring compliance by financial institutions with requirements to combat money laundering and terrorist financing.

"**the FATF Recommendations**" refers to these R ecommendations and to the F ATF S pecial Recommendations on Terrorist Financing.

ANNEX

INTERPRETATIVE NOTES TO THE FORTY RECOMMENDATIONS

INTERPRETATIVE NOTES

General

1. Reference in this document to "countries" should be taken to apply equally to "territories" or "jurisdictions".

2. Recommendations 5-16 and 21-22 state that financial institutions or designated non-financial businesses and professions should take certain actions. These references require countries to take measures that will oblige financial institutions or designated non-financial businesses and professions to comply with each Recommendation. The basic obligations under Recommendations 5, 10 and 13 should be set out in law or regulation, while more detailed elements in those Recommendations, as well as obligations under other Recommendations, could be required either by law or regulation or by other enforceable means issued by a competent authority.

3. Where reference is made to a financial institution being satisfied as to a matter, that institution must be able to justify its assessment to competent authorities.

4. To comply with Recommendations 12 and 16, countries do not need to issue laws or regulations that relate exclusively to lawyers, notaries, accountants and the other designated non-financial businesses and professions so long as these businesses or professions are included in laws or regulations covering the underlying activities.

5. The Interpretative Notes that apply to financial institutions are also relevant to designated non-financial businesses and professions, where applicable.

Recommendations 5, 12 and 16

The designated thresholds for transactions (under Recommendations 5 and 12) are as follows:

- Financial institutions (for occasional customers under Recommendation 5) - USD/EUR 15,000.
- Casinos, including internet casinos (under Recommendation 12) - USD/EUR 3000
- For dealers in precious metals and dealers in precious stones when engaged in any cash transaction (under Recommendations 12 and 16) - USD/EUR 15,000.

Financial transactions above a designated threshold include situations where the transaction is carried out in a single operation or in several operations that appear to be linked.

Recommendation 5

Customer due diligence and tipping off

1. If, during the establishment or course of the customer relationship, or when conducting occasional transactions, a financial institution suspects that transactions relate to money laundering or terrorist financing, then the institution should:

    a) Normally seek to identify and verify the identity of the customer and the beneficial owner, whether permanent or occasional, and irrespective of any exemption or any designated threshold that might otherwise apply.

b) Make a STR to the FIU in accordance with Recommendation 13.

2. Recommendation 14 prohibits financial institutions, their directors, officers and employees from disclosing the fact that an STR or related information is being reported to the FIU. A risk exists that customers could be unintentionally tipped off when the financial institution is seeking to perform its customer due diligence (CDD) obligations in these circumstances. The customer's awareness of a possible STR or investigation could compromise future efforts to investigate the suspected money laundering or terrorist financing operation.

3. Therefore, if financial institutions form a suspicion that transactions relate to money laundering or terrorist financing, they should take into account the risk of tipping off when performing the customer due diligence process. If the institution reasonably believes that performing the CDD process will tip-off the customer or potential customer, it may choose not to pursue that process, and should file an STR. Institutions should ensure that their employees are aware of and sensitive to these issues when conducting CDD.

CDD for legal persons and arrangements

4. When performing elements (a) and (b) of the CDD process in relation to legal persons or arrangements, financial institutions should:

a) Verify that any person purporting to act on behalf of the customer is so authorised, and identify that person.

b) Identify the customer and verify its identity - the types of measures that would be normally needed to satisfactorily perform this function would require obtaining proof of incorporation or similar evidence of the legal status of the legal person or arrangement, as well as information concerning the customer's name, the names of trustees, legal form, address, directors, and provisions regulating the power to bind the legal person or arrangement.

c) Identify the beneficial owners, including forming an understanding of the ownership and control structure, and take reasonable measures to verify the identity of such persons. The types of measures that would be normally needed to satisfactorily perform this function would require identifying the natural persons with a controlling interest and identifying the natural persons who comprise the mind and management of the legal person or arrangement. Where the customer or the owner of the controlling interest is a public company that is subject to regulatory disclosure requirements, it is not necessary to seek to identify and verify the identity of any shareholder of that company.

The relevant information or data may be obtained from a public register, from the customer or from other reliable sources.

Reliance on identification and verification already performed

5. The CDD measures set out in Recommendation 5 do not imply that financial institutions have to repeatedly identify and verify the identity of each customer every time that a customer conducts a transaction. An institution is entitled to rely on the identification and verification steps that it has already undertaken unless it has doubts about the veracity of that information. Examples of situations that might lead an institution to have such doubts could be where there is a suspicion of money laundering in relation to that customer, or where there is a material change in the way that the customer's account is operated which is not consistent with the customer's business profile.

Timing of verification

6. Examples of the types of circumstances where it would be permissible for verification to be completed after the establishment of the business relationship, because it would be essential not to interrupt the normal conduct of business include:

   - Non face-to-face business.
   - Securities transactions. In the securities industry, companies and intermediaries may be required to perform transactions very rapidly, according to the market conditions at the time the customer is contacting them, and the performance of the transaction may be required before verification of identity is completed.
   - Life insurance business. In relation to life insurance business, countries may permit the identification and verification of the beneficiary under the policy to take place after having established the business relationship with the policyholder. However, in all such cases, identification and verification should occur at or before the time of payout or the time where the beneficiary intends to exercise vested rights under the policy.

7. Financial institutions will also need to adopt risk management procedures with respect to the conditions under which a customer may utilise the business relationship prior to verification. These procedures should include a set of measures such as a limitation of the number, types and/or amount of transactions that can be performed and the monitoring of large or complex transactions being carried out outside of expected norms for that type of relationship. Financial institutions should refer to the Basel CDD paper[10] (section 2.2.6.) for specific guidance on examples of risk management measures for non-face to face business.

Requirement to identify existing customers

8. The principles set out in the Basel CDD paper concerning the identification of existing customers should serve as guidance when applying customer due diligence processes to institutions engaged in banking activity, and could apply to other financial institutions where relevant.

Simplified or reduced CDD measures

9. The general rule is that customers must be subject to the full range of CDD measures, including the requirement to identify the beneficial owner. Nevertheless there are circumstances where the risk of money laundering or terrorist financing is lower, where information on the identity of the customer and the beneficial owner of a customer is publicly available, or where adequate checks and controls exist elsewhere in national systems. In such circumstances it could be reasonable for a country to allow its financial institutions to apply simplified or reduced CDD measures when identifying and verifying the identity of the customer and the beneficial owner.

10. Examples of customers where simplified or reduced CDD measures could apply are:

    - Financial institutions – where they are subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations and are supervised for compliance with those controls.

[10] "Basel CDD paper" refers to the guidance paper on Customer Due Diligence for Banks issued by the Basel Committee on Banking Supervision in October 2001.

- Public companies that are subject to regulatory disclosure requirements.
- Government administrations or enterprises.

11. Simplified or reduced CDD measures could also apply to the beneficial owners of pooled accounts held by designated non financial businesses or professions provided that those businesses or professions are subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations and are subject to effective systems for monitoring and ensuring their compliance with those requirements. Banks should also refer to the Basel CDD paper (section 2.2.4.), which provides specific guidance concerning situations where an account holding institution may rely on a customer that is a professional financial intermediary to perform the customer due diligence on his or its own customers (i.e. the beneficial owners of the bank account). Where relevant, the CDD Paper could also provide guidance in relation to similar accounts held by other types of financial institutions.

12. Simplified CDD or reduced measures could also be acceptable for various types of products or transactions such as (examples only):

    - Life insurance policies where the annual premium is no more than USD/EUR 1000 or a single premium of no more than USD/EUR 2500.
    - Insurance policies for pension schemes if there is no surrender clause and the policy cannot be used as collateral.
    - A pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme.

13. Countries could also decide whether financial institutions could apply these simplified measures only to customers in its own jurisdiction or allow them to do for customers from any other jurisdiction that the original country is satisfied is in compliance with and has effectively implemented the FATF Recommendations.

    Simplified CDD measures are not acceptable whenever there is suspicion of money laundering or terrorist financing or specific higher risk scenarios apply.

Recommendation 6

Countries are encouraged to extend the requirements of Recommendation 6 to individuals who hold prominent public functions in their own country.

Recommendation 9

This Recommendation does not apply to outsourcing or agency relationships.

This Recommendation also does not apply to relationships, accounts or transactions between financial institutions for their clients. Those relationships are addressed by Recommendations 5 and 7.

Recommendations 10 and 11

In relation to insurance business, the word "transactions" should be understood to refer to the insurance product itself, the premium payment and the benefits.

Recommendation 13

1. The reference to criminal activity in Recommendation 13 refers to:

   a) all criminal acts that would constitute a predicate offence for money laundering in the jurisdiction; or
   b) at a minimum to those offences that would constitute a predicate offence as required by Recommendation 1.

   Countries are strongly encouraged to adopt alternative (a). All suspicious transactions, including attempted transactions, should be reported regardless of the amount of the transaction.

2. In implementing Recommendation 13, suspicious transactions should be reported by financial institutions regardless of whether they are also thought to involve tax matters. Countries should take into account that, in order to deter financial institutions from reporting a suspicious transaction, money launderers may seek to state *inter alia* that their transactions relate to tax matters.

Recommendation 14 (tipping off)

Where lawyers, notaries, other independent legal professionals and accountants acting as independent legal professionals seek to dissuade a client from engaging in illegal activity, this does not amount to tipping off.

Recommendation 15

The type and extent of measures to be taken for each of the requirements set out in the Recommendation should be appropriate having regard to the risk of money laundering and terrorist financing and the size of the business.

For financial institutions, compliance management arrangements should include the appointment of a compliance officer at the management level.

Recommendation 16

1. It is for each jurisdiction to determine the matters that would fall under legal professional privilege or professional secrecy. This would normally cover information lawyers, notaries or other independent legal professionals receive from or obtain through one of their clients: (a) in the course of ascertaining the legal position of their client, or (b) in performing their task of defending or representing that client in, or concerning judicial, administrative, arbitration or mediation proceedings. Where accountants are subject to the same obligations of secrecy or privilege, then they are also not required to report suspicious transactions.

2. Countries may allow lawyers, notaries, other independent legal professionals and accountants to send their STR to their appropriate self-regulatory organisations, provided that there are appropriate forms of co-operation between these organisations and the FIU.

Recommendation 23

Recommendation 23 should not be read as to require the introduction of a system of regular review of licensing of controlling interests in financial in stitutions merely for anti-money laundering purposes, but as to stress the desirability of suitability re view for controlling shareholders in financial institutions (bank s and non- banks in particular) from a FA TF point of view. Hence, where shareholder suitability (or "fit and proper") tests exist, the attention of supervisors should be drawn to their relevance for anti-money laundering purposes.

Recommendation 25

When considering the feedback that should be prov ided, countries should hav e regard to the FAT F Best Practice G uidelines on P roviding F eedback to R eporting F inancial I nstitutions and O ther Persons.

Recommendation 26

Where a country has created an FI U, it should cons ider applying for m embership in the Eg mont Group. Countries should hav e regard to the Eg mont Group Statem ent of Purpose, and its Principles for Information Exchange Between Financial Intelligence Units for Money Laundering Cases. These documents set out important guidance concerning the role and functions of FIUs, and the mechanisms for exchanging information between FIU.

Recommendation 27

Countries should consider tak ing measures, including legislative ones, at the national level, to allow their competent authorities inv estigating money launde ring cases to postpone or w aive the arrest of suspected persons and/or the seiz ure of the m oney for the purpose of identify ing persons involved in such activ ities or for ev idence g athering. Without such m easures the use of procedures such as controlled deliveries and undercover operations are precluded.

Recommendation 38

Countries should consider:

a) Establishing an asset forfeiture fund in its respective country into which all or a portion of confiscated property will be deposited for law enforcement, health, education, or other appropriate purposes.

b) Taking such m easures as m ay be necessary to enable it to share among or between other countries confiscated property, in particular, when confiscation is directly or indirectly a result of co-ordinated law enforcement actions.

Recommendation 40

1. For the purposes of this Recommendation:

   - "Counterparts" refers to authorities that exercise similar responsibilities and functions.

   - "Competent authority " refers to all adm inistrative and law enforcem ent authorities concerned with com bating m oney laundering a nd terrorist financing , including the FI U and supervisors.

2. Depending on the type of competent authority involved and the nature and purpose of the co-operation, different channels can be appropriate for the exchange of information. Examples of mechanisms or channels that are used to exchange information include: bilateral or multilateral agreements or arrangements, memoranda of understanding, exchanges on the basis of reciprocity, or through appropriate international or regional organisations. However, this Recommendation is not intended to cover co-operation in relation to mutual legal assistance or extradition.

3. The reference to indirect exchange of information with foreign authorities other than counterparts covers the situation where the requested information passes from the foreign authority through one or more domestic or foreign authorities before being received by the requesting authority. The competent authority that requests the information should always make it clear for what purpose and on whose behalf the request is made.

4. FIUs should be able to make inquiries on behalf of foreign counterparts where this could be relevant to an analysis of financial transactions. At a minimum, inquiries should include:

   - Searching its own databases, which would include information related to suspicious transaction reports.
   - Searching other databases to which it may have direct or indirect access, including law enforcement databases, public databases, administrative databases and commercially available databases.

   Where permitted to do so, FIUs should also contact other competent authorities and financial institutions in order to obtain relevant information.

Universitetet i Stavanger

Appendix C – FATFs 9 spesialanbefalinger

Financial Action Task Force Groupe d'action financière

FATF Standards

FATF IX Special Recommendations

22 October 2004

FATF Special Recommendations on Terrorist Financing

Recognising the vital importance of taking action to combat the financing of terrorism, the FATF has agreed these Recommendations, which, when combined with the FATF Forty Recommendations on money laundering, set out the basic framework to detect, prevent and suppress the financing of terrorism and terrorist acts.

I. Ratification and implementation of UN instruments

Each country should take immediate steps to ratify and to implement fully the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism.

Countries should also immediately implement the United Nations resolutions relating to the prevention and suppression of the financing of terrorist acts, particularly United Nations Security Council Resolution 1373.

II. Criminalising the financing of terrorism and associated money laundering

Each country should criminalise the financing of terrorism, terrorist acts and terrorist organisations. Countries should ensure that such offences are designated as money laundering predicate offences.

III. Freezing and confiscating terrorist assets

Each country should implement measures to freeze without delay funds or other assets of terrorists, those who finance terrorism and terrorist organisations in accordance with the United Nations resolutions relating to the prevention and suppression of the financing of terrorist acts.

Each country should also adopt and implement measures, including legislative ones, which would enable the competent authorities to seize and confiscate property that is the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organisations.

IV. Reporting suspicious transactions related to terrorism

If financial institutions, or other businesses or entities subject to anti-money laundering obligations, suspect or have reasonable grounds to suspect that funds are linked or related to, or are to be used for terrorism, terrorist acts or by terrorist organisations, they should be required to report promptly their suspicions to the competent authorities.

V. International Co-operation

Each country should afford another country, on the basis of a treaty, arrangement or other mechanism for mutual legal assistance or information exchange, the greatest possible measure of assistance in connection with criminal, civil enforcement, and administrative investigations, inquiries and proceedings relating to the financing of terrorism, terrorist acts and terrorist organisations.

Countries should also take all possible measures to ensure that they do not provide safe havens for individuals charged with the financing of terrorism, terrorist acts or terrorist

organisations, and should have procedures in place to extradite, where possible, such individuals.

VI. Alternative Remittance

Each country should take measures to ensure that persons or legal entities, including agents, that provide a service for the transmission of money or value, including transmission through an informal money or value transfer system or network, should be licensed or registered and subject to all the FATF Recommendations that apply to banks and non-bank financial institutions. Each country should ensure that persons or legal entities that carry out this service illegally are subject to administrative, civil or criminal sanctions.

VII. Wire transfers

Countries should take measures to require financial institutions, including money remitters, to include accurate and meaningful originator information (name, address and account number) on funds transfers and related messages that are sent, and the information should remain with the transfer or related message through the payment chain.

Countries should take measures to ensure that financial institutions, including money remitters, conduct enhanced scrutiny of and monitor for suspicious activity funds transfers which do not contain complete originator information (name, address and account number).

VIII. Non-profit organisations

Countries should review the adequacy of laws and regulations that relate to entities that can be abused for the financing of terrorism. Non-profit organisations are particularly vulnerable, and countries should ensure that they cannot be misused:

(i) by terrorist organisations posing as legitimate entities;

(ii) to exploit legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset freezing measures; and

(iii) to conceal or obscure the clandestine diversion of funds intended for legitimate purposes to terrorist organisations.

IX. Cash Couriers

Countries should have measures in place to detect the physical cross-border transportation of currency and bearer negotiable instruments, including a declaration system or other disclosure obligation.

Countries should ensure that their competent authorities have the legal authority to stop or restrain currency or bearer negotiable instruments that are suspected to be related to terrorist financing or money laundering, or that are falsely declared or disclosed.

Countries should ensure that effective, proportionate and dissuasive sanctions are available to deal with persons who make false declaration(s) or disclosure(s). In cases where the currency or bearer negotiable instruments are related to terrorist financing or money laundering, countries should also adopt measures, including legislative ones consistent with Recommendation 3 and Special Recommendation III, which would enable the confiscation of such currency or instruments.