BANKERS PLIKT TIL Å FORETA RISIKOBASERT KUNDEKONTROLL OG LØPENDE OPPFØLGING ETTER HVITVASKINGSLOVEN

Universitetet i Oslo
Det juridiske fakultet

Kandidatnummer: 610
Leveringsfrist: 25.april 2012

Til sammen 17953 ord

24.04.2012

Innholdsfortegnelse

1 Innledning

1.1 Oppgavens problemstilling

Formålet med oppgaven er å belyse hvordan banker kan overholde sin plikt til å foreta risikobasert kundekontroll og løpende oppfølging etter hvitvaskingsloven. Dette vil jeg gjøre ved blant annet å ta for meg følgende underproblemstillinger:
Hva innebærer prinsippet om risikobasert kundekontroll? Hvordan foreta kundekontroll og løpende oppfølging? Hvordan gjøre disse risikobasert? Hva skjer hvis plikten ikke overholdes?

Hvitvaskingsloven, lov av 2009 3. juni nr. 1, har til formål å «*forebygge og avdekke transaksjoner med tilknytning til utbytte av straffbare handlinger eller med tilknytning til terrorhandlinger*», jf. § 1. Loven er et redskap som skal gjøre det vanskeligere å utnytte det finansielle systemet til å skjule utbytte fra kriminell virksomhet og terrorfinansiering og enklere avdekke profittmotivert kriminalitet.

Loven fastsetter en plikt for en rekke institusjoner og yrkesgrupper som regelmessig utfører transaksjoner til å identifisere og registrere opplysninger om alle kunder ved hjelp av lovbestemte kundekontrolltiltak. Banker omfattes av denne plikten. Kundekontrollen og den løpende oppfølgingen skal utføres med utgangspunkt i en risikobasert vurdering, det vil si at kontrolltiltakene skal stå i forhold til risikoen for hvitvasking og terrorfinansiering.[1] Grunnen er at det forutsettes at risikoen vil være forskjellig blant annet ut ifra kunde, kundeforhold, produkt. Ressurser bør derfor benyttes der behovet er størst.[2] Slik vil man på en optimal måte minimere risikoen og oppdage hvitvasking.

[1] Når det i det følgende snakkes om hvitvasking omfattes normalt også terrofinansiering om ikke annet blir sagt eller fremgår av sammenhengen.

[2] Ot.prp.nr.3 (2008-2009) s.46

1.2 Kort om begrepene hvitvasking og terrorfinansiering

Hvitvasking vil si å sikre utbytte fra straffbar handling. Utbyttets egentlige, illegale opprinnelse skjules, og pengene kan reinvesteres i den legale økonomien uten å vekke mistanke hos myndighetene. Når utbyttet fremstår som lovlig fremskaffet sier vi de er «hvitvasket». Dette kan skje på mange måter og nye metoder utvikles stadig.

Det er vanlig å dele hvitvaskingsprosessen opp i tre stadier.[3] Det første er et plasseringsstadium. Dette kan innebære smugling av penger, kontantkjøp av verdifulle gjenstander osv. Det andre stadiet er tilsløringsstadiumet. Utbyttet kanaliseres gjerne gjennom en rekke transaksjoner over hele verden, gjerne via mellommenn, for å skjule utbyttes opphav og endelige destinasjon. Det siste stadiet er integreringsstadiet. Utbytte fra straffbar handling blandes med lovlige midler, for eksempel næringer med mye kontanter, som restaurantdrift, og følgelig blir de beskattet sammen med den lovlige inntekten og fremstår dermed som «rene/hvite» penger.

Hvitvaskingsbegrepet er ikke benyttet i de materielle bestemmelsene i hvitvaskingsloven. Definisjon av begrepet ble av lovgiver derfor ikke ansett hensiktsmessig, da lovens tittel og formålsparagraf ville være tilstrekkelig klargjørende.[4] I straffeloven ble begrepet innført i straffeloven § 317 ved endringslov 30. juni 2006 nr. 49. Paragrafen skiller i motsetning til hvitvaskingsloven, mellom heleri og hvitvasking.[5] I EU-direktivet er hvitvaskingsbegrepet videre enn i straffeloven og omfatter også de klassiske heleritilfellene. Å vise til strl.§ 317 ville derfor kunne skape inkonsekvens i lovverket.[6] I hvitvaskingsloven brukes derfor «*transaksjon* (som) *har tilknytning til utbytte av en straffbar handling*», jf. § 1.

---

[3] Høgberg (2008) s. 31

[4] Ot.prp.nr. 3 (2008-2009) s.23

[5] *Heleri:* Den som mottar eller skaffer seg eller andre del i utbytte av en straffbar handling. *Hvitvasking:* Den som yter bistand til å sikre slikt utbytte for en annen.

[6] Ot.prp.nr.3(2008-2009) s.22

Tiltak for å motvirke terrorfinansiering omfattes også av loven selv om lovens tittel gir inntrykk av et noe snevrere formål enn lovens reelle formål. Fordi uttrykket allerede var innarbeidet i praksis lot man det bli stående.[7]

Det er vanskelig å finne en entydig definisjon av hva terror er, FNs medlemsland har ikke klart å enes. I lov av 20. mars 1998 nr. 10 § 3 nr. 5 defineres terrorhandlinger som *«Ulovlig bruk av, eller trussel om bruk av, makt eller vold mot personer eller eiendom, i et forsøk på å legge press på landets myndigheter eller befolkning eller samfunnet for øvrig for å oppnå politiske, religiøse eller ideologiske mål.»* Straffeloven regulerer terrorhandlinger i §§ 147 a, 147b og 147c. Terrorfinansiering er definert i strl. § 147c som fremskaffelse eller innsamling av midler som indirekte eller direkte har til hensikt å bli brukt helt eller delvis til å fullbyrde en terrorhandling.

1.3 Avgrensning og videre fremstilling.

Hvitvaskingsregelverket deles gjerne inn i tre hovedplikter:[8]

1) Plikt til å foreta risikobasert kundekontroll og plikt til å påvise dette i ettertid,
2) plikt til å foreta løpende oppfølging, samt plikt til å rapportere og undersøke mistenkelige transaksjoner, og
3) plikt til å etablere forsvarlige interne kontroll- og kommunikasjonsrutiner samt opplæringsprogrammer.

Temaet for denne oppgave er bankers plikt til å utføre risikobasert kundekontroll samt plikten til å foreta løpende oppfølging. Sistnevnte regnes også som et av kundekontrolltiltakene. Plikten innebærer konkrete og skjønnsmessig vurderinger, og vil være ulik avhengig av hvilken bransje man befinner seg i. Oppgaven avgrenses således mot andre rapporteringspliktige som er opplistet i hvitvaskingsloven § 4. Momenter i risikovurderingen vil også kunne være relevante i vurderingen av om en transaksjon er mistenkelig. Rapporteringsplikten er imidlertid en selvstendig plikt, som

[7] Endringsloven gjennomfører FN-konvensjonen 31.oktober 2003 mot korrupsjon Ot.prp.nr.3(2008-2009)s.19

[8] Runskriv 8/ 2009 s. 3

i tid normalt inntrer *etter* plikten til å foreta kundekontroll og løpende oppfølging. Redegjørelse av denne er dermed ikke nødvendig for fremstillingen her.

Fremstillingen vil i hovedsak behandle de ulike deler av den risikobaserte kundekontrollen i den rekkefølge de kommer i tid. Noen områder vil likevel bli behandlet på steder der de, etter min mening, gir en bedre sammenheng og forståelse av prosessen for risikobasert kundekontroll og løpende oppfølging.

1.4 Lovens virkeområde

Hvitvaskingsloven får anvendelse på rapporteringspliktige. «Rapporteringspliktige» er en felles betegnelse på de mest sentrale foretak, virksomheter og personer som kan misbrukes til hvitvasking og de er opplistet i hvitvasking § 4. Navnet «rapporteringspliktige» kommer av at det for disse, som nevnt over, følger en plikt til å rapportere til Økokrim om mistenkelige transaksjoner.

Finansieringsinstitusjoner er rapporteringspliktige, jf. hvitvaskingsloven § 4 første ledd nr.1. Banker regnes som finansieringsinstitusjon, jf. lov av 6.juni 1988 nr.40 om finansieringsvirksomhet og finansinstitusjoner § 1-3 første ledd. Direkte pliktsubjekter etter loven er institusjonene, men vil også omfatte deres ansatte. Loven gjelder rapporteringspliktige som er etablert i Norge, herunder filialer av utenlandske foretak, samt for Svalbard og Jan Mayen, jf. hvitvaskingsloven § 3.

1.5 Rettskilder

De sentrale rettskildene på området er lov av 3. juni 2009 nr. 11, «Hvitvaskingsloven» med forskrifter og forarbeider. Andre sentrale kilder er rundskriv fra Finanstilsynet, EU-direktivet samt anbefalinger fra Financial Action Task Force (FATF).

Hvitvaskingsloven av 2009 gjennomfører EUs tredje hvitvaskingsdirektiv vedtatt 26.oktober 2005 som Norge er forpliktet til å gjennomføre gjennom EØS-avtalen. Dette erstatter første og andre hvitvaskingsdirektiv som den tidligere hvitvaskingsloven av 2003 bygget på. Forløper til denne igjen var lov av 1988 10.juni § 2-17. Loven bygger også på anbefalinger av FATF.

FATF er et mellomstatlig samarbeid etablert i 1989 med det formål å utvikle og fremskynde tiltak mot hvitvasking. De utarbeider anbefalinger og foretar regelmessig evalueringer av medlemslandenes gjennomføring av disse. Selv om FATF sine anbefalinger ikke er juridisk bindende slik som EU-direktivene, er vi som medlemmer av FATF forpliktet til å gjennomføre disse.[9]

16.februar 2012 ble FATFs tidligere 40 anbefalinger med tiltak mot hvitvasking og 9 spesialanbefalinger med tiltak mot terrorfinansiering slått sammen og revidert til 40 anbefalinger som styrker de tidligere anbefalingene på flere områder.

Norge ratifiserte FN-konvensjonen om bekjempelse av finansiering av terrorisme 9.desember 1999. Sammen med flere resolusjoner fra FNs sikkerhetsråd, som påla stater å straffesanksjonere terrorhandlinger, ble dette bakgrunnen for vedtakelsen av §§ 147 a og § 147 b.[10] Disse ble vedtatt ved lov av 22. juni 2002. Straffeloven § 147c ble tilføyd ved lov 19.desember 2008 nr. 114.[11]

I forbindelse med oppgaven har jeg intervjuet/ hatt samtale med sentrale hvitvaskingsansvarlige i den norske banknæring om deres måte å foreta risikobasert kundekontroll og løpende oppfølging. Jeg snakket med Tor Ivar Mysen i DNB, Ole Einar Jørgenrud og Jørgen Eitrå i Sparebank1, og Trude S. Eidsheim i Pareto bank. Jeg bruker dette til å illustrere og forstå hvordan loven kan gjennomføres i praksis.

[9] Norge ble medlem i 1991

[10] Resolusjonene kom i kjølvannet av 9/11 i 2001

[11] Paragrafen gjennomfører europarådskonvensjonen om forebygging av terrorisme art. 5 til 7.

2 Risikobasert kundekontroll- Når inntrer plikten?

2.1 Hva innebærer prinsippet om risikobasert kundekontroll?

Prinsippet om risikobasert kundekontroll er lovfestet i hvitvaskingsloven § 5 og innebærer en strukturert og systematisk måte å håndtere risiko tilknyttet hvitvasking.[12] Kundekontroll(«customer due diligence»), vil i denne sammenheng si å gjennomføre legitimasjonskontroll, finne reelle rettighetshavere og identifiserer formålet med kundeforholdet.[13] Nytt av hvitvaskingsloven av 2009 er at kundekontrollen er risikobasert («Risk-based approach»), der det sentrale er at omfanget av tiltakene skal tilpasses antatt risiko for hvitvasking ut ifra en risikovurdering («on a risk-sensitive basis»).[14] Banken må foreta en bedømmelse av risikoen for å bli utnyttet til hvitvasking. Det mest sentrale verktøy for å håndtere risiko og hindre at systemene misbrukes til dette er ved å ha god kjennskap til kunden. Dette omtales gjerne som «kjenn din kunde-prinsippet» (Know Your Customer/ KYC-prinsippet). Dette oppnår banken via kundekontrolltiltak. Når banken på denne måten blir kjent med kundens identitet og adferd synliggjøres risiko knyttet til kunden. Jo høyere risiko, jo høyere krav til kundekjennskap og løpende oppfølging. Slik kan avvik, som gjerne ansees som indikator på hvitvasking, oppdages. Ved at informasjon om kunden registreres kan man også spore tilbake til vedkommende som foretok transaksjonen ved en evt. etterforskning.[15]

Prosessen fram til oppfyllelse av plikten kan deles inn i fire steg:[16]

1. Innsamling av informasjon om risiko for hvitvasking som er aktuelle: Banken må se på egen virksomhet, anbefalinger og typologier fra myndighetene og internasjonale organisasjoner, fra politi, interne rapporter i banken, tidligere

[12] Återgärder mot penningtvätt m.m (2010) s 77

[13] Den engelske oversettelsen følger av hvitvaskingsdirektivet art. 8 nr. 2.

[14] Ot.prp.nr.3(2008-2009) s.49

[15] NOU 2005:13 punkt 5.2.8

[16] Booth (2011) og Återgärder mot pennintvätt m.m (2010)

mistenkte tilfeller, risikorapporter, compliancerapporter, nye trender og mønster m.m.

2. Risikovurdering: Banken skal bedømme risikoen for at den utnyttes til hvitvasking. Dette gjøres ved å analysere bankens kunder, produkter, tjenester og andre relevante faktorer for så å sette kunden inn den aktuelle risikogruppe, som gjerne omfatter lav-, middels- og høyrisikogrupper. Hvor mange nivåer er opp til banken selv å bestemme.

3. Risikohåndtering: Kundekontrolltiltakene tilpasses ut fra en risikobasert tilnærming og ressurser fokuseres, som nevnt, der risikoen anses høy. Vi deler gjerne inn i tre nivåer av kundekontroll: forenklet-, normal- eller forsterket kundekontroll. Også her vil det være opp til banken hvor mange nivåer det opereres med. Lav risiko innebærer gjerne forenklet kundekontroll mens normal risiko medfører normal kundekontroll og ved høy risiko settes kunden til forsterket kontrollnivå.

4. Oppdatering, dokumentering og rapportering: Risikovurderingene skal løpende oppdateres hvis for eksempel nye produkter eller tjenester kommer inn. Banken må også løpende følge opp kundene for å registrere avvik. Plikten innebærer også at banker i ettertid kan påvise at lovens krav er oppfylt, jf. § 5(2).

2.2 Hensyn bak reglene om risikobasert kundekontroll

Fordi kriminelle gjerne har et behov for å få midler inn i den legale økonomien via finanssystemene spiller finansnæringen en sentral rolle for å oppdage og melde fra om mistenkelige transaksjoner. Hensynet bak kundekontrollen er at bankene skal bli kjent med kunden og dens økonomiske adferdsmønster slik at avvik og mistenkelige transaksjoner oppdages. Regelen om at kundekontrollen skal være *risikobasert* har til formål å minske risikoen for hvitvasking på en optimal måte. Det ivaretar også hensynet til effektiv bruk av ressurser, ved at de settes inn der behovet er størst, et kost-/nytteprinsipp. Dette leder til at kundekontrollen blir individuelt tilpasset, og tar avstand

fra tanken «one size fits it all»[17] Risikobasert kundekontroll leder etter min mening til et større krav til kunnskap om hva som innebærer hvitvaskingsrisikoer enn tidligere. Økt kunnskap leder igjen til en større bevissthet hos banker og deres ansatte. En slik bevissthet tror jeg bidrar til en bedre risikovurdering og gjennomføring av kundekontrollen. God opplæring av ansatte er imidlertid en forutsetning.

Den preventiv effekt av regelen viser seg ved at huller i finanssystemet tettes, hvitvasking gjøres vanskeligere og en effekt av dette er forhåpentligvis mindre kriminalitet. Risikoen hvitvaskeren har for å bli tatt har blitt større og må veies opp mot utbyttet. Prinsippet om risikobasert kundekontroll har ikke bare vokst fram på bakgrunn av internasjonalt samarbeid, virksomhetsutøvere har også vært pådrivere, fordi banker også har en egeninteresse i å overholde plikten om risikobasert kundekontroll.[18] Et eksempel kan være avtaler med VISA eller MasterCard hvor det gjerne kreves Anti Money Laundering policy-documents som viser at banken har rutiner for å motvirke at den brukes til hvitvasking. Dårlig rutiner kan medføre tap av bankens renommé og troverdighet, og med dette tap av kunder.

Plikten er også et utslag av en avveining av behovet for å avdekke kriminalitet opp mot borgernes behov for beskyttelse mot for sterk kontroll. Personvernhensyn er ivaretatt ved at ut fra en risikovurdering ikke innhentes mer informasjon. Dette problematiseres nærmere i punkt 7.

2.3 Plikten til å foreta risikobasert kundekontroll etter § 5

Plikten til å foreta risikobasert kundekontroll og løpende oppfølging følger som sagt av hvitvaskingsloven § 5 hvor det står at den *« … 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 …»* Det er viktig å fremheve at dette er en *plikt* for banker. Rapporteringspliktige skal også kunne *påvise* at

[17] Återgärder mot penningtvätt m.m (2010) s. 75

[18] Återgärder mot penningtvätt m.m (2010) s.76, se punkt 8

omfanget av utførte tiltak er tilpasset den aktuelle risikoen for hvitvasking, jf. § 5 annet ledd.[19] Begrepene i § 5 kan gi nærmere veiledning om hva plikten går ut på.

2.3.1 Begrepet «risiko»

Etter hvitvaskingsloven § 5 første ledd skal kundekontrollen foretas på grunnlag av en «vurdering av risiko». Hvordan skal risikobegrepet forstås? Risiko vil si fare, sjanse eller sannsynligheten for et visst negativt utfall. [20] For å gi mening må risikoen knyttes til en viss konsekvens, i hvitvaskingsloven er risikoen knyttet til konsekvensen hvitvasking. Vi sier derfor at «risiko» består av to faktorer: 1) *sannsynligheten* for at en transaksjon har forbindelse med hvitvasking eller terrorfinansiering, 2) *konsekvensen* av at den har en slik forbindelse. Risikovurdering foretas som en sikkerhet mot hvitvasking. Risiko og sikkerhet blir ofte definert som komplementære størrelser, der høy risiko krever høy sikkerhet, og lav risiko krever lavere sikkerhet. Intensiteten på kontrolltiltakene økes altså ved antatt høy risiko.

For å komme frem til den aktuelle risiko må det foretas en risikovurdering. Risikovurderingen er en systematisk måte å gjennomgå hvilke senarioer som kan innebærer risiko og deretter analysere virksomheten og deres kunder. Hvilke momenter som kan være aktuelle for risikovurderingen, se punkt 4.

2.3.2 Transaksjon

Etter hvitvaskingsloven § 2 første ledd nr.2 omfatter transaksjon «*enhver overføring, formidling, ombytting eller plassering av formuesgoder*». Det uttales i Ot.prp.nr.3 (2008-2009) s. 97, jf Ot.prp. nr. 72 (2002-2003) punkt 4.3, at begrepet skal tolkes vidt. Åpning av bankkonto og leie av bankboks vil omfattes, selv om det i vanlig språkbruk ikke betegnes som transaksjoner.[21] I EUs tredje hvitvaskingsdirektiv art. 20 heter det at rapporteringspliktige skal være spesielt oppmerksomme på «any activity» relatert til hvitvasking eller terrorfinansiering. «Any activity» vil direkte oversatt innebære *enhver* aktivitet, men blir i praksis tolket til å innebære det samme som transaksjon etter hvitvaskingsloven.

---

[19] Se punkt 8

[20] Store Norske Leksikon på nett

[21] Ot.prp.nr.3 (2008-2009)

2.3.3 Tilknytning til utbytte av straffbar handling

Rapporteringspliktige plikter å vurdere risiko for *«transaksjon med tilknytning til utbytte av straffbar handling»*, jf. § 5. Utbyttet må stamme fra en straffbar handling eller på annen måte stå i nær sammenheng med en straffbar handling. [22] Det er vanlig å betegne dette som tilknytningskravet og kriminalitetskravet. Banker skal kun vurdere risikoen for hvitvasking, ikke risikoen for alle straffbare forhold. «Straffbar handling» omfatter både forbrytelser og forseelser.[23] Begrepet «utbytte» skal forstås likt som straffeloven § 317 dvs. alt det man skaffer seg av verdi ved å foreta en straffbar handling, jf. Ot.prp.nr.3 (2008-2009) s.98.[24] Utbyttebegrepet må forstås vidt, slik at også sparte utgifter, som skatte- og avgiftsunndragelse noen ganger omfattes.[25] Transaksjoner som leder til et senere ulovlig utbytte er derfor også omfattet av loven.

En språklig forståelse av ordlyden tilsier at det ikke kreves mye for at tilknytning foreligger. Kravet etter § 17 om rapportering av transaksjoner krever kun «mistanke» om tilknytning. Også dette taler for en lav terskel med hensyn til tilknytningskravet.[26]

2.3.4 Tilknytning til forhold som rammes av straffeloven §§ 147a, 147b eller 147c.

Banker skal vurdere risikoen for transaksjoner med tilknytning til terrorhandlinger, såkalt terrorfinansiering.[27] Det avgjørende her er hva pengene skal brukes *til*, ikke hvor de stammer *fra.* Terrorhandlinger vil etter straffeloven § 147 a ramme de handlinger som dekkes av en rekke straffebud loven ramser opp, dersom de begås med forsett om å skape destabilisering eller ødeleggelse av grunnleggende funksjoner i samfunnet, utføres med det forsett å skape alvorlig frykt i en befolkning eller urettmessig tvinge offentlig myndigheter til å gjøre noe. 147 b rammer den som «fremskaffer» eller

---

[22] Se også Ot.prp.nr.53(1992-1993) s.24

[23] Dette er i samsvar med forståelsen av uttrykket «criminal offence» i Europarådets konvensjon om hvitvasking art 8

[24] Ot.prp.nr.3(2008-2009) s.98

[25] Ot.prp.nr.3(2008-2009) s.98, Rt. 1997 s.1637

[26] Chanana (2008) s. 104

[27] Jf. hvitvaskingsloven § 1.

«samler inn» formuesgoder med det forsett at formuesgodene skal finansiere terrorhandlinger, og den som stiller aktiver eller finansielle tjenester til rådighet for terrorister eller terrorgrupper.[28] Forberedelseshandlinger straffes også.
Straffeloven § 147 c rammer oppfordring, rekruttering eller opplæring til de fleste av terrorhandlingene som nevnes i §§147a og147 b.[29]

2.4 I hvilke situasjoner inntrer plikten til å foreta kundekontroll?

Plikten til å foreta kundekontroll etter hvitvaskingsloven § 6 kan utløses i fire alternative situasjoner. Disse situasjonene er:

1) ved etablering av kundeforhold,
2) ved transaksjon over 100.000kr,
3) ved mistanke om at en transaksjon har tilknytning til utbytte av straffbar handling eller terrorfinansiering,
4) ved tvil om hvorvidt tidligere opplysninger er tilstrekkelige.

Nedenfor vil jeg analysere nærmere når situasjonene ovenfor oppstår.

2.4.1 «Kundeforhold» vs. «leilighetskunder»

Etter § 6 nr. 1 skal kundekontroll foretas ved «etablering av kundeforhold».
I norsk rett kan du være kunde uten at det nødvendigvis vil si at et kundeforhold er etablert, en hvilken som helst kontakt med banken vil derfor ikke være nok, jf. Ot.prp.nr.3 (2008-2009) s. 52. For slike «leilighetskunder» som altså ikke anses å ha etablert kundeforhold, skal det bare foretas kundekontroll ved transaksjon over 100.000kr eller ved mistanke om straffbar handling, jf. hvitvaskingsloven § 6 nr. 2 og 3. Begrunnelsen for bruken av ordet «kundekontroll», som begrenser kretsen av de som skal omfattes av kundekontrollen, antar jeg har bakgrunn i en avveining av effektiv kontroll og personvernhensyn som tilsier at det ikke bør foretas kundekontroll ovenfor alle bankens kunder. Spørsmålet blir i hvilket omfang banken må ha hatt kontakt med kunden for at kundeforhold anses å foreligge.

---

[28] §§ 147 a og 147 b gjennomfører Norges folkerettslige forpliktelse etter terrorfinansieringskonvensjonen art. 2 og Sikkerhetsrådets resolusjon 1373 punkt 1 bokstav b og d.

[29] § 147 c gjennomfører europarådskonvensjonen om forebygging av terrorisme art. 5 til 7.

Dette beror etter forarbeidene på en konkret vurdering der varighet, art og andre forhold vil være momenter av betydning.[30] Tidsfaktoren er derfor sentral i vurderingen, noe som også følger av EU-direktivet hvor det kreves «an element of duration»). EUs tredje hvitvaskingsdirektiv art. 3(9) bruker ordet «business relationship» og en nærliggende oversettelse vil være forretningsforbindelse, men hvitvaskingsloven får anvendelse også der kunden er privatperson, for eksempel en bankkunde, og oversettelsen «kundeforhold» ble etter forarbeidene derfor ansett å passe bedre. Etter hvitvaskingsforskriften § 2 skal kundeforhold anses etablert når kunden kan bruke den rapporteringspliktiges tjenester. Opprettelse av bankkonto vil i alle tilfeller anses som etablering av kundeforhold da dette som regel vil være en forbindelse av en viss varighet, jf. hvitvaskingsforskriften § 2.[31] Forskriften § 2 nevner også utstedelse av betalingskort. Det kan oppstå kundeforhold selv om forholdet er ment å være kortvarig, for eksempel opprettelse av konto, selv om det er klart at opprettelsen kun vil benyttes i et engangstilfelle og deretter lukkes, jf. Finanstilsynets rundskriv s. 11. De antar videre at enkeltstående innskudd av kontanter eller betaling av giro i en bank uten at konto opprettes derimot ikke vil innebære etablering av kundeforhold. Har du mottatt en sjekk og går i en bank du ikke har konto eller bankkort i vil det ikke bli foretatt annen kontroll enn bekreftelse av identitet for å sikre at du er rette eier av sjekken, med mindre beløpet er over 100.000kr. Banken vil i slike tilfeller ikke ha videre kontakt med kunden, og det anses ikke naturlig å se dette som et kundeforhold. Kausjonister og garantister faller etter Finanstilsynets rundskriv s. 11 heller ikke inn under begrepet kundeforhold i hvitvaskingsloven.

Konklusjonen blir at kundeforhold i hvert fall som hovedregel må anses å foreligge der det har en viss varighet. I noen tilfeller vil imidlertid også kortvarige forbindelser omfattes.

2.4.2 Beløp over 100.000kr

I forhold til beløpsgrensen på 100.000 kr skal transaksjoner som ser ut til å ha sammenheng, regnes samlet. For forhandlere av gjenstander fremgår det av

[30] Ot.prp.nr.3(2008-2009) s.54

[31] Ot.prp.nr.3(2008-2009) s.54

hvitvaskingsforskriften § 3 nr.2 at plikt til å foreta kundekontroll oppstår også ved beløp i utenlandsk valuta tilsvarende 100.000kr. Selv om det ikke står uttrykkelig i loven tilsier lovens formål at en slik regel også bør gjelde for banker da en slik transaksjon må antas å innebære enda større risiko for hvitvasking. Å se sammenheng mellom transaksjonene kan bli vanskelig når informasjon om kunden ikke må registreres. Dette kan lede til at hvitvaskingstransaksjoner under 100.000 kr vanskelig fanges opp av banken. Det kan drøftes om regelen om å se sammenhengen mellom transaksjoner derfor innebærer et indirekte krav om at kundekjennskapstiltak også skal foretas for mindre transaksjoner. Dette vil imidlertid lede til en svært utvidet plikt som jeg antar loven ikke hadde til hensikt å innføre.[32] Jeg begrunner dette i personvernhensyn som tilsier at hvitvaskingsrisiko ikke skal bekjempes for enhver pris, samt hensyn til at det praktisk blir svært krevende å gjennomføre.

2.4.3 Mistanke

Plikt til å foreta kundekontroll ette r§ 6 nr. 3 også ved «*mistanke om at en transaksjon har tilknytning til utbytte av straffbar handling eller forhold som rammes av §§ 147a, 147 b eller 147 c*». Dette er uavhengig av beløp og om det gjelder en leilighetskunde eller et kundeforhold som er etablert tidligere. Denne plikten vil vanligvis inntre samtidig som undersøkelsesplikten etter § 17.

2.4.4 Tvil om hvorvidt tidligere innhentede opplysninger er korrekte eller tilstrekkelige

Hvitvaskingsloven § 7 første ledd nr. 4 vil være aktuell for allerede eksisterende kunder. Da hvitvaskingsloven var ny og spørsmålet om hvordan man skulle forholde seg til eksisterende kunder var denne særlig aktuell. Ut i fra en risikovurdering må man avgjøre om tidligere innhentede opplysninger anses tilstrekkelig eller om det skal gjennomføres en kontroll av kundeforholdet. Dersom det skjer forandringer i kundeforholdets art eller omfang kan dette tilsi ny kontroll. En student som plutselig har tre overføringer til Colombia i måneden er et forhold som bør føre til at det vurderes

[32] Återgärder mot penningtvätt m.m (2010) s.111

om de eksisterende opplysninger er tilstrekkelige. Plikten må sees i sammenheng med plikten til å foreta løpende oppfølging etter § 14.

2.5 Tidspunkt for kundekontrollen

Når skal banken foreta kundekontroll? Etter hvitvaskingsloven § 9 første ledd er hovedregelen er at kontrolltiltakene skal gjennomføres før etablering av kundeforholdet eller utføring av transaksjon etter § 6 nr. 2 og 3. Det gjelder visse unntak etter § 9 annet ledd dersom det ved «*etablering av kundeforholdet er nødvendig for ikke å hindre den alminnelige forretningsdrift*» og det er liten risiko hvitvasking, jf. § 9.[33] Innhenting av opplysninger blir gjerne vanskeligere i ettertid, dette kan tilsi at etablering av kundekontroll derfor heller bør nektes enn å utsettes.

3 Gjennomføring av kundekontrollen - de alminnelige kundekontrolltiltak

Hvitvaskingsloven§ 7 første ledd stiller opp fire konkrete kundekontrolltiltak rapporteringspliktige, som hovedregel, må foreta for å identifisere og oppnå bedre kjennskap til kunden.[34] Dette er registrering etter § 8, bekreftelse av identitet, bekreftelse av identitet til reelle rettighetshavere og innhenting av opplysninger om formål og tilsiktet art. Tiltakene er, som nevnt, utslag av prinsippet «kjenn-din-kunde». Regelen tilsvarer mer eller mindre tredje hvitvaskingsdirektiv art. 8. nr. 1. I forarbeidene på s.46 kalles disse de «alminnelige» kontrolltiltak. På bakgrunn av lovens system blir de også kalt de normale, eller grunnleggende kontrolltiltak. De skal som hovedregel gjennomføres ovenfor alle kunder og før etablering av kundeforhold. Men som nevnt, beror omfanget og intensiteten av kundekontrolltiltakene på hvilken risiko kunden antas å innebære. Dette kan lede til at sterkere kontrolltiltak skal anvendes,

[33] Unntaket gjelder også der det gjelder tegning av livsforsikringspolise forutsatt at bekreftelse av identitet foretas før utbetalingstidspunkt, eller ved åpning av bankkonto der det sikres at transaksjoner ikke kan utføres før bekreftelse av identiteten er foretatt.

[34] Rundskriv 8/2009 s. 11

eller unntaket om forenklet kundekontroll som innebærer at kunden er unndratt fra de alminnelige kontrolltiltak, se mer om dette under.

Kundekontrollen etter hvitvaskingslovens § 7 første ledd skiller mellom identifisering på den ene siden og bekreftelse av identiteten på den andre siden, men ofte vil disse to skje samtidig.

3.1 Registrering av opplysninger – kontrolltiltak nr.1

Kundekontrollen innebærer registrering av opplysninger, jf. § 7 første ledd nr. 1. Nærmere beskrivelse av hvilke opplysninger som skal registreres følger av § 8, dette vil blant annet være navn/ foretaksnavn, adresse, fødselsnummer/ organisasjonsnummer. Dette er en videreføring av den gamle hvitvaskingslovens § 6 første ledd nr. 1 til 3. I forarbeidene på s. 49 uttales at «*registrering av opplysninger, vil gi mindre rom for risikobaserte tiltak, enn andre kundekontrolltiltak*», dette fordi de opplysninger som kreves registrert er så konkrete.

3.2 Bekreftelse av kundens identitet – kontrolltiltak nr. 2

Kundens identitet skal verifiseres på grunnlag av gyldig legitimasjon. Dette er et ufravikelig krav, men hvor mye og hva som kreves av legitimasjon vil bero på en risikovurdering. Det betyr at ikke alle dokumenter må godtas som gyldig dokumentasjon og at kravet vil være forskjellig avhengig av hvilket produkt kunden etterspør og den risiko det antas å innebære. Økende misbruk og forfalskning av legitimasjonsdokumenter var faktorer som etter en risikovurdering ledet til at DNB og Sparebank1 kun godtok pass og bankID som gyldig legitimasjon ved opprettelse av nettbank. For de helt grunnleggende banktjenester slik som opprettelse av bankkonto, godtok de imidlertid andre legitimajsonsbeviser. Selv om det i hvitvaskingsforskriften legges opp til at også andre dokumenter kan være tilfredsstillende, kan en risikovurdering lede til at forskriftens minimumskrav ikke ville oppfylt plikten etter § 5 til å gjøre kundekontrollen risikobasert. Også pass kan innebære risiko, et eksempel kan være pass utstedt fra det italienske konsulatet i Italia til italiensk statsborger. Italia har ikke konsulat i Italia, passet er ugyldig. Scannere som oppdager falske pass brukes, men oppdager ikke alt. Ved usikkerhet om passets gyldighet bør banken be om ytterligere dokumentasjon. Dette kan være bekreftelse fra ambassaden eller konsulatet. Hva gjelder

«gyldig legitimasjon» har asylsøkerbeviset blitt endret til nå å inneholde navnetrekk og bilde og er godkjent for opprettelse av de mest grunnleggende banktjenester. Selv om beviset oppfyller kravet til «gyldig legitimasjon» er dette kun minimumskrav til legitimasjon og bankene kan også kreve andre legitimasjonsbevis så lenge det ikke er diskriminerende. I forhold til bruk av falsk legitimasjon kan det oppstå fare for feilregistrering og personer som registrerer seg flere ganger. Systemer som for eksempel krysseksaminerer fødselsnummer med navn kan kanskje forhindre dette.

Der kundebehandler er helt sikker på kundens identitet vil det være unødvendig å kreve gyldig legitimasjon, jf. § 7 femte ledd. Det er imidlertid få situasjoner dette unntaket kan tenkes anvendt. Eksempler kan være i små lokalsamfunn der man er sikker på kundens identitet.

3.3 Elektronisk legitimasjon

Verifisering kan som nevnt over, også skje på grunnlag av elektronisk legitimasjon, som Bank- ID. De krav som gjelder for dette er nærmere fastsatt i forskriftens § 6.

3.4 Reelle rettighetshavere

Rapporteringspliktige plikter etter hvitvaskingsloven § 7 første ledd nr. 3, å finne ut om det befinner seg reelle rettighetshavere bak kunden, og i så fall hvem dette er. Begrunnelsen er at kompliserte eierforhold gjerne brukes som «selskapsslør» som fremmer anonymitet og dermed gjør hvitvaskingen lettere.[35] Det er derfor viktig at banken identifiserer hvem som er den virkelige eier. Dette kan være vanskelig. Spørsmålet blir derfor når banken anses å ha oppfylt sin plikt til å identifisere reelle rettighetshavere.

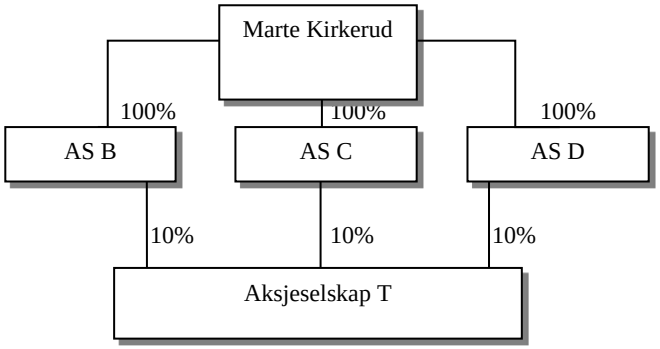
Begrepet reell rettighetshaver («beneficial owner») er definert i hvitvaskingsloven § 2 første ledd nr. 3 som «*fysiske personer som i siste instans eier eller kontrollerer en kunde eller som en transaksjon gjennomføres på vegne av*». «Siste instans» refererer til den siste personen i en eventuell kjede av personer som utøver eierskap eller kontroll. Lovens ordlyd «på vegne av» tilsier en vid tolkning, men enhver interesse i

[35]Høg/ Busck-Nielsen (2008) s.56

transaksjonen vil allikevel ikke føre til at man regnes som reell rettighetshaver.[36] En viss veiledning gis i § 2 nr. 3 a-e: Reell rettighetshaver er person som direkte eller indirekte kontrollerer mer enn 25% av eierandelene i et selskap, b) utøver kontroll over ledelsen av en juridisk person på samme måte som i bokstav a, c) skal overta 25% av formuesgodene i en stiftelse, d) har hovedinteressen i en stiftelse. Finanstilsynet antar i sitt rundskriv på s.17 at oppregningen ikke er uttømmende og at også andre personer enn de som nevnes etter en konkret vurdering kan regnes som reell rettighetshaver. Finnes det reelle rettighetshavere bak kunden, skal banken ut fra en risikovurdering og på grunnlag av «egnede tiltak», innhente tilstrekkelig informasjon til å forstå eierskapet og kontrollstrukturen hos kunden.[37] Selv om dette ikke har kommet like klart til uttrykk i hvitvaskingsloven som i EU-direktivets art. 8.1 bokstav b, fremheves i Rundskrivet på s. 17 at det ikke er tvil om at de krav som der stilles også må gjelde etter norsk lov.

Eksemplet nedenfor illustrerer at eierstrukturene kan være komplekse, og derfor gjøre det vanskelig å identifisere reelle rettighetshavere: [38]

Figur 1



Dersom T som er et AS der B, C og D, eier 10 % hver av aksjene, mens Marte Kirkerud eier alle aksjer i B, C og D er Marte den reelle rettighetshaver med indirekte kontroll over 30% av aksjene i T. Kjedene er gjerne lenger enn eksemplet viser.

Banker bruker offentlige registre over reelle rettighetshavere, som Brønnøysundregistrene (herunder stiftelsesregisteret, enhetsregisteret eller

[36] Rundskriv 8/2009 s.16

[37] Rundskriv 8/2009 s.17

[38] Återgärder mot penningtvätt m.m (2010) s.125

frivillighetsregisteret). For utenlandske selskap finnes tilsvarende registre. Elektronisk sjekk mot disse er vanlig, men de er ikke pålitelige nok, og navn bør også sjekkes opp manuelt. Kunden bes gjerne om å fylle ut skjema hvor det skal opplyses om reelle eierforhold. Foretakets årsregnskap, aksjeeierbok, selskapsavtale etc. bør også brukes for å bekrefte reelle rettighetshavere. Dette er ofte forhold som ikke vil fremkomme av registrene og må derfor undersøkes manuelt. For børsnoterte selskap vil eierforhold skifte hele tiden, og man kan spørre seg om bankene noen gang kan være sikker på identiteten.

For kunde som oppfyller kravene for forenklet kundekontroll etter § 13, vil prinsippet om risikobasert kundekontroll medføre at nærmere undersøkelser av reelle rettighetshavere ikke er nødvendig. Ved mistanke om hvitvasking etter § 6 nr. 3 gjør imidlertid § 13 ikke unntak fra å foreta kundekontroll. Relle rettighetshavere må da også undersøkes.

Det er også gjort unntak for plikten til å foreta kundekontroll etter § 6 nr. 1,2 og 4 for konti med midler fra flere personer som føres av advokater og andre uavhengige jurister, jf. hvitvaskingsforskriften § 10. Transaksjoner som gjøres på vegne av et stort antall personer gjøres gjerne uten at banken har kontakt med den egentlige eier, og mulighet for å få gode nok opplysninger om formålet er ofte vanskelig.[39] I utgangspunktet vil dette innebære forhøyet risiko. At banken i hvert fall forstår virksomhetsstrukturen vil derfor være viktig.[40] I praksis vil imidlertid konti med midler fra flere personer gjerne være omfattet av reglene om forenklet kundekontroll, særlige kontrollregler for reelle rettighetshavere kommer da ikke til anvendelse.

Redegjørelsen ovenfor viser at banken må forstå eierskapet og kontrollstrukturen hos kunden. Jeg vil på bakgrunn av redegjørelsen over anta at elektronisk sjekk av kunden opp mot ulike offentlige registre vil være egnede tiltak.

[39] Rundskriv 8/2009 s.20

[40] Rundskriv 8/2009 s.20

3.5 Opplysninger om kundeforholdets formål og tilsiktede art

Banken plikter å registrere opplysninger om formål og tilsiktet art for kundeforholdet, jf. § 7 første ledd nr. 4. Gjennom slike opplysninger vil banken bli kjent med kundens normale transaksjonsmønster. Dette er viktig slik at evt. avvik fra registret kundeprofil kan oppdages i den løpende oppfølgingen, § 14, da avvik kan indikere hvitvasking. Lov og forskrift gir ingen fasit på hvordan plikten etter § 7 nr. 4 oppfylles annet enn at den skal være risikobasert, jf. § 5. En språklig forståelse av «kundeforholdets formål» innebærer informasjon om hvilke produkter og tjenester kunden ønsker og hvorfor hun ønsker disse. Med «tilsiktet art» forstår jeg informasjon om hvordan kunden forventer å bruke kundeforholdet, slik at banken føler den har kjennskap til kundens normale bruk. Dette vil være informasjon om hva bankkontoen skal benyttes til, hvilke transaksjoner kunden normalt vil utføre, til hvem, og i hvilke valutaer m.m. I Finanstilsynets generelle observasjoner til tematilsyn vedrørende gjennomføring av hvitvaskingsloven i mars 2009 presiseres at opplysninger om formål og tilsiktet art skal baseres på informasjon fra kunden og ikke på institusjonens egne antakelser alene. Rapporteringspliktige må derfor innhente «*tilstrekkelige kundeopplysninger som muliggjør løpende oppfølging i henhold til lovens § 14*» jf. Finanstilsynets rundskriv 8/2009 s. 21.Hva som anses som «tilstrekkelige kundeopplysninger» for banken, må banken selv ta stilling til ut fra en risikobasert vurdering. Spørsmål for å oppnå dette kan være:[41]

- Hva kundeforholdet skal brukes til; sparing og evt. hvilken type sparing, boliglån, lønn/brukskonto, innskudd valuta, finansiering og hvilken type etc. (hva det blir spurt om her vil bero på de produkter banken tilbyr).
- Midlenes opprinnelse
- Om det er sannsynlig at kunden vil foreta kontantinnskudd på til sammen mer enn 100.000kr pr. kalenderår, hvis ja, hva er årsaken til dette?
- Om kunden vil foreta betalinger eller investere på vegne av andre på til sammen mer enn 100.000kr pr. kalender år? Hvis ja, hva er formålet samt navn på person eller organisasjonsnummer.
- Hvis juridisk person; brukes kontanter mye i næringen?

[41] Hentet fra kundeerklæringsskjemaer i Sparebank1 og Pareto bank.

- Om det er sannsynlig at kunden vil foreta større overførsler til/fra utlandet (som for eksempel overstiger 100.000kr for privat kunde eller 200.000kr for juridiske personer)?

Ved å samle inne all disse opplysninger, gjerne via skjema i banken eller over nett, vil man få et inntrykk av kundens antatte normale bruk av kontoen. Rundskrivet viser til innhenting av samme type opplysninger. Opplysningene kan lede til at kunden må settes på forsterket kontrollnivå, eller mistanke om at kunden vil bruke kundeforhold til hvitvasking noe som kan lede til rapporteringsplikt. Riktignok kan kunden som vil hvitvaske penger fra et skatteparadis opplyse at penger vil bli overført derfra fordi han har en rik onkel der. Slike løse utsagn vil som regel ikke de store bankene ha kapasitet til å følge opp med det antall kunder de har, men store overføringer bør lede til nærmere undersøkelser. Kunden får så opprettet en kundeprofil eller «intended users profile». Profilen har på forhånd utpekt hva som anses for «normal bruk» for den og den kunden, for eksempel student, pensjonist, diplomat etc. samt ut ifra de opplysninger kunden gir om formål og tilsiktet art. I følge Finanstilsynets runskriv på s. 21 vil det som hovedregel ikke være påkrevet med en «detaljert og finmasket» inndeling av kundegruppene, men jo mer detaljert, jo bedre løpende oppfølging.

3.6 I hvilken grad kan kundekontroll utført av tredjepart eller utkontraktringsavtale brukes for gjennomføring av kundekontrollen?

Det følger av § 11 at gjennomføring av kundekontrolltiltak som nevnt i § 7 nr. 2-4 kan legges til grunn når de er utført av de tredjeparter loven stiller opp(dette er stort sett andre rapporteringspliktige). Registrering av opplysninger som nevnt i § 8 må de imidlertid foreta selv. Banker kan også utkontraktere/outsource eller avtale at andre firmaer eller rapporteringspliktige utfører de normale kundekontrolltiltakene, jf. hvitvaskingsloven § 12. Både §§ 11 og 12 er unntak fra hovedregelen om at rapporteringspliktige selv utfører kundekontrollen. Ansvar for at kundekontroll gjennomføres i samsvar med lov og forskrift gjøres det imidlertid ikke unntak fra. Dette vil til syvende og sist alltid ligge på den rapporteringspliktige, jf. §§ 11 annet ledd nr. 2 og § 12 tredje ledd.

3.7 Følger av at kundekontroll ikke kan gjennomføres

Dersom kundekontroll ikke kan gjennomføres, følger det av hvitvaskingsloven § 10 at banker ikke skal etablere kundeforhold. Er kundeforholdet allerede etablert skal det avvikles hvis fortsettelse medfører risiko for hvitvasking. Spørsmålet blir da om dette skal rapporteres til Økokrim. Lovens formål kan tale for det (og slik var praksis i banker jeg intervjuet), da slik informasjon kan bidra til å avdekke hvitvaskingsoperasjoner ved at viktig etterretningsinformasjon gis til Økokrim.

4 Prosessen for risikovurderingen

Kundekontroll og løpende oppfølging må, som nevnt flere ganger, foretas på grunnlag av en «*vurdering av risiko*» for hvitvasking. Risikoen skal «*vurderes ut fra type kunde, kundeforhold, produkt eller transaksjon*», jf. § 5. Spørsmål om hva som er akseptabel risiko, hvilke forhold som innebærer risiko, deres vekt i en risikovurdering og hvordan selve systemet for å foreta en slik vurdering av den enkelte kunde skal gjennomføres i henhold til loven er problemstillinger som oppstår. Disse blir belyst under.

Selv om en kunde antas å innebære høy risiko betyr ikke dette at banker skal forbys å ha slike kunder. All økonomisk aktivitet vil innebære en risiko og så lenge prosedyrene for å håndtere og følge opp kundeforholdet etter prinsippet om risikobasert kundekontroll er på plass vil man som regel ligge på et akseptabelt risikonivå.

Lovgiver har til en viss grad identifisert kunder med høy risiko, dette vil jeg komme tilbake til i punkt 5.1, de øvrige må grupperes av banken etter en konkret risikovurdering. I hvitvaskingsforskriften § 12 nevnes noen situasjoner som kan utløse undersøkelses- og rapporteringsplikt. Finanstilsynet antar at disse situasjoner etter en konkret vurdering også vil kunne være relevante eksempler på situasjoner som etter sin art kan innebære høy risiko og utløse forsterkede kontrolltiltak.[42] Situasjonene som

[42] Rundskriv 8/2009 s.27

nevnes er tatt med i vurderingene nedenfor. Stort mer sier ikke lov og forskrift om risikovurderingen.

En del banker opererer ikke med kategorien lav risiko, men kun normal, høy og ekstra høy risiko.[43] Begrunnelsen var at kunder som omfattes av forenklet kundekontroll etter § 13 var de eneste som ville innebære lav risiko. Hvilke kunder dette gjaldt fulgte etter deres oppfatning klart av loven, og ga ikke rom for noen vurdering. Om vilkårene for forenklet kundekontroll foreligger, beror imidlertid på en vurdering, se punkt 5.3.

Et problem som kan oppstå er at en kunde som er utpekt som høy risiko i lovgivningen, også er vurdert som lavrisikokunde.[44] Jeg antar da at det må foretas en konkret risikovurdering for å avgjøre dette.

4.1 Hvilke faktorer bør tas i betraktning ved risikovurderingen?

Hva som innebærer risiko er ingen statisk vurdering og vil endre seg over tid ettersom samfunnsforholdene utvikler seg og trusselen endres.[45] Det legges opp til skjønnsmessige og konkrete vurderinger hos bankene. En uttømmende liste over hvilke faktorer som innebærer risiko for at banken utnyttes til hvitvasking kan derfor ikke lages. Momentene nedenfor vil imidlertid være relevante. De bygger blant annet på typologier utarbeidet av internasjonale organisasjoner, tilsynsmyndigheter og erfaring innenfor virksomheten. I Finanstilsynets Runskriv på s. 6 gis en rekke linker til slike internasjonale kilder.

Identifiseringen av risikomomenter i forhold til terrorfinansiering vil ha mange likheter men også noen ulikheter sammenlignet med hvitvasking. Terrorfinansiering vil være vanskelig å oppdage fordi de ikke trenger å ha ulovlig opprinnelse. I tillegg vil det gjerne være småbeløp som ikke gir utslag for avvik i et elektronisk system. De parametere som vanligvis brukes er om personer eller organisasjoner står på sanksjonslister (terrorlister). Eksempler på slike lister er EU-listen og OFAC-listen,

[43] Samtale med Ole Jørgen Eitrå, Sparebank1 25.01.2012

[44] Återgärder mot penningtvätt m.m (2010) s.93

[45] FATF *Guidance on the Risk-Based Approach* s. 15

disse nevnes i Finanstilsynets rundskriv s. 28. Andre internasjonale lister vil også være aktuelle, for eksempel FNs såkalt terrorliste over individer og enheter som antas å ha forbindelse til Taliban, Al Qaida eller Osama Bin Laden sitt tidligere nettverk. Å stå på listen har ingen strafferettslige konsekvenser, men FNs medlemsland skal blant annet fryse deres økonomiske midler. Banker foretar en elektronisk sjekk av sine kunder opp mot slike lister. En rekke firmaer tilbyr banker å abonnement på slike lister, for eksempel World Check som er en portal som tilbyr lister fra hele verden. Listene som tilbys bygger gjerne på «open source» -informasjon fra internasjonale myndighetsorganer.[46] Det gis lite rom for risikovurdering ved en slik sjekk. Dersom kunden får treff bør banken sjekke opp manuelt om kunden virkelig er personen på listen. I sin kamp mot terror har USA utarbeidet egne sanksjonslister som norske banker gjerne sjekker sine kundeprofiler opp mot. Dette som følge av krav fra amerikanske banker de samarbeider med. Vurderingen nedenfor dreier seg derfor i hovedsak om risikomomenter i forhold til hvitvasking, men mange av de samme momentene vil være aktuelle også for å oppdage terrorfinansiering.

Målet for risikovurderingen er å finne ut *hvilken* risiko kunden innebærer. Vi må derfor kartlegge *hvem* som hvitvasker, *hvor* men viktigst *hvordan* hvitvasking skjer. Som FATF i *Guidance to Risk- Based Approach,* har jeg delt opp i fire hovedkategorier av risiko eller segmenter. Innenfor den enkelte gruppe vil det være flere inndelinger. Jo mer finmasket vurderingen er og jo mer finmasket risikovurdering og bedre risikobasert kundekontrollen. Vekten disse faktorer og kategorier gis vil ut fra en risikovurdering kunne være ulike avhengig av den enkelte bank, jf. § 5.

4.1.1 Hvilke kunder innebærer høy risiko?

- Privatkunder

Økokrim har laget en oversikt over viktige risikoindikatorer som bygger på konkrete hvitvaskingsmetoder og rapporter fra hele verden.[47] Eksempler vil være kunder som tilbakeholder eller mangler opplysninger om for eksempel postboksadresse, tviler når

[46] Eksepler på kilder til lister World check bygger på: Office of foreign assets control:USA, New York Stock Exchange), HM Treasury (The UK's economics & finance ministry), Interpol, Europol, CIA, FBI, Iran sanksjoner(Bureau of international security and nonproliferation sanctions) for å nevne noen.

[47] Økokrim, Indikator på hvitvasking (2010)

vedkommende skal svare eller viser lite interesse for omkostninger og renter. Kunder som ikke velger enkleste transaksjonsform, men går via unødvendige omveier kunden ikke kan gi noen utførlig forklaring på eller gir en forklaring som virker innlært kan også være forhold som bidrar til at kunden anses å innebære høy risiko. Hvis kundens klær, biler eller bostedsadresse ikke harmonerer med inntekten, for eksempel der den består av trygd og sosialstøtte, kan dette tyde på at midlene kommer fra kriminelle handlinger. Kunder som er mistenkt for straffbare forhold bør bli vurdert som høyrisikokunder særlig dersom vedkommende er mistenkt for økonomisk kriminalitet eller andre lovbrudd som kan generere et økonomisk utbytte. Dette kan banker få en viss oversikt over ved å følge med i media.

- Bedriftskunder

Selskapskonstruksjoner er viktige i den legale økonomien, men kan utnyttes av kriminelle, da det her kan skjules store beløp. Komplisert selskaps- og eierstruktur kan gjøre det vanskelig og ressurskrevende å avdekke hvitvasking og dermed lettere å skjule midlenes opphav. Et foretak med komplisert struktur kan derfor innebære høy risiko dersom det ikke fremstår noen fornuftig grunn for en slik organisering av virksomheten. Eksempler er selskaper som opprettes i en rekke land og selskaper som ikke har noen reell aktivitet og kun brukes til å hvitvaske penger. Transaksjoner til nærstående kan være et ledd i å unndra midler fra selskapet, ved at de utad fremstår som utgifter.

Enkeltmannsforetak er en selskapstype som innebærer større risiko for hvitvasking. Den Ofte blandes den private økonomien med bedriftens, slik blir det lettere å skjule den egentlige inntekten og dermed unndra skatt. En håndverker kan for eksempel unnlate å føre opp alle oppdrag vedkommende har hatt. Har personen felles konto for foretaket og sin private økonomi vil det ikke være unaturlig om en del summer som kommer inn på konto ikke er med i regnskapet. Det samme gjelder ansvarlige selskap (ANS), hvor det ofte er få personer og ingen til å kontrollere hva som gjøres. Muligheten for hvitvasking er derfor større der enn i et stort firma der man gjerne har overordnede som følger med på hva som skjer nedover i firmaet. For norskregistrerte utenlandske foretak (NUF) er det erfaringsvis større fare for selskapsstrukturer som kun er laget for å skjule midler fra ulovlige handlinger. Grunnen kan være at det for disse er lempeligere krav om revisjon og aksjekapital. Etter at nye regler som kun krever egenkapital på 30.000kr for AS er

det trolig at mange som tidligere valgte NUF nå vil velge AS, jf. lov av 13. juni 1997 nr. 4, Aksjeloven, § 3-1. Banker bør derfor også rette oppmerksomheten mot AS med mindre egenkapital. Veldedige organisasjoner (NGOer) kan innebære høy risiko for hvitvasking dersom de ikke er subjekt for noen overordnet kontroll. Særlig de som arbeider på tvers av landegrenser, da slike transaksjoner gjør at midlere lettere kan skjules.[48] Banken bør derfor finne ut av om det er forbindelse mellom NGO-ens formål og transaksjonen, og om transaksjoner foretas uten noe økonomisk formål.[49] Et selskap uten revisor til å kontrollere regnskapet vil også innebære høyere risiko. Er det en stor og uforklarlig avstand mellom foretaket og der kundene er, eller det sendes store og uforklarlige beløp til andre institusjoner kan dette være også indikatorer på hvitvasking, jf. FATF *Guidance to Risk-Based Approach* s. 23.

- Profesjonalitetshjelpere

For profesjonelle hvitvaskere, som har et utbytte av en slik størrelse at det ikke lar seg skjule ved privat forbruk, brukes gjerne profesjonalitetshjelpere eller «gatekeepers»)som har god innsikt i det finansielle systemet. De har kunnskap slik at svarte penger kan integreres i en eller hvit virksomhet.[50] Ettersom rapporteringspliktige gjerne befinner seg innenfor den finansielle sektoren, der økonomisk kriminalitet lett kan finne sted, vil de også kunne yte viktig bistand til hvitvaskeren. De har derfor mulighet til å tilsløre midlere ved å gi hjelp til å etablere selskaper, pengetransaksjoner, eller gi finansielle og juridiske råd for hvordan pengene bør plasseres.[51] Klientkontoer kan innebære risiko. De brukes av blant annet advokater, meglere, inkassatorer og andre som driver mellommannsvirksomhet og oppretter konto som er adskilt fra egne midler. De kan misbrukes på flere måter fordi overføringer til klientkonto i utgangspunktet stopper spor og vanskeliggjør oppklaring av saker. Kontoen registreres i banken på for eksempel advokatens navn, kunden/ klientens navn forblir anonym. Behov for klientkonto kan være ved forskudd på salær, til erstatningsoppgjør der man venter på klientens instruks omkring hvordan midlene skal disponeres etc. I forhold til advokaters

[48] FATF *Guidance to Risk-Based Approach* s. 24

[49] Økokrim, Indikator på hvitvasking (2010)

[50] Stridbeck (2008) s. 55

[51] Økokrim: *Trendrapport hvitvasking 2011* s. 24.

klientkonto vil taushetsplikten gjerne gjøre seg gjeldende. Eksempel på dette har vi i Rt.2010.1638, der Økokrim gav et advokatfirma pålegg om å utlevere opplysninger om hvem som var mottakere av tre spesifiserte overføringer over firmaets klientkonto. Høyesterett kom til at advokaters taushetsplikt var til hindre for dette.[52] Begjæringen om utleveringspåstand ble derfor ikke tatt til følge.

Bankansatte selv kan være aktuelle medhjelpere for hvitvaskeren, se punkt 4.2.2. De kundegrupper loven på forhånd har utpekt som høyrisikokunder behandles under i punkt 0.

4.1.2 Hvilken næring innebærer høy risiko?

Hvilken næring kunden arbeider i kan gi ulike muligheter for hvitvasking. Erfaringsmessig vil næringer med stor kontantstrøm innebære en høyere risiko for hvitvasking. Dette kan være utesteder, bilverksted, bygg- og anleggsbransjen etc. Kontanter er fortsatt viktig for kriminelle, de legger ikke igjen elektroniske spor og er derfor vanskeligere å spore. Ulovlig utbyttet tas ofte inn i kontantbasert næring, som senere oppføres som lovlig inntjent inntekt. Under- og overfakturering er kjent hvitvaskingsmodus. Et skoleeksempel har vi i en sak fra Nedre Romerike tingrett 6. februar 2012 der to personer ble dømt for heleri etter at de hadde etablert et malerfirma som i realiteten kun opererte som et faktureringsselskap og uttaksledd for andre selskaper. 12 millioner var kommet inn på tiltaltes konto ved hjelp av fiktive fakturaer til andre selskaper, og via 67 kontantuttak ble pengene tatt ut og levert tilbake til de respektive selskapene. Slik unngikk de skatt og kunne betale svarte lønninger. Mannen fikk selv en fortjeneste på 5-7 % av det hvitvaskede beløpet. Operasjonen ble gjort mulig via bankkonto skaffet på bakgrunn av falsk ID og registret firma. Saken viser viktigheten av at banken forstår selskapets struktur og hva som foregår i selskapet, men også at det innenfor håndverknæring er fare for slik fiktiv fakturering.[53] Banker må derfor være oppmerksomme på om inntekten harmoniserer med omfanget av virksomheten, eller om konsumet, for eksempel fine biler, dyre klær tilsier at midler også må komme fra andre steder enn lovlig inntekt. Har en virksomhet som var på

[52] Se også Rt. 2911 s.1

[53] Se også LB-2010-62670-2 «Undervisningsbygg»

konkursens rand plutselig et uforklarlig oppsving i økonomien, kan dette skyldes at ulovlige midler settes inn i den legale bedriften.[54] Banker bør, så vidt mulig, følge med i aviser og på markedet i de ulike næringer. I Pareto bank fikk jeg opplyst at fordi de har en stor andel bankkunder innen verdipapirhandel, vil deres ansatte ha svært god kunnskap og innsikt i markedet.[55] Slik kan de oppdage unormalt store gevinster. Også fiskerinæringen antas å innebære høy risiko da det her kan forekomme ulovlig fiske og utbyttet av dette da vil være fra et straffbart forhold. Drosjenæringen i Oslo har hatt store saker om hvitvasking og antas derfor å innebære høy risiko, ut fra en konkret risikovurdering av drosjenæringen i Hamar vil ikke Sparebanken Hedmark nødvendigvis klassifisere næringen på samme måte.

Rengjøringsbransjen er en bransje der det ofte forekommer hvitvasking. Gjennomsnittslønnen er gjerne under tariffavtalesatsene og skatt unndras. I en sak i Oslo Tingrett fra mai 2005 hadde en person mottatt flere millioner på kontoen sin. De ble raskt tatt ut i kontanter. Banken fant ut at de kom fra store selskaper innen rengjøringsbransjen. Totalt var 9 millioner unndratt skatte- og avgiftsberegning. Selskapet var i arbeidsgiverregisteret registret uten arbeidstakere, mens det egentlig hadde vært 15-20 polakker som hadde arbeidet for mistenkte. Dette er bare en av flere saker om straffbare forhold i rengjøringsbransjen. Banker bør derfor vurdere sterkere kontrolltiltak ved transaksjoner til/fra personer eller virksomheter i denne næringen.

4.1.3 Hvilke områder eller land innebærer geografisk risiko?

Geografisk risiko knytter seg ikke bare til hvilket statsborgerskap eller hvilken bostedsadresse *kunden* har, men også til hvilke land *transaksjoner* kommer fra, hvor transaksjoner sendes til, hvor bedriftens kundemasse geografisk befinner seg etc. Spørsmålet blir hvilke land som må anses å innebære høy risiko for at banken utnyttes til hvitvasking.

Det finnes ingen fullstendig og uttømmende liste over land eller geografisk områder som representerer høyere risiko, men ulike faktorer kan til sammen lede til at område

[54] Stridbeck (2008) s. 50

[55] Samtale med Trude S. Eidsheim i Pareto 13.03.2012

innebærer risiko. En relevant faktor vil være at et land støtter terrororganisasjoner. Det er som nevnt i punkt 4.1 utarbeidet ulike lister av ulike internasjonale organer over slike områder, land og personer. I FATF sin Guidance to Risk-Based Approach s. 28, påpekes at land som er subjekt for sanksjoner av for eksempel FN, kan innebære høy risiko. Dersom et land ikke har tilfredsstillende hvitvaskingslovgivning eller kontrollmekanismer er dette kan indikere høy risiko. På FATF sine hjemmesider finnes lister over hvilke land dette gjelder, senest oppdater 16. februar 2012.[56] Egmont Group og the World Bank er andre kilder til slik informasjon.[57] Land identifisert med høy korrupsjon eller annen kriminalitet vil også medføre høyere risiko. Transparency International fører statistikk over områder med høy korrupsjon.[58] Innenfor EU kan det også foreligge ulike grader av risiko for hvitvasking, EU har derfor utarbeidet «Compendium Paper on the supervisory implementation practices across EU member states of the Third Money Laundering Directive 2005/60/EC».

Opererer kunden i et såkalt «skatteparadis» er det en sterk indikator på høy risiko. Eksempler på slike land kan være Cayman Island og Panama.[59] Landene gir skattemessige fordeler og hemmelighold. Midler som opprinnelig kommer fra legal virksomhet kan på denne måten skjules fra det offentlige, slik at de unndras beskatning. Siden identiteten til kunden skjules og det er lite kontroll i disse landene er det påregnelig at skatteparadiser tiltrekker seg personer som har noe å skjule, og derfor brukes som bindeledd mellom ulovlig utbytte fra kriminalitet og lovlig virksomhet.[60] Transaksjoner som går via mellomledd og over landegrenser lager i seg selv barrierer mot innsyn, men kobles de i tillegg opp mot skatteparadiser blir det enda mer komplisert å spore opp midlene. Her ser vi behovet for internasjonalt samarbeid på området. I den såkalte Transocean-saken har Økokrim etterkommet begjæring fra Skattedirektoratet og besluttet å fremme erstatningskrav på vegne av den norske stat på 1,8 milliarder. To skatterådgivere, begge partnere i to anerkjente advokatfirmaer, er tiltalt for medvirkning til grovt skattesvik. Skatteunndragelsene var i forbindelse med

[56] FATF, *Highrisk and non-cooperativ jurisdictions,* 2012

[57] FATF *Guidance on the Risk-Based Approach* s. 28

[58] Transparency international –Corruption perceptions index 2011.

[59] Financial Secrecy Index

[60] Eriksen 2009 og Økokrim: *Trendrapport økonomisk kriminalitet og miljørkiminalitet* 2008-2009 s.35

drift og salg til forskjellige selskaper på Cayman Islands. Saken er berammet til begynnelsen av desember i år og viser hvilke verdier som unndras i skatteparadiser samt hvordan profesjonalitetshjelpere kan brukes som medhjelpere til økonomisk kriminalitet og derfor kan innebære høy risiko.[61]

Statsborgerskap og bosted må oppgis til banken, jf. hvitvaskingsloven § 8 fjerde ledd. Ovenfor utenlandske kunder bør banker alltid foreta sterkere kontroll og finne ut av hvorfor de vil åpne konto i dette landet når de har bostedsadresse i et annet land.[62] I Økokrim sin rapport fra 2011 kommer det fram at mange rapporter om mistenkelige transaksjoner gjelder personer med arabisk utseende. Det uttales i FATF sin rapport om Norges gjennomføring av anbefalingene i 2005, bekymringer for systemets effektivitet pga. bankers fokus på transaksjoner foretatt av utlendinger, istedenfor å fokusere på transaksjonens art og natur i seg selv.[63] Fokus bør derfor i større grad rettes mot mistenkelig *transaksjon*, istedenfor kun mistenkelig *person*. I 2009 kom FATF ut med en follow-up rapport, som igjen påpeker dette. På tross av at kommunikasjonen mellom myndigheter og rapporteringspliktige har lagt vekt på at statsborgerskap bare er en av flere faktorer når man identifiserer risiko, viste det seg at 70% av rapportene om mistenkelige transaksjoner var basert på transaksjoner foretatt av utlendinger.[64] Mye har skjedd siden 2009, men ut fra de samtalene jeg har hatt med kundebehandlere synes det fortsatt som de er raske med å klassifisere personer med utenlandsk utseende som høyrisikokunde. Jeg tror derfor det er viktig at banker ikke lar bostedsland eller statsborgerskap være avgjørende, men at det kan være berettiget å ta med som et moment i risikovurderingen. Har kunden tilknytning til et land med høy korrupsjon, dårlig legitimasjon og uvanlig begrunnelse for overføring kan dette altså til sammen føre til at kunden antas å innebære høy risiko.

---

[61] Økokrim, nyheter (2012)

[62] FATF *Guidance to Risk-Based Approach*.

[63] FATF *Summary of the 3rd mutual evaluation report* 10. juni 2005 s. 12

[64] FATF *Mutual Evaluation Fourth Follow-Up Report* 26. februar 2009 s.57

På bakgrunn av det store antall saker i retten med tilknytning til Nigeria må det være berettiget å klassifisere Nigeria som et høyrisiko land.[65] Et eksempel er RG. 2011 s.569 hvor en nigeriansk kvinne hadde vekslet flere beløp som til sammen utgjorde 1 900 000 Euro. Spørsmål var om pengene stammet fra narkotikakriminalitet.[66] Økokrim skriver i sin årsrapport 2011 at det har blitt en nedgang i nigerianer som veksler penger, men at de nå kanskje vil foreta dette via strømenn. Jeg vil påpeke at hitvaskingstransaksjoner gjerne går via mange land, og ofte ikke kommer direkte. Dette kan gjøre det vanskelig å oppdage opprinnelseslandet.

4.1.4 Hvilke produkter og tjenester innebærer høy risiko?

Bankene må foreta en risikovurdering av alle tjenester og produkter de tilbyr og avgjøre hvilke tjenester som innebærer høy risiko for hvitvasking. De må også vurdere om deres virksomhet i seg selv og som et hele innebærer høy risiko. For eksempel vil DNB sin virksomhet, som i mye større grad enn Sparebank1 er en forretningsbank, innebærer flere kunder og filialer i utlandet og større andel av produkter med antatt høy risiko for hvitvasking. En bank med en stabil, velkjent kundebase vil innebære lavere risiko for hvitvasking, og motsatt vil en bank med stor og voksende kundemasse i et stort og adspredt geografisk område innebære høy risiko.[67] Er kundebehandlerne relativt stabile og ikke i utskiftning særlig ofte vil også dette innebære at banken kan sees på som en bank der risikoen er lav, kundebehandleren vil da lære å kjenne igjen de ulike kunder, samt følge godt opp prosedyrene for risikovurdering.[68]

Det følger blant annet av Ot.prp.nr.3(2008-2009) og fortalen til EUs tredje hvitvaskingsdirektiv at valutavirksomhet er et område som er særlig utsatt for hvitvasking. Det bør derfor klassifiseres som høyrisikoprodukt. Bakgrunnen er at saker som innebærer et stort utbytte, og derfor har behov for å hvitvaskes gjennom det finansielle systemet, ofte innebærer aktivitet som strekker seg på tvers av landegrenser.

---

[65] Økokrim: *Trendrapport hvitvasking 2011* s.23

[66] Se bl.a. LG-2011-14553, LG-2010-179947 og Rt.2004 s.598.

[67] Basel Committee on Banking Supervision- Risk Matrix, vedlagt Annex 2 i FATF sin *Guidance on the Risk-Based Approach*.s.36-37

[68] Basel Committee -Risk Matrix

Trafficking av mennesker, narkotikasmugling og korrupsjonsbetalinger er eksempler på operasjoner der flere land vil være involvert i prosessen fram til endelig utbytte. Penger veksles da til en valuta som er lett omsettelig før de fraktes ut eller inn i landet. I 2010 beslagla Tollvesenet 19 millioner norske kroner kontant i utenlandsk valuta. [69] Dette antas bare å være en liten del av det som smugles. Det vanligste er å veksle utbyttet i Euro eller US dollar da dette er lett omsettelig valuta.[70] Etter § 7 nr.4 må som nevnt banken samle inn informasjon om formål ved store vekslinger formålet kan da få innflytelse på om et produkt anses som spesielt risikofylt.

Sjekk, innskudd via automat og bankremisser er eksempler på andre produkter som av erfaring kan innebære høyere risiko for hvitvasking. Disse fremmer anonymitet, noe som i alminnelighet antas å innebære høyere risiko jf. også hvitvaskingsloven § 15 fjerde ledd. Bruk av bankboks er egnet for å skjule deler av formuen slik at skatt unndras fordi bankens ansatte har begrenset tilgang. Såkalte 31.12-uttak bør banker være oppmerksomme på, da disse gjerne foretas for å unngå formuesskatt. Bankremisser blir også brukt mer aktivt før årsskiftet da bankremisser lettere kan skjule reell kjøper.[71] Nattsafe eller innskudd via automat kan misbrukes for å unngå spørsmål fra kundebehandler i banken. Innskudd i utenlandsk valuta må allikevel foretas av kundebehandler. Egmont Group har lagt ut 100 eksempler på virkelige hvitvaskingssaker som er sendt inn av medlemslandenes FIUs[72] Sak 15 gjaldt en mann som skjulte utbytte fra straffbar handling ved å legge deler av utbyttet i nattsafe hver kveld, slik at de skulle fremstå som dagens inntjening i hans virksomhet. Utbyttet bestod av gamle hundrelapper, som var på vei ut av markedet og som han måtte få vekslet inn raskt. Problemet var at banken ble mistenksom når dagens inntjening stort sett bestod av gamle sedler. Mannen forklarte han hadde brukt nattsafe, så han slapp

[69] Økokrim: *Trendrapport hvitvasking 2011 s.22*

[70] Økokrim: *Trendrapport hvitvasking 2011 s.22*

[71] Økokrim: *Trendrapport hvitvasking 2011 s.17*

[72] The Egmont Group of Financial Intelligence Units arbeider med anti-hvitvasking og terrorfinansiering og består av ulike nasjoners Financial intelligence units(FIUs). Enheten for finansiell etterretning(EFE), del av Økokrim, er Norges nasjonale FIU. De mottar og analyserer rapporter om mistenkelige transaksjoner.

konfrontasjon og spørsmål fra kundebehandler. Bankens oppmerksomhet ledet allikevel til at han ble avslørt for hvitvasking.

Internettbaserte banktjenester er også risikoprodukter. Selv om kunden ikke er anonym, kan det være vanskelig å fastslå kundens sanne identitet. Den store økningen og utviklingen gjør området sårbart. Levetiden på produktene er ofte korte og leder til behov for stadig endringer i informasjonsteknologien til en bank. Det kan legge press på å håndtere risikoen, og medføre dårligere kvalitet på sikkerheten. Nye produkter krever derfor ekstra oppmerksomhet fra banken da det er vanskelig å forutse hvilken risiko disse kan innebære.

Ved lån kan det forekomme høyere risiko for hvitvasking. Egenkapitalen ved boligkjøp kan komme fra ulovlig utbytte, eller lånet innfris raskt etter lånopptak, og ved å vise lånebeviset fremstår utbyttet i hvert fall i en viss grad som lovlig utad. Høy verditakst, som ikke er reell, gir dårlig sikkerhet for banken og kan indikere kriminelle forhold.[73] Banken bør derfor i en viss grad ha kjennskap til boligmarkedet for lettere å oppdage slik svindel. Banker kan være fristet til å godta innfrielse av lån selv om det kan være fra ulovlig utbytte for å kunne sikre seg mot egne tap.[74] Banker bør også være oppmerksomme på lån som har pant i verdifulle gjenstander, da gjenstandene kan være utbytte fra straffbare handlinger eller kjøpt med ulovlige midler for å skjule midlenes opphav. Auksjonshus utbetaler gjerne fortjenesten ved salg med sjekk, og når sjekken løses ut er pengene «rene» og kan investeres på nytt.[75] Dette kan være vanskelig å oppdage. Ved innskudd av fortjeneste ved salg av antikviteter kan spørsmål fra oppmerksom kundebehandler være et kontrolltiltak for å avsløre slike operasjoner.

4.1.5 Hvilke transaksjoner kan innebære høy risiko?

En vanlig måte å hvitvaske penger på er å tilsløre utbyttets opprinnelse ved å sende penger via ulike konti. Pengene går frem og tilbake på ulike konti innen en viss tidsramme, eller en større sum splittes i flere mindre summer, for så å samles igjen på

[73] Jf. sak i Follo tingrett 16.03.2012. Saken har sammenheng med et stort sakskompleks om bankbedrageri som er berammet til 13. august.

[74] Økokrim: *Trendrapport hvitvasking 2011*, s.23

[75] Stridbeck (2008) s.46

samme konto ved hjelp av ulike personer, såkalt «smurfing». Det reelle formålet er å skjule midlenes opprinnelse. Vet den som utfører transaksjonen lite om formålet med transaksjonen og hvem som tilslutt skal få pengene kan dette tyde på at transaksjonen fortas for en annen noe som bør lede til nærmere undersøkelser fra banken. Som nevnt tidligere, er det i forskriftens § 12 noen situasjoner som kan utløse undersøkelses- og rapporteringsplikt som etter en konkret vurdering også kan være eksempler på situasjoner og kundeforhold som etter sin art innebærer høy risiko for hvitvasking.[76] Et eksempel forskriften nevner er «at transaksjonen synes å mangle et legitimt formål». Man må da vurdere om transaksjonen i seg selv fremstår som fornuftig eller naturlig. «Legitimt formål» vil det for eksempel ikke være dersom formålet er å unndra skatt, eller transaksjonen foretas for å skjule reelle rettighetshavere. Andre indikatorer som forskriften nevner er der en transaksjon er uvanlig stor eller kompleks, eller har grenseoverskridende karakter.[77] Banken bør undersøke om kunden har et forhold til landet transaksjonene foretas til /fra og derfor fremstår som normalkundens. Etter et konkret skjønn må banken se på den store/uvanlige transaksjonen i forhold til den kjennskap den har om kunden.. Et eksempel fra rettspraksis der transaksjonens store beløp trolig var grunnen til at den ble oppdaget har vi i Rt. 2008 s.1473. To bankremisser på henholdsvis 2,8 og 16,65 millioner kroner ble sendt via banken fra tiltaltes private konti til hans kone. Utstedelsen utløste såkalt mistenkelig transaksjon-rapport til Økokrim, som innledet etterforskning i saken. Tiltalte ble av Høyesterett dømt for grov utroskap og grov korrupsjon av over 100 millioner kroner. Her ser vi hvor store beløp det er tale om, og viktigheten av et godt system i bankene.

Konklusjonen blir at faktorene i de ulike kategoriene ovenfor kan gi et godt utgangspunkt og grunnlag for en risikovurdering. Plikten vil allikevel alltid bero på en konkret skjønnsvurdering av den enkelte bank og ut ifra den enkelte kunde. En konsekvens av at dette er at de ulike bankene vil kunne oppdage ulike typer av kunder og transaksjoner da de gjerne har ulike systemer, indikatorer og sanksjonslister de kjører kundene opp mot.

---

[76] Rundskriv 8/2009 s. 28

[77] Se også NOU 2007: 10 s.31

En forutsetning for at risikovurderingen og den løpende oppfølgingen skal virke etter sin hensikt er at banken løpende oppdaterer med aktuelle risikofaktorer. En risikovurdering som spiller på risikomomenter som var relevante for 10 år siden vil ikke finne de områdene som i dag innebærer høy risiko. Saker i rettsapparatet, som gjerne blir kjent via media, vil være en kilde, svakheten er at disse gjerne har blitt kjent for politiet gjennom MT-rapporter, som igjen har bygget på de faktorene man av erfaring vet innebærer risiko. Slik får man en «sirkel» som i stor grad bygger på faktorer kjent fra før, og ikke nye. Jeg kommer tilbake til dette i punkt 7.

4.2 Hvordan foreta risikovurdering i praksis?

Loven opp til stor fleksibilitet og gir få retningslinjer med hensyn til hvordan man kan gjennomføre risikovurdering etter § 5. Risikovurderingen innebærer et konkret skjønn fra den enkelte rapporteringspliktige og vil derfor variere fra bank til bank. En annen ting er at også selve *systemet* for gjennomføringen vil variere. Dette leder til spørsmål om hvordan plikten skal gjennomføres i praksis. Jeg har intervjuet sentrale hvitvaskingsansvarlige i banker som en kilde til å forstå hvordan gjennomføring av pliktene kan foregå og illustrere hvilken praksis som brukes. Jeg snakket med Tor Ivar Mysen i DNB 24.01.2012, Ole Jørgen Eitrå og Ole Jørgenrud snakket jeg med 25.01.2012 og Trude S. Eidsheim i Pareto bank snakket jeg med 13.03.2012.

Alle rapporteringspliktige som omfattes av hvitvaskingsloven må tilfredsstille kravene til internkontroll og prosedyrer som sikrer at pliktene etter hvitvaskingsloven blir oppfylt, jf. § 23. I større banker har man gjerne en egen «compliance-gruppe» som er ansvarlig for at hvitvaskingsloven blir overholdt. DNB startet sitt arbeid allerede i 2006 og bygget sine systemer og prosedyrer på EUs tredje hvitvaskingsdirektiv. På et tidspunkt var opptil 61 ansatte i arbeid med å klargjøre systemet for risikobasert kundekontroll. Dette viser at pliktene i hvitvaskingsloven er omfattende, og at store ressurser kreves for å oppfylle disse.

Første trinn i kundekontrollen er kundefrontsystemer i kundeetableringsfasen der kunden blir spurt om legitimasjon, navn og adresse, hva vedkommende vil med kundeforholdet og hvilke tjenester vedkommende regner med å bruke, jf. kravene til registrering etter § 8 som er omtalt ovenfor. Det som er viktig for risikovurderingen blir

skrevet inn i det elektroniske systemet og i løpet av sekunder sjekket opp mot sanksjonslister som nevnt over. Hvilke lister kunden sjekkes opp mot vil bero på hva banken føler den har behov for ut ifra en risikovurdering av deres virksomhet og kundemasse. I andre banker ble kunder kun sjekket mot listen over politisk eksponerte personer (se punkt 5.1.1).

Andre risikofaktorer vurderes gjerne ved hjelp av en risikomotor som hjelper til å vurdere kundens risikonivå. «Risikomotor» vil si et system som reagerer på visse «scenarioer» banken antar innebærer risiko for at banken brukes til hvitvasking. Banken må analysere hva som indikerer høy risiko i deres bank, når dette er klart plottes risikofaktorene inn i en «risikomotor» der hvert parameter (segment) gis en tallverdi. I Sparebank1 hadde de en risikomotor hvor det ble satt inn vekttall 1-3 i de ulike «segmentene» dvs. de ulike gruppene av forhold som kan ha betydning for hvitvasking:[78]

Figur 2

Vekttall 1	Mindre betydning i risikoberegningen
Vekttall 2	Middels betydning i risikoberegningen
Vekttall 3	Høy betydning i risikoberegningen

[78] Tabellene jeg har laget bygger på samtale med Ole Jørgen Eiterå og Einar Jørgenrud i Sparebank 1 25.01.2012.

De ulike «segmentene» og deres betydning i forhold til hvitvasking var i Sparebank1 følgende:

Figur 3

Segment	**Vekttall**
Bransje	3
Transaksjonstype	3
Kontotype	3
Motpostland for transaksjon	3
Bostedsland	3
Næringssektor	2
Statsborgerskap	1
Seks transaksjoner til utlandet i løpet av 11 måneder vil slå ut.	

Vekttallene for hvert segment legges sammen slik at vi finner kundens «risikoscore». Grenseverdien for forsterket kontrollnivå ble satt til 6. Har kunden over dette vil vedkommende med en gang bli satt i «høyrisikogruppen» med forsterket kontrollnivå. Banken må avgjøre hvilke forhold innenfor hvert segment som skal gi utslag i risikomotoren. Indikatorer som har kommet fram ved innhenting av risikofaktorer vil være relevante. Disse er behandlet ovenfor.

I Sparebank1 delte de hvert segment inn i tre ulike risikokategorier. Kundens opplysninger ved kundekontrollen ville være grunnlaget for klassifiseringen:

Figur 4

Risikokategori	**Konsekvens**
Ekstra høy risiko	Gir kunden automatisk forhøyet risiko og forsterket kontrollnivå. For eksempel kan man bestemme at alle drosjefirmaer skal ha forhøyet kontrollnivå uavhengig av andre treff i søkemotoren. Ingen beregning blir foretatt i slike tilfeller.
Høy risiko	Gir utslag i risikomotoren. Dersom kunden også får utslag på høy risiko i andre segmenter i risikoklassifisering kan det føre til forsterket kontroll dersom grenseverdien på 6 nås.
Normal risiko	Gir ikke utslag i risikoberegningen. Når det gjelder segmentet statsborgerskap, vil for eksempel det å være nordmann i Norge ikke være noe som antas å innebære høyere risiko for hvitvasking.

Eksempel på kunde som vil bli satt til forsterket kontroll er person som jobber i bygg- og anleggsbransjen, driver enkeltmannsforetak (ANS) og har bostedsadresse i annet land enn Norge. Segmentet «bransje» gis vekttall 3, bygg- og anleggsbransjen innebærer høy risiko og segmentet «virksomhet» gis vekttall 2, og ANS anses å innebære høy risiko. Bostedsadresse i utlandet gir høy risiko, og segmentet «bostedsland» gis vekttall 3 i risikomotoren. Til sammen er risikoscoren 8. Dette innebærer forsterket kontrollnivå fordi grenseverdien på 6 er nådd. «Motpostland for transaksjoner», altså det landet transaksjonen blir sendt til/fra anså Sparebank1 å ha høy betydning, med vekttall 3. Risikomotoren reagerte dersom det ble foretatt flere enn seks transaksjoner til utlandet i løpet av 11 måneder. Dette ble registrert via den elektroniske og løpende kontrollen over transaksjoner. I Sparebank1 var det kun Norge som bostedsland som var satt til standard eller normal risiko. Person bosatt i Norge, med utenlandsk statsborgerskap, kan avhengig av hvilket land det er tale om, også bli ansett å innebære høy risiko. Kundebehandler hadde i tillegg mulighet til manuelt å sette kunden opp til høyrisikonivå i skjermbildet på bakgrunn av gitte kriterier og subjektiv oppfatning basert på kundens svar og oppførsel vedrørende formål og tilsiktet art.

Kunder som krever forsterket kontrollnivå blir ennå ikke klassifisert som høyrisiko kunder av bankene, da de høye verdiene kan ha en naturlig forklaring. For eksempel vil mange betalinger til Colombia, som i første omgang kan mistenkes for narkotikahandel, kanskje kunne forklares med at man har slekt der. Høy risikoscore medfører kun at det skal foretas sterkere kundekontrolltiltak, hvor banken *deretter* bekrefter eller avkrefter om dette er en høyrisikokunde, som derfor krever sterkere løpende oppfølging. Risikovurderingen er derfor et slags «forstadium» før risikonivået for den løpende oppfølging fastsettes. Kundebehandler kan da stille noen tilleggsspørsmål, føler kundebehandleren fortsatt at kunden skal settes på forsterket kontrollnivå vil en egen sikkerhetsavdeling i banken foreta den nærmere kontrollen av kunden og avgjøre om kunden skal fortsette under forsterket kontrollnivå som høyrisikokunde eller settes til normalt kontrollnivå. Detter er også en grunn til at risikovurderingen kun anses å være midlertidig.[79] Dersom denne avdelingen etter undersøkelser ennå ikke har fått en naturlig forklaring på høy risikoscore må en leder på relativt høyt nivå beslutte om personen skal tas som kunde.[80] Ved at kundens «profil» overprøves på denne måten blir sikkerheten høyere. Over tid kan kundeforholdet utvikle seg, noe som i den løpende oppfølgingen kan lede til at kontrollnivå på kunden endres.

DnB og Pareto bank var ikke villige til å angi hvilken vekt de ulike segmentene hadde, da de ble spurt. DNB ville heller ikke oppgi hva de anså som risikofaktorer. Begrunnelsen var at informasjonen var taushetsbelagt. Jeg antar at årsaken var å sikre at systemet ikke ble omgått eller utnyttet av hvitvaskere. Forarbeider og de ulike internasjonale anbefalinger gir imidlertid mange pekepinner på hva og når man bør foreta forsterket kontroll og jeg antar at DNB sine vurderinger ikke ligger langt fra disse.

4.2.1 Risikobasert kundekontroll gjennom elektroniske systemer

Finansinstitusjoner plikter å etablere elektroniske overvåkningssystemer, jf. hvitvaskingsloven § 24 og hvitvaskingsforskriften § 18. Kravet er en videreføring av

[79] Återgärder mot penningtvätt m.m. (2010) s.146

[80] Etter hvitvaskingsloven § 23(2) skal det utpekes en person i ledelsen som har et særskilt ansvar for å følge opp rutinene.

tidligere hvitvaskingslov § 15. Som redegjørelsen ovenfor viser, foregår nå også selve risikovurderingen ved hjelp av elektroniske systemer. Tilsyn Finanstilsynet foretok i mars 2009 viser at alle institusjoner i deres utvalg ved fastsettelse av interne rutiner, jf. hvitvaskingsloven § 23, hadde valgt å risikoklassifisere nye kunder gjennom implementering av systemløsninger som ivaretar klassifisering og verifisering av kunden.

Firmaer som EVRY, tidligere kalt EDB, tilbyr systemløsninger til banker slik at lovens krav til elektroniske systemer tilfredsstilles.[81] Det er viktig å presisere at plikten til å ha en tilfredsstillende risikobasert kundekontroll alltid vil ligge hos banken. Den kan altså ikke kjøpe seg fra ansvar via elektroniske løsninger og systemer.

4.2.2 Manuell eller elektronisk?

Systemet i DNB fremkom som noe mer automatisert enn systemet i Sparebank1 og Pareto bank. Dette kan begrunnes i deres store kundemasse og pengene de har investert i ulike elektroniske systemer. Sparebank1 opplyste at også de etter hvert ville få på plass mer automatisert kundekontroll enn det de nå hadde. Spørsmålet blir da om elektronisk eller manuell risikobasert kundekontroll oppfyller lovens krav best.

Ved etablering av kundeforhold ved oppmøte i banken, vil kundebehandlerens fysiske observasjon av kundens oppførsel og holdning på den ene siden kunne bidra med viktige skjønnsmessige momenter i risikovurderingen. Dette krever bevissthet og erfaring fra kundebehandler om hva som er en «normal» kunde slik at atypiske situasjoner oppdages, og vil kunne registrere faktorer et elektronisk system aldri vil fange opp.

På den andre siden vil et slikt system være sårbart, og selv om banken ser det, kan det være lett å vende det blinde øyet til. Én utro kundebehandler vil ha stor innflytelse og kan bidra til store huller i en kundes kundeprofil som gjør at den reelle risikoen for hvitvasking ikke registreres og systemet ikke fanger opp de situasjoner det skal. Bankpersonell kan for eksempel bli truet eller bestukket til å registrere falskt navn og

[81] IT-selskapene EDB og Ergo Group ble fusjonert sammen og byttet navn til EVRY 17. mars 2012.

andre opplysninger om en kunde.[82] En forutsetning for at den risikobaserte kundekontrollen skal virke etter sin hensikt er at man kan stole på at registrerte opplysninger stemmer og har blitt registrert slik loven foreskriver.

Egmont Group sak 88 kan illustrere hvordan bankansatte kan brukes som medhjelpere i hvitvaskingsnettverk.[83] En kvinne skulle skjule penger fra en kriminell operasjon. Pengene ble fraktet i kontanter til nabolandet. De ble klarert i tollen via en utro bankansatt som sørget for at tolldokumenter var på plass. Pengene ble så satt inn på en konto og sendt til Sør- Amerika. Banken oppdaget et større antall kontantinnskudd på samme beløp som raskt ble transferert videre til Sør-Amerika. Banken fant ut, via tolldokumentene, at en av sine bankansatte var involvert i alle transaksjoner. Dette var starten på politiets undersøkelser av en person som det viste seg hadde hvitvasket over 14 700 000 US dollar. Bankens fokus på rekruttering av egnede, ærlige personer er viktig. Viktigere er det at etiske retningslinjer blir fulgt opp og at internkontrollen i banken er god.[84] Etter hvitvaskingsloven § 23 annet ledd, fastsettes en plikt for rapporteringspliktige til å ha en person i ledelsen som har ansvar for at rutiner følges opp. Dette begrenser handlingsrommet for en utro kundebehandler. Hvis alle i banken følger opp sitt kontrollansvar skal det mer til for at enkeltpersoner kan gjennomføre disposisjoner alene og uten medhjelpere.[85]

En annen svakhet ved en risikovurdering som bygger på kundebehandlers observasjoner og subjektive oppfatning er at det kan lede til diskriminering av kunder. Som nevnt, i punkt 4.1.3, gjaldt FATA sin kritikk av Norge fokuset på mistenkelig person, i stedet for mistenkelig transaksjon. Videre har Økokrim laget en liste med indikatorer på hvitvasking som legger opp til subjektivt skjønn fra den enkelte kundebehandler i banken.[86] En kundebehandler jeg snakket med i en bank sa hun ikke ville etablere kundeforhold dersom hun ikke følte seg trygg på de opplysninger kunden gav. Hennes subjektive oppfatning av kunden og erfaring vil spille inn i denne vurderingen.

---

[82] Stridbeck (2008) s.55

[83] Se fotnote 72 s.31 for nærmere informasjon om Egmont Group.

[84] Gottschalk (2010) s. 210

[85] Olsen 2007 s. 199

[86] Økokrim, Indikatorer på hvitvasking, (2010)

Kundebehandleren hadde sett et TV-program om forfalskning av pass for folk fra østblokkland, hun var derfor spesielt skeptisk til disse. Dersom subjektive vurderinger blir tillagt for stor vekt, kan det innebære en svakhet ved risikovurderingen, men som nevnt over kan det også være berettigede skjønnsmessig vurdering som bidrar til en god risikovurdering, og ikke nødvendigvis et utslag av fremmedfrykt.

En elektronisk kundevurdering gjør at vi kan etablere kundeforhold via bankens nettside. Kunden slipper da å møte i banken, og risikovurderingen skjer på grunnlag av på forhånd utvalgte kriterier. Slik unngår man risikoen for utro tjenere og diskriminering, men innslaget av skjønn mistes. At dette antas å innebære høyere risiko, og kanskje fare for falsk identitet ser vi i hvitvaskingsloven § 7 fjerde ledd, som krever ytterligere legitimasjon for å «kompensere for den forsterkede risikoen unnatt personlig fremmøte innebærer.»[87] Visse risikofaktor vil nesten alltid bli sjekket elektronisk. Slik som sjekk av kunden opp mot sanksjonslister og om kunden er politisk eksponert person, se neste punkt. Dette er mest praktisk, og sikrere enn å stole kun på kundens egne opplysninger. Bankene pekte på at det ved treff, allikevel vil være behov for manuelt å sjekke om kunden virkelig er personen på listen.

Som drøftelsen ovenfor viser vil både elektronisk og manuell risikovurdering ha sine fordeler. Elektroniske systemer har sin styrke i lik vurdering av alle ut fra gitte kriterier, mens en manuell kontroll kan bidra med skjønnsmessige momenter et elektronisk system aldri vil registrere. Etter dette ser det ut til at en kombinasjon av manuell og elektronisk risikovurdering, der momenter fra begge vurderes sammen vil være det beste alternativet. I praksis er det også dette som er det vanlige.

5 Hvordan tilpasse kundekontrolltiltakene til den enkelte risiko?

Dersom en kunde etter risikovurderingen antas å innebære høy risiko, må kontrolltiltakene tilpasses deretter. Loven setter i slike tilfeller krav om forsterkede og andre kontrolltiltak i tillegg til de alminnelige, jf. § 15. Innebærer en kunde lav risiko,

[87] Ot.prp.nr.3 (2008-2009) s.24, se også s. 45

foretas forenklet kundekontroll. Det er et unntak fra hovedregelen om alminnelige kontrolltiltak. Slik gjøres kundekontrollen «risikobasert». Fordi den forenklede kundekontrollen er en konsekvens av en risikobasert tilpasning mener jeg det passer å behandle kontrolltiltaket her, selv om det i tid riktignok ikke skjer etter den alminnelige kundekontroll, slik fremstillingen kan gi inntrykk av, men istedenfor.

5.1 Forsterkede kontrolltiltak

- Kundekontrolltiltak for situasjoner med antatt høy risiko

Hvitvaskingsloven § 15 første ledd fastsetter en *generell plikt* til å anvende forsterkede kontrolltiltak i situasjoner som innebærer høy risiko. Regelen er ny i forhold til tidligere hvitvaskingslov. Den gjennomfører tredje hvitvaskingsdirektiv art. 13 og art. 3(1) nr.8.

«Forsterkede kontrolltiltak» vil si andre og skjerpede kontrolltiltak i tillegg til de som følger av hvitvaskingsloven §§5-14, jf. § 15. Disse skal anvendes i situasjoner som «etter sin art» innebærer høy risiko for hvitvasking. Bestemmelsen har et visst motstykke i FATF-anbefaling 5(4) hvor det står at institusjonen skal iverksette forsterkede kontrolltiltak overfor «higher risk categories». De opplysninger som er innhentet ved den alminnelige kundekontroll vil inngå i bankens vurdering av om det er tale om en slik kunde. Hvilke kundeforhold som «etter sin art» innebærer høy risiko er et svært lite konkret kriterium og loven inneholder ingen legaldefinisjon av høyrisikosituasjoner. Identifisering av mulige høyrisikosituasjoner ble behandlet i punkt 4.1. og er en meget viktig del av den risikobaserte tilnærmingen, de samme momenter der vil være aktuelle ved vurderingen her.[88] Lovverket inneholder heller ingen konkrete eksempler på forsterkede eller andre kontrolltiltak som skal benyttes (med unntak for PEPs og korrespondentbankforbindelser). Banken må derfor etter en konkret risikovurdering bestemme hvilke andre kontrolltiltak som i tillegg vil være nødvendig, samt omfanget av disse. Skjerpet elektronisk kontroll og manuell oppfølging av kundeforholdet og transaksjoner vil være relevant.[89] Der hele kundemassen eller virksomheten antas å innebære høy risiko, bør rutinen rundt den grunnleggende kundekontrollen ta høyde for dette og muligens ha forsterket kontroll

[88] Ot.prp.nr.3 (2008-2009) s.90

[89] Rundskriv 8/2009

som hovedregel for alle kunder.[90] Et tiltak kan være at banken ber kunden fylle ut et skjema med mer utfyllende opplysninger om kundeforholdet. I Pareto bank ble kunder med høy risiko bedt om å fylle ut et skjema med mer utfyllende opplysninger om kundeforholdet. Bedriftskunder ble spurt om å spesifisere selskapsstruktur, eierandeler og land dersom selskapet var en enhet i et konsern med internasjonal. Videre ble det innhentet opplysninger om omsetning, hvilke land de har bankforbindelser, samt underskrift på at de vil gi beskjed hvis opplysningene endres.[91] Personkunder ble spurt om informasjon om samboer/ektefelle/partner, barn, utenlandsforhold, bankforbindelser i utlandet, eierinteresser utenfor Norge, forventet inntekt samt spesifisering av disse opplysninger.

I visse tilfeller har loven på forhånd utpekt kundeforhold som anses som særlig risikofylte og derfor automatisk blir satt til forsterket kontrollnivå. Hvitvaskingsloven § 15 annet ledd kan man derfor si er en presisering av hva som innebærer høy risiko. Loven fastsetter også minimumskrav til kontrolltiltak som skal anvendes ovenfor disse, jf. §§ 15 og 16. Dette behandlers under.

5.2 Politisk eksponerte personer (PEPs)

Ovenfor Politisk eksponerte personer, såkalte PEPs, fra annen stat enn Norge, skal ikke banken foreta noen vurdering av om høy risiko foreligger, loven presumerer at disse *alltid* vil være en høyrisikogruppe som det *alltid* skal iverksettes forsterkede kontrolltiltak ovenfor. Prinsippet om risikobasert tilnærming gjelder bare for fremgangsmåter for å fastslå om kunden er PEP. Etter § 15, vil politisk eksponert person bety fysisk person som:

> *«1. innehar eller i løpet av det siste året har innehatt høytstående offentlig verv eller stillingen 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»*

Hvitvaskingsforskriften § 11 lister nærmere opp hvilke situasjoner som innebærer at en person anses å være PEP, for eksempel medlemmer av regjering, nasjonalforsamling

[90] Återgärder mot penningtvätt m.m (2010) s. 103

[91] Samtale med Trude S. Eidsheim i Pareto bank 13.03.2012

eller Høyesterett i annen stat enn Norge. Personer med høytstående verv i Norge anses altså ikke som PEPs i Norge, men vil bli omfattet i andre stater med tilsvarende regler. Begrunnelsen for at det ovenfor PEPs skal foretas forsterket kundekontroll er at de innebærer høy risiko for hvitvasking av korrupsjonspenger.

Kundekontrollen skal identifisere opprinnelsen til kundens formue og den kapital som inngår i kundeforholdet eller transaksjonen, jf. § 15 annet ledd nr. 2. Loven krever rutiner for å oppdage PEPs, men sier ikke hvordan.[92] Forarbeidene antar at den mest praktiske tilnærming trolig vil være å kjøpe/ abonnere på internettjenester med oppdaterte lister over PEPs.[93] I praksis kjøres kunden opp mot disse ved etablering av kundeforhold og senere under den løpende oppfølgingen. Hvitvaskingsansvarlige i bankene jeg hadde samtale med mente listene var dårlig oppdaterte og upålitelige. Som tidligere nevnt, er derfor praksis at det også foretas manuell kontroll av om kunden var den samme som på listen, eller kun en person med samme navn. Ved kundeetablering blir i praksis kunden derfor spurt om å fylle ut et skjema hvor det skal oppgis om vedkommende er omfattet av de personer loven nevner i lovens § 15, jf. hvitvaskingsforskriften § 11. Kundebehandler må innhente samtykke fra overordnet før etablering av kundeforhold med PEP, jf. § 15 annet ledd nr. 1.

Som tidligere nevnt, kom FATF 16. februar 2012 ut med sine reviderte anbefalinger. Formålet er å styrke de tidligere standarder. Særlig i relasjon til de økende internasjonale bekymringer knyttet til korrupsjon, er det foretatt endringer i forhold til PEPs. Anbefalingene utvides nå til også å omfatte PEPs fra rapporteringspliktiges hjemland (domestic PEPs). Etter FATF sin anbefaling nr. 12 plikter banker å foreta rimelige tiltak for finne ut om en kunde er en PEP fra hjemlandet(domestic PEP) eller en person som har blitt betrodd denne funksjonen av en internasjonal organisasjon. Ved situasjoner som innebærer høy risiko skal det i forhold til domestic PEPs benyttes de samme forsterkede kontrolltiltak som kreves for utenlandske PEPs (undersøkelse av formuens opprinnelse, forsterket løpende oppfølging og samtykke fra overordnet). En styrking av anbefalingene på dette punktet var noe jeg så behovet for, og forventet at

[92] Återgärder mot penningtvätt m.m. (2010) s. 186

[93] Ot.prp.nr.3(2008-2009) s.94

kom. Korrupte politikere har behov for å bruke finanssystemet også i sitt hjemland. Når de nå må gi inngående opplysninger om formuens opphav m.m. og bankansatte plikter å være oppmerksomme på sammenhengen mellom inntjeningsevnen og formuen, vil dette være forhold som vanskeliggjør bruken av korrupsjonspenger. Jeg ser dette som et positivt tiltak i anti -hvitvaskingsarbeidet.

5.2.1 Korrespondentbankforbindelser, § 16.

På side 90 i Ot.prp.nr.3 (2008-2009) beskrives korrespondentbank som: *«… bank som en norsk kredittinstitusjon (respondentbanken) har inngått samarbeidsavtale med i den hensikt å utføre betalingsoppdrag for sine kunder.»* Etter § 16 pålegges banken visse plikter ved korrespondentbankforbindelser med institusjoner fra stater utenfor EØS. Banken må innhente informasjon slik at den fullt ut forstår arten av virksomheten, kan fastslå institusjonens omdømme og tilsynets kvalitet. Banken må også vurdere korrespondentinstitusjonens kontrolltiltak for forebyggelse og bekjempelse av hvitvasking. Som tidligere nevnt oppdaterer FATF på sin hjemmeside hvilke stater som har implementert deres anbefalinger. [94] Befinner banken seg i et av disse landene kan det bety at den ikke har tilfredsstillende tilsynsordninger. Videre setter hvitvaskingsloven i § 16 annet ledd forbud mot å inngå korrespondentbankforbindelse med «tomme bankselskaper». Etter tredje ledd skal tomme bankselskaper forstås som kredittinstitusjon som er opprettet i en stat der institusjonen ikke er fysisk til sted med reell ledelse og administrasjon, og som ikke er tilknyttet et regulert finanskonsern.

5.2.2 Anonymitet

Etterhvitvaskingsloven § 15 fjerde ledd, som gjennomfører hvitvaskingsdirektivet art. 13 nr. 6 skal transaksjoner og produkter som fremmer anonymitet vies særlig oppmerksomhet. Bestemmelsen er langt på vei en presisering av regelen om forsterkede kontrolltiltak, da anonymitet i alminnelighet antas å representere høy risiko.[95]

5.2.3 Fysiske personer som ikke møter personlig

Kravet om personlig frammøte ved identitetskontrollen etter tidligere hvitvaskingslov er erstattet av krav om «ytterligere dokumentasjon». Som nevnt tidligere, skal dette

---

[94] FATF, *High risk and non-cooperative jurisdictions* 2012

[95] Ot.prp.nr.3 (2008-2009) s. 93

kompensere for den forsterkede risikoen som unnlatt personlig fremmøte innebærer, jf. § 7 fjerde ledd.[96] Nærmere regler følger av hvitvaskingsforskriften § 5 tredje ledd, der et av tiltakene er kopi av kundens legitimasjon eller bekreftelse via elektronisk legitimasjon, for eksempel bank-ID.

5.3 Når kan det foretas forenklet kundekontroll?

Hvitvaskingsforskriften § 10 fastsetter et unntak fra vesentlige deler av plikten til å foreta kundekontroll. Dette vil være for kundeforhold og nærmere angitte produkter lovgiver på forhånd har vurdert vil innebære lav risiko. Kravet til kundekontroll kan derfor senkes. Listen i § 10 er uttømmende. Selv om disse forhold på forhånd er vurdert som lav risiko, må vi i det enkelte tilfellet vurdere *når og om* slike forhold foreligger. Unntaket fra normal kundekontroll gjelder i utgangspunktet kap. 2, herunder § 7 selv om lov eller forskrift ikke viser til denne er det § 7 som beskriver hva kundekontrollen etter § 6 skal omfatte og derfor kontrollpliktene i § 7 det gjøres unntak fra.[97] Forenklet kundekontroll vil gjelde for de som i praksis ikke kan opptre under falsk identitet som for eksempel børsnoterte selskaper, finansinstitusjoner eller verdipapirforetak, jf. hvitvaskingsforskriften § 10 første ledd nr. 1. Som nevnt tidligere i oppgaven gjelder unntaket ikke ved mistanke om at en transaksjon har tilknytning til hvitvasking etter hvitvaskingsloven § 6 nr. 3, da må de normale kontrolltiltak allikevel gjennomføres, jf hvitvaskingsloven § 13. Unntaket gjelder ikke for den løpende oppfølging.[98] Dette kommer jeg tilbake til under punkt 6.

Etter hvitvaskingsloven § 13 må tilstrekkelig opplysninger innhentes for å fastslå om forholdet dekkes av den aktuelle unntaksbestemmelse. Banken må med andre ord være sikker på at vilkårene i forskriftens § 10 er oppfylt *før* den unnlater å foreta kundekontroll. Ved opprettelse av konto gjelder ikke unntak fra registrering av opplysninger som navn, fødselsnummer, organisasjonsnummer og adresse etter § 8 første til tredje punkt. jf. § 13 annet ledd. Finanstilsynet antar imidlertid at det antagelig også vil være i bankens egeninteresse å registrere slike opplysninger. Også EU-

[96] Regelen bygger på EUs tredje hvitvaskingsdirektiv art. 13 nr. 2

[97] Rundskriv 8/2009 s. 25

[98] NOU:2007:10 på side 50, se mer under «løpende oppfølging»

kommisjonen har tolket loven slik at forenklet kundekontroll ikke betyr helt unnlatelse av kundekontroll.[99] I tilfeller hvor banken har andre rapporteringspliktige som kunder, og handler på vegne av disse, legger Finanstilsynet til grunn at forenklet kundekontroll kan praktiseres, men det forutsettes da at disse er underlagt EU-direktivet eller FATFs anbefalinger. I forhold til utenlandske finansinstitusjoner bør man inkludere i vurderingen om de står på FATF sin liste over land som ikke har tilfredsstillende hvitvaskingsregelverk.[100] Etter min mening kan det være lurt å huske at implementering av regler og kontrollmekanismer ikke er det samme som at reglene følges opp i praksis. Stor utbredelse av korrupsjon i et land bidrar til at transaksjoner med tilknytning til hvitvasking ikke blir fanget opp selv om reglene og kontrollmekanismene skulle tilsi det. At finansinstitusjonen er fra et land som ikke står på FATF sin liste bør derfor ikke automatisk gi grunnlag for forenklet kundekontroll, men være et moment i en risikobasert vurdering.

Redegjørelsen over viser at det må vurderes konkret når vilkårene for forenklet kundekontroll er oppfylt. Om vilkårene fortsatt foreligger må undersøkes under den løpende oppfølgingen.

Som nevnt i punkt 3.2, finner vi også et unntak fra den normale kundekontrollen i § 7 femte ledd. Det gis unntak fra krav til gyldig legitimasjon der kundebehandleren er helt sikker på hvem kunden er fordi det er en person kundebehandleren har personlig kjennskap til. I praksis vil dette være sjelden, og bestemmelsen hjemler heller ikke omfattende unntak fra den alminnelige lovpålagte kundekontrollen.

---

[99] Runskriv 8/2009 s.26 som viser til Referat fra EU-kommisjonen 15.januar 2007 fra «First transposition workshop», 16.november 2006.

[100] Rundskriv s. 26 og FATF *High- risk and non-cooperativ jurisdictions, 2012*

6 Løpende oppfølging

Kundekontroll skal ikke bare anvendes på nye kunder, men også på passende tidspunkter for eksisterende kunder, på grunnlag av en risikovurdering, jf. § 5, jf. § 14.[101] Denne plikten kalles løpende oppfølging («ongoing monitoring») og følger av hvitvaskingsloven § 14. Den er en viktig del av prinsippet kjenn-din-kunde. Spørsmålet blir hvordan banken kan oppfylle denne plikten.

Bankens plikt til å følge opp eksisterende kundeforhold innebærer at de må undersøke om de transaksjoner kunden foretar er i samsvar med bankens kjennskap til kunden og det som er registret i kundens virksomhet og risikoprofil, jf. § 14. Profilen vil være laget på grunnlag av opplysninger hentet inn ved de andre kontrolltiltakene. Særlig antar jeg opplysninger om kundeforholdets formål og tilsiktede art, jf. § 7 nr. 4, vil gi et viktig grunnlag for løpende oppfølging da dette gir informasjon som vil være spesifikt for hva kunden normalt foretar seg. Oppdages avvik må det ut fra en konkret risikovurdering foretas nærmere kontroll. Det kan lede til at transaksjonen fremstår som lovlig, eller det leder til at kundeprofilen må endres til nivået høy risiko slik at kunden fremover er under sterkere oppsyn. Det kan også føre til at en person ikke lenger anses å innebære høy risiko. Videre kan den løpende oppfølging føre til at undersøkelsesplikten om mistenkelige transaksjoner oppstår, jf. § 17. Det er en klar sammenheng mellom undersøkelsesplikten for mistenkelige transaksjoner og løpende oppfølging, forskjell kan være at løpende oppfølging tar mer sikte på avvik fra kunden, men undersøkelsen mer fokusere på transaksjoner som ut fra kjente hvitvaskingsscenarioer kan innebære risiko.[102] Risikovurderingen kan ikke føre til at løpende oppfølging helt utelates. Som nevnt vil også kunder som omfattes av forenklet kundekontroll være underlagt løpende oppfølging. Begrunnelsen er at løpende oppfølging er et svært viktig virkemiddel for å kunne avdekke mistenkelige transaksjoner, samt rapporteringspliktiges behov for mulighet til å vurdere om kunden fortsetter å kvalifisere for unntak. At en kunde er omfattet av unntaksreglene vil imidlertid tilsi lav risiko, og kan være et moment i risikovurderingen som ligger til grunn for løpende oppfølging.[103] For kunder som

[101] Ot.prp.nr.3(2008-2009) s.87

[102] Återgärder mot penningtvätt m.m (2010) s. 168

[103] NOU 2007:10 s.50

omfattes av forsterkede kontrolltiltak, skal også den løpende oppfølgingen være forsterket, dette følger av hvitvaskingsloven § 5 som lovfester at løpende oppfølging skal være risikobasert.

Inntreden av plikten for de andre kontrolltiltak knyttes til konkrete skjæringspunkter, har kort varighet og utføres for å oppnå konkret informasjon. Dette gjelder ikke for løpende oppfølging, og er noe av grunnen til at den er skilt ut som en egen plikt.[104] Tiltaket må sees i sammenheng med § 6 første ledd nr. 4 om plikt til å foreta kundekontroll ved tvil om innhentede opplysninger om kunden er korrekte eller tilstrekkelige. Sees § 6 første ledd nr. 4 i sammenheng med § 14 ble det etter forarbeidene unødvendig å presisere at kontrollen må foretas på passende tidspunkt på grunnlag av en risikovurdering.[105]

I motsetning til andre rapporteringspliktige, vil banker ofte ha mulighet til å se mønster hos kunden over tid. Sammenligningsvis vil et vekslingskontor kun se kunden i 30 sekunder før det er neste kunde igjen. Banker er derfor spesielt viktige når det gjelder å oppdage uvanlige transaksjonsmønstre og avvik.

For kundeforhold som banken hadde før kravet til identitetskontroll kom i 1994, skal løpende oppfølging foretas dersom det ut ifra en konkret risikovurdering anses påkrevd.[106] For å oppnå lovens formål vil det være like viktig å ta hensyn til opplysninger om nye kundeforhol, som for eldre. En risikobasert tilnærming til plikten vil imidlertid begrense pliktens omfang ovenfor eldre, passiv kundeforhold.[107]

Som nevnt over, er banker pålagt plikt til elektronisk overvåkning etter hvitvaskingsloven § 24. I Pareto ble transaksjonsovervåkning foretatt hver natt via elektroniske overvåkningssystemer som fanger opp pengestrømmer og betalingsmønster på grunnlag av ulike indikatorer som er lagt inn i systemet på bakgrunn av en

[104] Ot.prp.nr.3 (2008-2009) s. 87

[105] Ot.prp.nr.3 (2008-2009) s. 87

[106] Ot.prp.nr.3 (2008-2009) s. 88

[107] Ot.prp.nr.3 (2008-2009) s. 88

risikovurdering som nevnt ovenfor.[108] Det elektroniske systemet er altså et slags filter hvor banken manuelt velger hvilke forhold som skal lede til at en transaksjon flagges ut. Denne manuelle tilpasning av de elektroniske systemer er viktig og bidrar til at plikten gjennomføres risikobasert i forhold til den enkelte bank. Andre registrerte opplysninger som for eksempel eierforhold, sjekkes gjerne kvartalsvis, hvert år, eller annet hvert år, avhengig av kundens risikokategori. Dette kan foretas elektronisk og/eller manuelt. I Pareto hadde de en «sjekkliste» for løpende oppfølging av kunder på forsterket kontrollnivå. Det skulle undersøkes om kunden fortsatt var PEP eller NUF og fortsatt skulle ha forsterket kontrollnivå, nye produkter, endring i formålet eller nye transaksjonsmønster, endring i styre og ledelse, adresse, disponenter, samt subjektiv vurdering. Løpende oppfølging foretas med forskjellig intensitet ovenfor de ulike risikogrupper. I Sparebank1 og DNB ble kunder med normal risiko «sluset» gjennom risikomotoren annet hvert år. Sparebank1 hadde månedlig vask av kunderegisteret mot terrorlister, årlig oppdateringsvask mot PEP-listen og kontinuerlig transaksjonsovervåkning.[109] Kvartalsvis var det oppdatering av kundens kontrollnivå. For kunder som innebar høy risiko ble det foretatt «vask» minst én gang i året. For kontoer som ikke har vært i bruk på over 40 år, vil det normalt ikke være nødvendig med en slik løpende oppfølging hvert år. Men dersom kontoen plutselig tas i bruk bør det undersøkes, da dette kan indikere hvitvasking. Banken kan da sette inn et filter, som flagger ut transaksjoner fra konto som ikke har vært i bruk for eksempel de fem siste år. Det bør i slike tilfeller foretas blant annet ny legitimasjonskontroll, da man etter så mange år ikke vil være sikre på om registrerte opplysninger stemmer, jf. også § 6 første ledd nr. 4 som stiller krav om å foreta kundekontroll ved tvil om innhentede opplysninger stemmer.

6.1 Manuell eller elektronisk løpende oppfølging?

Spørsmålet blir om plikten til å foreta løpende oppfølging best kan ivaretas ved elektronisk eller manuell løpende oppfølging.

[108] Samtale med Trude S. Eidsheim i Pareto bank 13.03.2012

[109] Samtale med Ole Jørgen Eitrå i Sparebank1, 25.01.2012

På nettsiden bankID.no kan man se at gjennomsnittlig antall transaksjoner med bankID en vanlig formiddag er ca 20 pr. sekund. Når man i tillegg tar med transaksjoner utført uten bankID blir dette et enormt antall transaksjoner pr. døgn. Løpende overvåkning av transaksjoner foretas som en følge av det store antall transaksjoner først og fremst elektronisk, dette er som nevnt også et krav ett hvitvaskingsloven § 24.Banken bestemmer selv hvilke kriterier transaksjoner skal oppfylle for å fanges opp av filtrene. Et slikt kontrollsystem vil også fange inn kunder som foretar helt lovlige transaksjoner uten tilknytning til noe lovbrudd. Et eksempel kan være at man kjøper en leilighet man pusser opp og selger før man flytter inn, plutselig vil man da få en stor sum penger på konto, noe som i et slikt tilfelle jo vil ha en helt naturlig forklaring. Transaksjoner som «flagges ut» fordi systemene identifisere de som mistenkelige, atypiske eller unormale må derfor etter en konkret vurdering også undersøkes manuelt av banken. Dette legger også Finanstilsynet opp til i sitt rundskriv på s. 21.

I Pareto bank, som bare har en kundemasse på ca. 7000 kunder hadde de kapasitet til å foreta en relativt manuell oppfølging av kundeforholdet, men elektronisk sjekk inngikk også. Det ble ansett å være mest økonomisk lønnsomt, da systemer for risikovurderinger gjerne er dyre. Det ble også sett på som det sikreste alternativet, da de mente elektroniske systemer ennå ikke var godt nok utviklet til å oppdage endringer i opplysninger om formål og tilsiktet art, samt endring i eierforhold. I Pareto bank fikk hver kundebehandler ansvar for et visst antall kunder, og én gang i året måtte de gå igjennom kundens opplysninger og registrere om det var foretatt noen endringer i disse. På grunn av den store kundemassen i DNB ble en slik manuell løpende oppfølging svært krevende. Det elektroniske systemet var derfor mer tilfredsstillende. Dette betyr ikke dermed at den løpende oppfølgingen i DNB var dårligere. Behovet for sterkere kontroll var i følge banken større i Pareto bank. Som relativt nyoppstartet bank måtte de ofte ta imot kunder som hadde fått nei til for eksempel finansiering i andre banker. Flere av kundene opererte i næringer som var utsatt for hvitvasking, noe som ifølge Pareto bank medførte behov for mer kontakt og manuell oppfølging avkunden for å oppfylle lovens plikter.

Stig Hallgeir Øksnes kunne fortelle meg at det EVRY leverte elektroniske systemer til de fleste banker i Norge, men de største bankene hadde egne, mer sofistikerte systemer.

Disse var dyrere, og i Norge hvor vi har mange små banker som ikke har like stor økonomisk disposisjonsevne var det også behov for et noe enklere elektronisk system. Begge vil oppfylle lovens krav, men enklere system tilsier krav om mer manuell oppfølging.

Redegjørelsen ovenfor viser at elektroniske systemer kun er et hjelpemiddel som gir god og helt nødvendig hjelp, men fordi det aldri kan lages en fasit på hva som er hvitvasking, kan vi heller aldri lage et elektronisk system som fanger opp alt. Transaksjoner som ser ut som hvitvasking kan jo være fullt lovlige. Vi er avhengig av en konkret manuell oppfølging og kompetanse fra banken. Konklusjonen blir derfor at løpende oppfølging etter § 14, jf. §5, best oppfylles ved bruk av både elektronisk og manuell kontroll.

7 Hvilke situasjoner fanges ikke opp av systemet?

Hvilke huller eller hindringer er knyttet til den risikobaserte kundekontrollen og løpende oppfølgingen? I hvem sin interesse er det at det foretas en god risikobasert kundekontroll og løpende oppfølging av kunden?

Det vil alltid finnes måter for hvitvaskeren å utnytte det finansielle systemet. Dette er en konsekvens av at nye produkter stadig utvikles, og dermed også nye hvitvaskingsmetoder. Som nevnt ovenfor, er det er også en konsekvens av hensynet til personvern som setter restriksjoner på mengden kontrolltiltak og opplysninger som kan kreves, jf. EMK art. 8 som beskytter retten til privatliv. Bankene påpekte at en svakhet ved systemet var at de ikke så «hele bildet» av kunden. Den manglende kontroll de hadde med tjenestene og produktene kunden brukte i andre banker og/ eller andre deler av finanskonsernet gjorde at de ikke fikk foretatt en reell risikovurdering. Operasjoner som til sammen kan indikere hvitvasking, men som hos den enkelte bank fremstår som normalt ville bli oppdaget ved utveksling av informasjon til risikovurderingen. En person som har fem bankkontoer og setter inn småbeløp som blir sendt til Afghanistan vil derfor vanskeligere bli mistenkt for terrorfinansiering da beløpene lett kan forklares

som gaver til familien. Hadde man sett alle transaksjonene denne personen foretok i sammenheng, ville beløpet kanskje blitt så stort at det vanskelig kunne forklares som vanlig underhold til familien. I høringsuttalelser ble dette påpekt av finansnæringen. I forarbeidene kom man allikevel fram til at hensynet til personvern i denne omgang måtte tillegges større vekt enn hensynet til yterligere effektiv risikovurderingen i kundekontrollen og kostnadsbegrensning innen konserner.[110] I Rundskrivet på s. 39 tillates kun utveksling av nøytrale opplysninger mellom foretak i finanskonsern.

Bankene jeg snakket med ville ikke si stort mer om svakheter, vanskeligheter eller huller de møtte ved den risikobaserte kundekontrollen. De brukte sikkerhet som begrunnelse. Svake punkter må ikke bli kjent slik at hvitvaskeren omgår systemet. Jeg tror vi heller ikke må glemme selv om banker ikke ønsker å bli utnyttet til hvitvasking, så er de profittmotiverte virksomheter som gjerne har større interesse av å tjene penger. Rapporteringspliktige er som regel ikke interessert i flere plikter. Avsnittet over viser dette. Finansnæringen så det som en svakhet at risikovurderingen ikke kunne sentraliseres for selskaper i et finanskonsern, en annen, viktigere grunn vil jeg allikevel anta, var at dette ville være mer kostnadsbesparende og praktisk for bankene. Dersom rapporteringspliktige ikke gir tilbakemelding, fordi de ser slik informasjon som noe kostnadskrevende, vil de trolig være lite behjelpelige med tilbakemeldinger på svakheter og forbedringspotensialer. I hvor stor grad dette er tilfellet vet jeg ikke.

Gjentatte overføring av midler til utlandet vil gjerne «flagges ut» i det elektroniske overvåkningssystemet (se eksempler på risikomotor over), men hva om man benytter seg av tjenester fra virksomheter som driver betalingsformidling, som Western Union og Money Gram, når man skal overføre til utlandet ? Selv om også disse er rapporteringspliktige, kan det være hensiktsmessig å legge inn et «filter» i systemet som reagerer ved gjentatte overføringer også til slike virksomheter.

Jeg har tidligere nevnt at de risikofaktorer som velges ut beror på erfaring, noe som medfører at transaksjoner utført med andre metoder enn de vi kjenner «siles» ut av

[110] Ot.prp.nr.3(2008-2009) s.50

systemet.[111] En undersøkelse gjort av Enheten for finansiell etterretning(EFE) der de tok for seg 100 rapporter om mistenkelige transaksjoner viste at det var stor overvekt av rapporter som gjaldt kontante transaksjoner.[112] Hvitvasking av kontanter er kjent hvitvaskingsmodus, og fanges derfor gjerne opp. Som eksemplene på systemer i banker ovenfor viser, er dette fordi systemet blant annet reagerer på scenarioer og indikatorer som tar sikte på spesielle mønster i transaksjoner. Transaksjoner som har en uvanlig karakter eller er spesielt store og som ikke passer med kundens historiske registrerte opplysninger, altså avvikende adferd fanges opp. Hos en kunde som er hvitvasker fra før vil systemet derfor ikke oppdage avvik dersom kunden fortsetter sin hvitvaskingsvirksomhet som tidligere. Det må imidlertid legges til at det ikke bare er avvik, men også inngående kundekjennskap som ligger til grunn for bankens vurdering av risikoen til en kunde og transaksjon.

8 Sanksjoner

8.1 Plikt til å påvise at tilstrekkelig tiltak er utført

Hvitvaskingsdirektivet art. 39 stiller krav om at rapporteringspliktige skal kunne straffes dersom ikke pliktene oppfylles. Det vil derfor være behov for å etterprøve om tiltak i henhold til loven er utført, og hvitvaskingsloven § 5 angir derfor ikke bare en plikt til å foreta risikobasert kundekontroll, men i annet ledd også en plikt til å «*påvise at omfanget av utførte tiltak er tilpasset den aktuelle risiko*». Det kreves i følge forarbeidene ikke skriftlighet, men at det antageligvis vil være den beste måten å få det til på en forsvarlig måte. Kravet må ses i sammenheng med plikten til å utarbeide kontroll- og kommunikasjonsrutiner som også vil kreve en viss registrering, jf. § 23.

[111] Brå Rapport 2011:4

[112] Økokrim: *Trendrapport hvitvasking 2011* s.35

8.2 Pålegg, tvangstiltak, straff

Det er styrets og ledelsens ansvar å påse og sørge for at regelverket til enhver tid etterleves. Finanstilsynet er det organet som fører kontroll med bankers etterlevelse av hvitvaskingsloven med forskrifter, jf. lov av 7. juli 1956 nr. 1, Finanstilsynsloven. De har møter med banker, og kan gi skriftlige advarsler. Etter § 27 kan de gi pålegg om at forhold i strid med hvitvaskingsloven skal opphøre innen en gitt frist. Etterkommes ikke dette kan det fastsettes en tvangsmulkt.

Etter hvitvaskingsloven § 28 kan bøter anvendes ved forsettlig eller grov uaktsom overtredelse eller medvirkning til overtredelse av §§ 5-8, 15-18 og 22 eller forskrifter. Ved særlig skjerpende omstendigheter kan fengsel på inntil ett år anvendes. I forarbeidene påpekes, at det ikke er hensiktsmessig at ansatte gjøres til direkte pliktsubjekter i enkelte lovbestemmelser slik tilfellet var etter tidligere hvitvaskingslov. Ansatte i en bank vil likevel kunne straffes, men da på grunnlag av medvirkningsansvar etter straffeloven § 317.

I Norge har til nå ingen banker blitt straffet for brudd på plikt til å gjennomføre risikobasert kundekontroll etter § 5. Det britiske finanstilsynet nylig ilagt bot på 80 millioner for brudd på hvitvaskingsreglementet til den britiske banken Coutts, jf. Financial Services Authoritys «final notice» til Coutts på deres hjemmeside. Mer enn andre rapporteringspliktige er banker avhengig av at rutiner for hvitvasking blir fulgt av hensyn til omdømmerisiko og deres forhold til andre banker, særlig amerikanske. Skal penger sendes til land norske banker ikke har filialer eller samarbeid med gjøres dette gjerne via amerikanske banker som kan videreformidle slike betalinger. Mange utenlandske transaksjoner må dessuten ofte veksles om i US dollar før de sendes videre. Tilsynsorganer i USA krever at samarbeidsbanker har gode rutiner for anti-hvitvasking, hvis ikke kan transaksjoner fra denne banken innebære risiko for hvitvasking. Dette stiller krav også for norske banker.

8.3 Kan banker bli erstatningsansvarlig for brudd på hvitvaskingsloven?

Det har vært diskusjon rundt bankens erstatningsansvar ovenfor kunder som har blitt misbrukt til hvitvasking. I en sak fra Oslo Tingrett i 2009 (Baaslandsaken), påsto kunden at DNB NOR burde varslet Økokrim om at Baasland, en mann uten arbeid og

formue, kunne disponere over store summer som han jevnlig overførte til internasjonale spilleselskaper. Kunden mente videre at ved å unnlate å rapportere muliggjorde DNB at tapet ble så stort, derfor forelå årsakssammenheng og erstatningsansvar for banken. Saken ble avgjort uten at det ble tatt stilling til spørsmålet.

Erling Grimstad, som prosederte saken over, mener et erstatningsansvar vil synliggjøre de kostnadene som er forbundet med slik virksomhet og gi økonomisk motivasjon som bidrar til å forhindre hvitvasking.[113] Offentligrettslige regler vil da bli blandet med privatretten. Heller ikke internasjonalt har det vært foreslått å operere med erstatningsansvar ovenfor rapporteringspliktige. På bakgrunn av kan det se ut som Grimstad drar lovens formål for langt.

En dom i Follo tingrett 16.03.2012 kom imidlertid til at det forelå erstatningsansvar. Saken gjaldt Scandiabankens krav om erstatning fra Meglerhuset Meum, med brudd på hvitvaskingsloven som ansvarsgrunnlag. Banken hadde gitt lån på bakgrunn av alt for høy verdivurdering. Det var mistanke om proformahandel, det burde ledet til rapportering, stans av oppdrag og beskjed til banken. Retten mente det var årsakssammenheng mellom meglers uaktsomme handlinger og bankens tap. Saken er ikke rettskraftig før 2.mai, og blir trolig anket. Det blir spennende å se hva resultatet blir.

9 Avslutning

Den risikobaserte kundekontrollen har ført til at ressurser kan benyttes mer effektivt. Jeg tror den også har ført til at hvitvasking bekjempes mer effektivt. Loven krever at banker *selv* må vurdere hvor det er behov for sterkere kundekjennskap, jf. hvitvaskingsloven § 5. Dette krever økt kunnskap om hva som innebærer risiko enn tidligere. Etter min mening har den økte kunnskapen økt til større bevissthet, som igjen

[113] Grimstad, Erling og Kristian Dahle Trygstad- *Kritisk Juss 2010(36) nr. 4*

bidrar til en bedre risikovurdering og dermed et bedre system for å motvirke at banker misbrukes til hvitvasking. Systemet leder også til at det ikke bare er Finanstilsynet som presser bankene til å overholde reglene. Bankene presser også hverandre, ved at loven stiller krav om at også korrespondentbankforbindelser skal ha anti-hvitvaskingsrutiner, jf. § 16.

Lovens effektivitet er allikevel vanskelig å måle, da vi ikke vet sikkert hvor store midler som hvitvaskes. Hvitvaskingsreguleringens kostnader antas å være 300 millioner for norsk banknæring.[114] Når vi ikke vet effekten kan det være vanskelig å si hva som er akseptabel kostnad, men så lenge vi ikke har noe alternativt system vil nok samfunnet fortsette å utvikle det nåværende systemet.

Å bekjempe hvitvasking er som å skyte på et bevegelig mål(«moving target»). Det er stadig utvikling på området, noe som viser seg i det stadig økende internasjonale samarbeidet. Erfaring vil vise hva som trengs av nye regler og prosedyrer. Bankens og lovgivers anti-hvitvasking- og terrorfinansieringssarbeid må stadig oppdateres, og slik ser jeg for meg at utviklingen vil fortsette.

[114] Larsson, Paulo og Dan Magnusson, *Hvitvaskingsreguleringens kostnader*, Nordisk Tidsskrift for kriminalvidenskap 2009, s. 20

10 Litteraturliste

Lover:

1902 Almindelig borgerlig straffelov (Straffeloven) av 22. mai 1902 nr. 10

1956 Lov om tilsynet med finansinstitusjoner mv. (Finanstilsynsloven) av 7. desember 1956 nr. 1

1961 Lov om sparebanker (Sparebankloven) av 24. mai 1961 nr. 1.

1968 Lov til gjennomføring av bindende vedtak av De Forente Nasjoners Sikkerhetsråd av 7. juni nr. 4

1981 Lov om forretningsbanker av 24. mai 1981 nr. 2

1988 Lov om finansieringsvirksomhet og finansinstitusjoner (Finansieringsvirksomhetsloven) av 10. juni 1988 nr. 40

1992 Lov om gjennomføring i norsk rett av hoveddelen i avtale om Det europeiske økonomiske samarbeidsområde (EØS-loven) av 27. november 1992 nr. 109

1997 Lov om aksjeselskaper av 13. juni 1997 nr. 44.

1998 Lov om forebyggende sikkerhetstjeneste (Sikkerhetsloven) av 20.mars 1998 nr.10

2003 Lov om tiltak mot hvitvasking av utbytte fra straffbare handlinger mv. av 20. juni 2003 nr. 41 (tidligere hvitvaskingslov, nå erstattet av lov av 2009)

2004 Lov om register over opplysninger om valutaveksling og overføring av betalingsmidler inn og ut av Norge (Valutaregisterloven) av 28. mai 2004 nr. 29.

2005 Straffelov av 20. mai 2005 nr. 28 (ikke trådt i kraft)

2009 Lov om tiltak mot hvitvasking og terrorfinansiering mv.(Hvitvaskingsloven) av 6. mars 2009 nr. 11

Forskrifter:

FOR 1999-12-22 nr. 1374 Forskrift om sanksjoner mot Usamba bin Laden, Al-Qaida og Taliban

FOR 2009-03-13 nr. 303 Forskrift om kontrollutvalget for tiltak mot hvitvasking .

FOR 2009-09-22 nr. 1080 Forskrift om risikostyring og internkontroll

FOR 2009-03-13 nr. 302 Forskrift om tiltak mot hvitvasking og terrorfinansiering mv. (Hvitvaskingsforskriften).

Forarbeider:

NOU 2007:10	Om tiltak mot hvitvasking og terrorfinansiering (gjennomføring av EØS-regler tilsvarende EUs tredje hvitvaskingsdirektiv i norsk rett)
Ot.prp.nr.61 (2001-2002)	Om lov om endringer i straffeloven og straffeprosessloven mv.(lovtiltak mot terrorisme - gjennomføring av FN- konvensjonen 9. desember 1999 om bekjempelse av finansiering av terrorisme og FNs sikkerhetsråds resolusjon 1373 28.september 2001)
Ot.prp.nr.79 (2007-2009)	Om lov om endring av straffeloven 1902 mv. (straffebud mot oppfordring, rekruttering og opplæring til terrorhandlinger).
Ot.prp.nr.3 (2008-2009)	Om lov om tiltak mot hvitvasking og terrorfinansiering mv. (hvitvaskingsloven)
Innst. O.nr. 42 (2008-2009)	Innstilling fra finanskomiteen om lov om tiltak mot hvitvasking og terrorfinansiering mv. (Hvitvaskingsloven)

Konvensjoner, resolusjoner, etc:

Terrorfinansieringskonvensjonen	FN-konvensjonen 9. desember 1999 om bekjempelse av finansiering av terrorisme
FNs sikkerhetsråds resolusjon 1373	28. september 2001
FNs sikkerhetsråds resolusjon 1371	Gjennomført i norsk rett ved endringslov 28. juni 2002 nr. 54
FN konvensjonen mot korrupsjon	31. oktober 2003. Gjennomført ved endringslov 30. juni 2006 nr. 49.

EØS-avtalen, vedlegg IX, finansielle tjenester kap. II

Financial Action Task Force on money laundering, the forty recommentations. June 2003

Financial Action Task Force nine special recommendtations October 2001 (incorporating all subsequent amendments until February 2008)

The FATF Recommendations, International standards on combating money laundering and the financing of terrorism and proliferation, February 2012

Direktiver:

91/308/EØF	RÅDSDIREKTIV av 10.juni 1991om tiltak for å hindre at det finansielle system brukes til hvitvasking av penger (første hvitvaskingsdirektiv).
2001/97/EF	EUROPAPARLAMENT- OG RÅDSDIREKTIV av 4.desember 2001 om endring av rådsdirektiv 91/308/EØF om tiltak for å hindre at det finansielle system brukestil hvitvasking av penger (andre hvitvaskingsdirektiv**).**
2005/60/EF	EUROPAPARLAMENTS- OG RÅDSDIREKTIV av 26.oktober 2005 om tiltak for å hindre at det finansielle systemet blir benyttet til hvitvasking av penger og finansiering av terrorisme (tredje hvitvaskingsdirektiv).

Rundskriv:

Finanstilsynets Rundskriv	8/2009 Veiledning til lov og forskrift med tiltak mot hvitvasking
Finanstilsynets Rundskriv	3/ 2009 Veiledning til forskrift om risikostyring og internkontroll

Dommer:

Rt. 1998 s.1022

Rt. 2011 s.1

Rt. 2008 s.1473

Rt. 2004 s.598

RG.2011 s.569

LG-2011-14553

LG-2010-179947

LB-2010-62670-2

Follo tingretts dom 16. mars 2012 (10-110071TVI-FOLL)

Nedre Romerike tingretts dom 06. februar 2012 (12-001903-MED-NERO)

Bøker:

Booth 2011: Robin Booth: *Money Laundering law and regulation: A practical guide*, Oxford 2011.

Chanana 2008: Mita Chanana: «Advokaters undersøkelses- og rapporteringsplikt» i: *Hvitvasking*, (Ulf Stridbeck og Alf Petter Høgberg red) Oslo 2008, s. 89-122.

Eriksen 2008 Morten Eriksen: «Hvitvasking gjennom skatteparadiser» i: *Hvitvasking*, (Ulf Stridbeck og Alf Petter Høgberg red.) Oslo 2008 s. 152-243.

Eskeland 2011: Ståle Eskeland: *De mest alvorlige forbrytelser*, Oslo 2011.

Gotschalk 2010: Petter Gotschalk: *Ledelse og økonomisk kriminalitet*, Oslo 2010.

Grahn m. fl. 2010: Thomas Grahn, Fredric Lundén, Kent Madstedt, Björn Wendleby: *Åtegärder mot penningtvätt m.m.- En praktisk vägledning och kommentar*, 2010.

Høg/ Busck-Nielsen 2008: Ulla Høg og Kim Busck-Nielsen: *Hvidvaskloven med kommentarer*, København 2008.

Høgberg 2008: Alf Petter Høgberg: «Hvitvaskingsmekanismen og den rettslige regulering» i: *Hvitvasking*, (Ulf Stridbeck og Alf Petter Høgberg red.) Oslo 2008, s. 30-42

Johansen 1996: Per Ole Johansen: *Nettverk i gråsonene, et perspektiv på organisert kriminalitet*, Oslo 1996

McClean 2007: David McClean: *Transantional organized crime*, Oxford 2007.

Olsen 2007: Anders Berg Olsen: *Økonomisk kriminalitet- avdekking, gransking og forebygging*, 2007.

Stridbeck 2008: Ulf Stridbeck: «Hvem er i hvitvaskingsbransjen- et blandet persongalleri»i: *Hvitvasking*, (Ulf Stridbeck og Alf Petter Høgberg red.) Oslo 2008 s.43-56.

Artikler:

Grimstad, Erling og Kristian Dahle Trygstad, *Bankenes samfunnsansvar ved pengespill,* Kritisk Juss 2010(36) nr. 4

Annet:

Økokrim: *Trendrapport hvitvasking 2011*- fra Enheten for finansiell etterretning

Økokrim: *Trendrapport økonomisk kriminalitet og miljørkiminalitet* 2008-2009

Brå Rapport 2011:4: *Penningtvätt- Rapportering och hantering av misstänkta transaktioner.* (Brå- centrum för kunskap om brott och åtgärder mot brott. Brottsförebyggande rådet(Brå) utarbeider fakta og kunnskap om lovbrudd).

Politi- og justisdepartementet, Finansdepartementet: *Regjeringens handlingsplan mot økonomisk kriminalitet*, 2011

FATF *Summary of the 3rd mutual evaluation report on anti-money laundering and combating the financing of terrorism- Norway* 10. juni 2005.

FATF *Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing- High Level Principles and Procedues*, June 2007

FATF *Mutual Evaluation Fourth Follow-Up Report* 26 February 2009

FATF *Guidance Anti –Money laundering and terrorist financing measures and Financial Inclusion* June 2009

FATF *Money Laundering Using New Payment Methods* October 2010

FATF *Annual Report* 2010-2011

FATF *High- risk and non-cooperative jurisdictions,* Public Statement 16 February 2012

Basel Committee on Banking Supervision- Risk Matrix, vedlagt i anneks 2 i FATF sin *Guidance on the risk-based approach.*s.36-37

Samtale med Tor Ivar Mysen i DNB 24 januar 2012

Samtale med Ole Jørgen Eitrå og Einar Jørgenrud i Sparebank1 25. januar 2012 +kundeetableringsskjema

Samtale med Trude S. Eidsheim i Pareto bank 13. mars 2012 + kundeetableringsskjema

Samtale med Stig Hallgeir Øksnes i Evry 18. april 2012

Internettdokumenter (gyldig URL per 17.04.2012):

Økokrim, Trendrapport for hvitvasking, Oslo 2011:
http://www.hvitvasking.no/Artikler/Trendrapport_hvitvasking_2011/

Økokrim, *Indikatorer på hvitvasking*, Oslo 2010:
http://www.hvitvasking.no/Hvitvasking/Indikatorer-pa-hvitvasking---hva-kan-rapporteringspliktige-se-etter/

Finanstilsynet v/ Rune Grundekjøn, *Hvitvaskingsregelverket -plikter og praktiske utfordringer*, 2009:
http://www.hvitvasking.no/upload/Foredrag/Foredrag_Hvitvaskingsregelverket_Verdipapirforetakene20090616.pdf

Finanstilsynets generelle observasjoner ved tematilsyn vedrørende gjennomføring av lov om tiltak mot hvitvasking og terrorfinansiering mv. av 6.mars 2009 nr. 11 med tilhørende forskrift:
http://www.finanstilsynet.no

Compendium Paper on the supervisory implementation practices across EU Member States of the Third Money Laundering Directive [2005/60/EC], 2009:
http://www.esma.europa.eu/system/files/3L3_AML_TF_Compendium_Paper_supervisory_implementation_practices_re_3MLD__2_.pdf

Larsson, Paul og Dan Magunssong, *Hvitvaskingsreguleringens kostnader*, Nordisk Tidsskrift for Kriminalvidenskab, 2009
http://brage.bibsys.no/politihs/bitstream/URN:NBN:no-bibsys_brage_16568/1/hvitvaskingsregulering.pdf

Link til FATF- publikasjoner:
http://www.fatf-gafi.org

Link til Egmont group: 100 sanitised cases
http://egmontgroup.org/library/cases

Link til Basel Committee on Banking Supervision:
http://www.bis.org/publ/bcbs85.pdf

Link til oversikt over korrupte land:
http://www.transparency.org/publications/publications/other/corruption_perceptions_index_2011

Link til oversikt over skatteparadiser:
http://www.financialsecrecyindex.com/

Link til div statistikk fra Finansnæringens fellesorganisasjon:
http://www.fno.no/no/Hoved/Statistikk/Bank/

Link til spørsmål vedrørende Ot.prp.nr.3 om lov om hvitvasking fra fremskrittspartiets fra Kristin Halvorsen 21. januar 2009:
http://www.regjeringen.no/nb/dep/fin/dok/andre/brev/brev_stortinget/2009/sporsmal-vedrorende-otprp-nr-3-2008-2009.html?id=543249

Link til nyhetsartikkel om saken i Follo tingrett 16.mars 2012:
http://www.f-b.no/nyheter/fem-millioner-og-tap-for-meum-1.7140004

Link til nyhetsartikkel i the Economist 21. januar 2012:
http://www.economist.com/node/21543132/

Link til nyhetsartikkel om Baasland 9. desember 2009:
http://www.dagbladet.no/2009/12/09/nyheter/baasland/innenriks/bedrageri/konkurs/9424361/

Link til definisjon av risikobegrepet:
http://no.wikipedia.org/wiki/Risiko

11 Lister over tabeller og figurer