



STATSADVOKATEN

STATSADVOKATEN FOR SÆRLIG
ØKONOMISK OG INTERNATIONAL
KRIMINALITET

KAMPMANNSGADE 1
1604 KØBENHAVN V

TELEFON 72 68 90 00
FAX 45 15 00 16

E-mail: saoek@ankl.dk
www.anklagemyndigheden.dk
www.politi.dk

Hvidvask i Danmark

Den nationale risikovurdering 2018

Indhold

1. Forord	3
2. Sammenfatning.....	4
3. Introduktion.....	7
Hvad er hvidvask?	8
4. Konsekvenser for samfundet.....	11
Førforbrydelser og afledt kriminalitet	11
Strukturelle og samfundsøkonomiske konsekvenser.....	11
5. Metode og data i risikovurderingen.....	13
Identifikation af trusler og sårbarheder	14
Analyse af trusler og sårbarheder	15
6. Omverdensforhold.....	17
Hvidvasklovgivningen, hvidvaskdirektivet og hvidvaskstrategien	17
Internationalt samarbejde	17
Økonomiske faktorer.....	18
Sociale faktorer.....	18
Teknologiske faktorer.....	19
7. Tendenser i den profitmotiverede kriminalitet	20
Aktører inden for profitmotiveret kriminalitet	21
Nuværende kriminalitetstendenser	22
Fremadrettede kriminalitetstendenser	24
8. Fældende afgørelser for hæleri.....	26
9. Analyse og vurderinger (ikke offentligt tilgængelige).....	32
10. Litteratur.....	33
Bilag 1: Begreber og definitioner.....	40

1. Forord

Hvidvask af udbytte af kriminalitet er et alvorligt samfundsproblem, der er med til at understøtte kriminel aktivitet og underminere integriteten i det finansielle system og dermed sikkerheden og trygheden i samfundet. Hvidvask er samtidig et komplekst problem, fordi det ofte involverer metoder fra både den legale og illegale økonomi til at dække over de kriminelle aktiviteter.

For effektivt at kunne forebygge og bekæmpe hvidvask er det nødvendigt at identificere og analysere de risikofaktorer, der har betydning for udbredelsen af hvidvask. Den nationale risikovurdering udgør et centralt element i denne risikobaserede tilgang til bekæmpelsen af hvidvask.

Den første nationale risikovurdering på hvidvaskområdet blev udgivet i 2015. Kravene til myndighederne og de private aktører, der arbejder med forebyggelse og bekæmpelse af hvidvask, er siden blevet større i takt med, at de kriminelles metoder er blevet mere sofistikerede, og antallet af sager inden for navnlig økonomisk it-kriminalitet er steget markant. Derudover har flere større hvidvask-sager over de senere år været med til at skærpe opmærksomheden på bekæmpelsen af hvidvask og sætte fokus på behovet for et stærkere samarbejde mellem myndighederne og de private aktører på området.

Risikovurderingen for 2018 tager derfor udgangspunkt i en ny og forbedret risikomodel, der skal sikre myndighederne og private aktører bedre indblik i grundlaget for analyserne og gøre dem i stand til hurtigere og bedre at spore nye tendenser på hvidvaskområdet. Modellen er anvendt til at analysere og vurdere hvidvaskrisikoen inden for en række nærmere identificerede risikoområder.

I processen med at udarbejde risikovurderingen er der endvidere lagt vægt på at inddrage relevante myndigheder på området og andre offentlige samt private samarbejdspartnere, herunder repræsentanter for finansielle institutioner og andre underretningspligtige, som alle har bidraget til at gøre den nationale risikovurdering bedre og mere anvendelig i arbejdet med at forebygge og bekæmpe hvidvask.

SØIK vil i den forbindelse gerne takke alle samarbejdsparter for indsatsen i forbindelse med udarbejdelsen af risikovurderingen.

Morten Niels Jakobsen

Statsadvokat

2. Sammenfatning

Formålet med den nationale risikovurdering af hvidvaskområdet er at vurdere risikoen for hvidvask af udbytte fra kriminalitet og identificere de risikoområder, som i særlig grad bliver benyttet og er sårbare over for udnyttelse til hvidvask i Danmark.

Ved analyse af de identificerede risikoområder vurderes det, at nogle områder er mere attraktive at benytte til hvidvask end andre. De områder, som samlet set er vurderet til at have den højeste hvidvaskrisiko, er:

- **Pengeoverførselsvirksomheder og alternative pengeoverførere** bliver ofte benyttet af organiserede kriminelle til hvidvask af midler, der stammer fra kriminalitet. Pengeoverførere, herunder alternative overførere såsom *hawala*, kan benyttes til at føre illegitime midler til lande, hvor der ikke eksisterer en moderne, formel banksektor og hvor kontrolforanstaltningerne er svage. Særligt gældende for små pengeoverførselsvirksomheder og alternative pengeoverførere er der udfordringer i forhold til at leve op til hvidvaskforpligtelserne og de er vanskeligere at kontrollere og føre tilsyn med end større kædeoperatører og deres agenter. Området kategoriseres som værende et høj-risiko-område, bl.a. fordi det er svært at opdage kriminaliteten, idet flere pengeoverførere undlader at registrere sig i de lovpligtige registre hos myndighederne, og fordi sandsynligheden for retsforfølgelse og dom er lav, især ved sager med et internationalt aspekt.
- **Valutavekslingsvirksomheder** bliver i mange kriminelle miljøer benyttet til hvidvask. En af metoderne er omveksling af mindre pålydende pengesedler, som er tjent på ulovlige aktiviteter, til pengesedler med høj pålydende værdi. Især har 500-eurosedlen været populær, men EU har valgt at udfase denne ved udgangen af 2018. Omveksling til større sedler gør det lettere for kriminelle at opbevare eller transportere penge ud af landet, idet de derved fylder mindre rent fysisk. Risikoområdet vurderes som værende nemt tilgængeligt og meget attraktivt grundet muligheden for at forblive anonym, og da det hverken kræver særlig viden eller planlægning at benytte sig af en valutavekslingsvirksomhed. På dette område ses det også, at kriminelle selv opretter valutavekslingsvirksomheder, hvilket gør det til en attraktiv og nem metode at benytte. Der eksisterer ligeledes ”uofficielle” valutavekslingsvirksomheder, som ikke har søgt om tilladelse til udbud af valutavekslingsvirksomhed, og som oftest opererer via mindre forretninger. Disse udgør alt andet lige en højere hvidvaskrisiko. Området vurderes som et høj-risiko-område, hvilket ligeledes var vurderingen i sidste risikovurdering. Dog skal det bemærkes, at der siden sidste risikovurdering har været et øget fokus på valutavekslingsvirksomhederne og tilsynet er nu overgået fra Erhvervsstyrelsen til Finanstilsynet, hvilket bl.a. har medført en reduktion i antallet af tilladelser til at drive valutavekslingsvirksomhed.

- **Legale virksomhedskonstruktioner** benyttes i mange kriminelle kredse og i alle faser af hvidvaskprocessen. Metoden benyttes især i forbindelse med kædesvigs- og ”moms-karrusel”-sager ved brug af fiktiv fakturering for arbejde, som aldrig er udført. Der er eksempler på kriminelle, som enten selv opretter eller overtager allerede aktive selskaber, som benyttes til hvidvask. Det ses også, at stråmænd indsættes som ejere eller direktører for at skjule den reelle ejer- og beslutningskreds, og derved bevarer den kriminelle aktør sin anonymitet. Hvidvask via legale virksomhedskonstruktioner kan også foregå via mindre forretninger, som ved handelsbaseret hvidvask, hvor der sker en sammenblanding af legitime og illegitime midler, hvorved alle midlerne i sidste ende fremstår som lovlige. Området kategoriseres som et høj-risiko-område, da det vurderes som værende meget attraktivt at benytte til hvidvask og opdagelsesrisikoen er lav. Der er ikke nogen egentlig tilsynsmyndighed på området i hvidvask-regi, og fra myndighedernes side kræver det derfor ofte et grundigt kontrolarbejde for at opdage og identificere hvidvask.

- **Fysisk transport af valuta** vurderes i høj grad at blive benyttet til at kanalisere kriminelt udbytte ud af Danmark og eventuelt til placering af udbytte i lande med svagere AML-kontrol. Pengeinstitutterne opgraderer løbende deres overvågning af mistænkelige transaktioner, hvilket gør det vanskeligere for kriminelle at flytte penge via det finansielle system, hvorfor alternative metoder benyttes. Fysisk transport er relativt nemt og kræver ikke megen planlægning. Det vurderes at være et høj-risiko-område, blandt andet fordi der er lav opdagelsesrisiko, især ved fysisk transport af valuta ved grænseovergange på land eller til vands. Det er desuden vanskeligt at udlede forførbrydelsen fra hvidvask, og derved fastlægge hvorfra pengene stammer, da kontanter ikke er sporbare. På europæisk plan arbejdes der på ændring af lovgivningen vedrørende kontrol med likvide midler over EU's ydre grænser. Disse ændringer vil bl.a. medføre et udvidet samarbejde mellem myndigheder.

- **Landbaserede væddemål**, som er væddemål, hvor spiludbyder og spiller mødes fysisk, omfatter bl.a. køb og salg af gevinstkvitteringer. Dette er en populær hvidvaskmetode i mange kriminelle miljøer, hvor gevinstkvitteringer handles med det formål at få kriminelt udbytte til at fremstå som legale gevinster fra spil. Tidligere blev metoden primært benyttet til hvidvask af kontanter fra narkotikakriminalitet, men sidenhen er andre kriminelle miljøer ligeledes begyndt at benytte sig af metoden. Herudover er der også eksempler på forhandlere og udbydere af landbaserede væddemål, der faciliterer hvidvask ved enten at bistå kriminelle i at omgås kundekendskabsprocedurer eller ved at opkøbe gevinstkvitteringer med henblik på videresalg. Det vurderes som værende nemt tilgængeligt at hvidvaske via landbaserede væddemål, da det hverken kræver særlig planlægning eller viden og herudover er det attraktivt, da det er forholdsvist billigt og desuden er relativt nemt at bibeholde anonymiteten. Opdagelsesrisikoen er lav, hvilket til dels skyldes, at det er spiludbyderen, og ikke selve forhandleren af landbaserede væddemål, der er underlagt hvidvasklovens forpligtelser.

3. Introduktion

Hvidvaskaktiviteter spiller en vigtig rolle i forhold til at facilitere organiseret kriminalitet både nationalt og internationalt, men omfanget af hvidvask er meget vanskeligt at opgøre¹. Ifølge Basel Institute on Governance (2016) findes der hverken nationalt eller internationalt oplysninger, der kan anvendes til at beregne omfanget af hvidvask fyldestgørende.

Ifølge en rapport fra Europol (2017) er de primære kriminalitetsområder, som benytter sig af hvidvask til sløring af midlers oprindelse, narkotikasmugling, migrantsmugling, menneskehandel, cyberkriminalitet, diverse former for svindel (CEO-fraud, dokumentfalsk mv.) og handel med både lovlige og ulovlige varer. Processen med at hvidvaske udbytte fra alvorlig og organiseret kriminalitet involverer forskellige og ofte komplekse metoder, der kombinerer elementer fra den legale og illegale økonomi. Sammenblandingen af illegale og legale transaktioner sker blandt andet gennem pengeinstitutter, vekselkontorer, spiludbydere, betalingsinstitutter, pengeoverførselsvirksomheder og forskellige virksomhedskonstruktioner.

Ifølge Financial Action Task Force (FATF)² udgør en national risikovurdering fundamentet i en risikobaseret tilgang til forebyggelse og bekæmpelse af hvidvask. Det er derfor vigtigt løbende at identificere, vurdere og ikke mindst forstå risiciene for hvidvask for at opnå en effektiv indsats på området.

Den første nationale risikovurdering blev offentliggjort i 2015 (SØIK 2015), og den nye udgave er en videreudvikling, som bl.a. bygger på en forbedret metodik, især i identifikationsfasen, og øget transparens bag risikovurderingerne. Formålet med den nationale risikovurdering af hvidvaskområdet er fortsat at vurdere risikoen for hvidvask af udbytte fra kriminalitet og identificere de risikoområder - dvs. sektorer, systemer og produkter/services - som i særlig grad bliver benyttet og er sårbare over for udnyttelse til hvidvask i Danmark.

Den nationale risikovurdering er til brug for tilsynsmyndighederne og de underretningspligtige virksomheder og personer (jf. hvidvasklovens § 1). Det forventes, at såvel tilsynsmyndighederne som de underretningspligtige anvender risikovurderingen til at arbejde risikobaseret og til at udvikle egne risikovurderinger inden for sektorerne (jf. forarbejderne til hvidvasklovens 2016/1 LSF41, afsnit 3.4). Risikovurderingen er herudover til brug for dansk politi og anklagemyndigheden, idet den kan hjælpe til at skabe klarhed over, hvilke metoder der aktuelt kan anvendes til hvidvask af udbytte fra strafbare forhold. Samtidig skal rapporten bidrage til større offentlig indsigt i hvidvask-

¹ Beregninger fra et internationalt forskningsprojekt viser, at hvidvaskpotentialet i Danmark er på ca. 2,7 mia. euro (Utrecht University 2013). Af en senere rapport fremgår det, at der årligt genereres ca. 1,6 mia. euro fra illegale markeder i Danmark (Savona, Ernesto U. & Riccardi, Michele 2015). I begge rapporter er beregningerne baseret på oplysninger, der i dag er knap 10 år gamle, hvorfor den store forskel i det beregnede hvidvaskpotentiale må tilskrives valg af metode.

² FATF er et mellemstatsligt samarbejde under OECD, der beskæftiger sig med udvikling af anbefalinger til bekæmpelse af hvidvask og terrorfinansiering.

området for herved at give det politiske niveau, myndigheder og den private sektor et styrket grundlag for at tilrettelægge indsatsen mod hvidvask og udvikle forebyggende strategier, der kan dæmme op for og reducere omfanget af hvidvask i Danmark.

Hvad er hvidvask?

Hvidvask defineres i hvidvasklovens § 3 som:

1. uberettiget at modtage eller skaffe sig eller andre del i økonomisk udbytte eller midler, der er opnået ved en strafbar lovovertrædelse,
2. uberettiget at skjule, opbevare, transportere, hjælpe til afhændelse eller på anden måde efterfølgende virke til at sikre det økonomiske udbytte eller midler fra en strafbar lovovertrædelse eller,
3. forsøg på eller medvirken til sådanne dispositioner.

Hvidvaskloven omfatter også dispositioner foretaget af den, der har begået den strafbare lovovertrædelse, som udbyttet eller midlerne hidrører fra.

Visse virksomhedstyper (fx finansielle virksomheder) og udøvere af erhverv (fx revisorer, advokater og ejendomsmæglere) er ved hvidvaskloven pålagt en række undersøgelses- og underretningspligter, der udgør et led i den private sektors forebyggende foranstaltninger mod hvidvask. Manglende efterlevelse af disse pligter kan straffes med bøde eller fængsel.

Strafferetligt er hvidvask dækket af straffelovens følgende to bestemmelser:

Straffelovens § 290 som har følgende ordlyd: *For hæleri straffes med bøde eller fængsel indtil 1 år og 6 måneder den, som uberettiget modtager eller skaffer sig eller andre del i udbytte, der er opnået ved en strafbar lovovertrædelse, og den, der uberettiget ved at skjule, opbevare, transportere, hjælpe til afhændelse eller på lignende måde efterfølgende virker til at sikre en anden udbyttet af en strafbar lovovertrædelse, medmindre forholdet er omfattet af § 290 a.*

Stk. 2. Straffen kan stige til fængsel i 6 år, når hæleriet er af særligt grov beskaffenhed navnlig på grund af forbrydelsens erhvervsmæssige eller professionelle karakter eller som følge af den opnåede eller tilsigtede vinding, eller når et større antal forbrydelser er begået.

Stk. 3. Straf efter denne bestemmelse kan ikke pålægges den, som modtager udbytte til sædvanligt underhold fra familiemedlemmer eller samlever, eller den, der modtager udbytte som normalt vederlag for sædvanlige forbrugsvarer, brugsting eller tjenester.

§ 290, hæleri, vedrører alle former for udbytte fra strafbare forhold (fx tyveri, menneskesmugling, narkotikakriminalitet og bedrageri). Ifølge straffeloven kan såvel fysiske som juridiske personer (selskaber, foreninger mv.) blive idømt straf for hæleri/hvidvask.

Straffelovens § 290 a har følgende ordlyd: *For hvidvask straffes med bøde eller fængsel indtil 1 år og 6 måneder den, der konverterer eller overfører penge, som direkte eller indirekte er udbytte af en strafbar lovovertrædelse, for at skjule eller tilsløre den ulovlige oprindelse.*

Stk. 2. Straffen kan stige til fængsel i 8 år, når hvidvasken er af særligt grov beskaffenhed navnlig på grund af forbrydelsens erhvervsmæssige eller professionelle karakter eller som følge af den opnåede eller tilsigtede vinding, eller når et større antal forbrydelser er begået.

§ 290 a tager sigte på hvidvask af penge, både når det direkte udbytte af førforbrydelsen er penge, og når et udbytte i andet end penge er blevet omsat til penge, som derefter hvidvaskes. Bestemmelsen kriminaliserer en del af de handlinger vedrørende håndtering af udbytte fra en strafbar lovovertrædelse, der tidligere var omfattet af straffelovens § 290 om hæleri. I modsætning til § 290 omfatter bestemmelsen i § 290 a også handlinger, som gerningsmanden til førforbrydelsen selv foretager. I forhold til gerningsmanden til førforbrydelsen er bestemmelsen således udtryk for en vis nykriminalisering. I praksis vil gerningsmanden til førforbrydelsen navnlig kunne straffes efter hvidvaskbestemmelsen i § 290 a, hvis de hvidvaskehandlinger, den pågældende har foretaget, går væsentligt ud over sædvanlig håndtering af udbyttet af en lovovertrædelse.

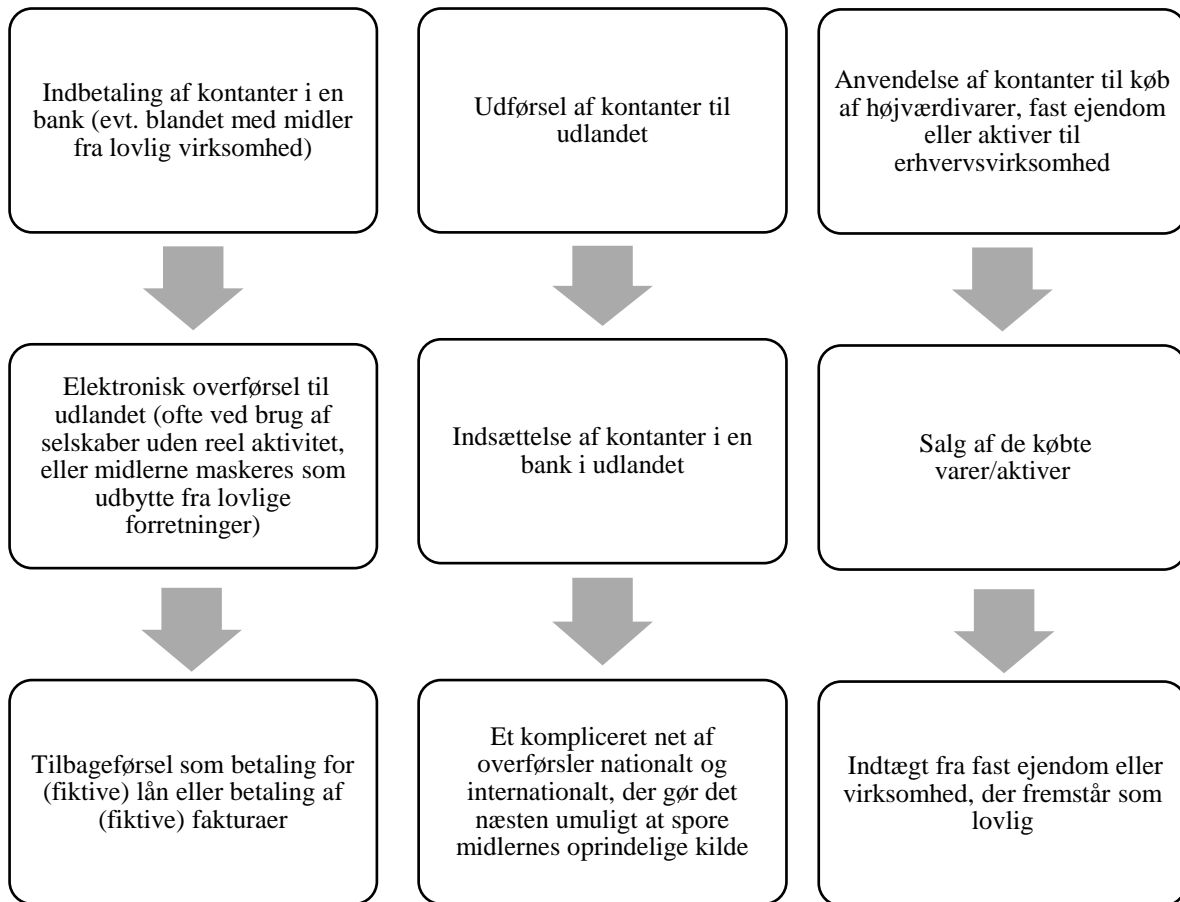
Hvidvasktransaktioner kan antage forskellige former og har til formål at ændre identiteten af kriminelt udbytte eller midler, således at det på et tidspunkt kan komme til at fremstå som lovlige midler eller aktiver.

Hvidvask kan foregå i flere faser:

1. Anbringelse: Den fysiske anbringelse af udbyttet - placering i det finansielle system
2. Sløring: Adskillelse af udbyttet fra dets kilde gennem (finansielle) transaktioner for at skjule revisionssporet og opnå anonymitet
3. Integrering: Tilbageførsel af midler til formuesfære i en form, hvor udbyttet er konverteret til midler, der fremstår som lovlige

I praksis kan disse faser eksempelvis foregå på følgende måder:

Figur 1 Eksempler på hvidvask



4. Konsekvenser for samfundet

Det har alvorlige konsekvenser for samfundet, når der hvidvaskes udbytte fra kriminalitet og dette er uafhængigt af hvilken hvidvaskemetode, som benyttes.

Det er vurderingen, at kriminelle aktører som udgangspunkt hverken tager højde for eller lader sig påvirke af konsekvenserne for samfundet, når de hvidvasker udbytte fra kriminalitet. På denne baggrund vurderes det ikke, at konsekvenserne for samfundet på forskellig vis påvirker risikoen for hvidvask i de identificerede risikoområder. Af denne årsag er konsekvenserne for samfundet vurderet samlet og ikke under de enkelte risikoområder i analysen.

Førforbrydelser og afledt kriminalitet

Hvidvaskaktiviteter er forbundet til stort set al profitskabende kriminalitet (Europol 2017). Det er politiets erfaring, at hvidvasksager ofte har forbindelse til organiseret kriminalitet, fx narkotikakriminalitet eller skatte- og momssvig. Hvidvask er ofte afhængig af, at personer benyttes eller udnyttes som stråmænd eller muldyr. Dette indebærer en risiko for at personer, som ikke nødvendigvis er kriminelle i forvejen, kan lade sig friste til at medvirke til kriminalitet mod betaling. Ligeledes kan der i stråmands- og muldyrssager være tale om menneskehandel, hvor udlændinge tvinges ud i kriminalitet. Derudover er der også en stigende tendens til organisering af egentlige hvidvasknetværk, som tilbyder hvidvask for tredjemand, uden udbyderen af hvidvaskprocessen behøver at have været involveret i førforbrydelsen.

Hvidvask af kriminelt udbytte fastholder og bidrager til væksten på de kriminelle markeder på tværs af EU (Europol 2017). Ved at forebygge, bekæmpe og besværliggøre hvidvask, kan det blive vanskeligere for kriminelle aktører at udføre de førforbrydelser, som genererer udbytte der kan hvidvaskes, samt reducere den profit, der kan genereres ved kriminalitet.

Strukturelle og samfundsøkonomiske konsekvenser

Kriminelle aktørers bestræbelser på at tilsløre udbytte fra strafbare forhold kan medføre svækket tillid til det finansielle system. Det kan skade den finansielle sektors integritet, stabilitet og omdømme samt true det indre marked og den internationale udvikling, hvis finansielle institutioner anvendes til hvidvask (Den Europæiske Unions Tidende 2015).

Det kan ligeledes være skadeligt for andre, tilknyttede finansielle institutioner, lovgivende myndigheder og almindelige kunder i institutionen. (FATF n.d.).

Derudover kan det virke krænkende for befolkningens retsfølelse, hvis der er en opfattelse af, at hvidvask forbliver uopdaget eller ustraffet. Det er samtidig skadeligt for samfundsøkonomien, når

kriminelle aktører hvidvasker udbytte fra kriminalitet. Der er både direkte og indirekte konsekvenser, hvoraf de direkte konsekvenser ses i form af mistede skatter og afgifter. De indirekte konsekvenser kan eksempelvis ses i de tilfælde, hvor der placeres en stor mængde udbytte fra kriminalitet i specifikke typer af varer eller ydelser. Dette kan have negative konsekvenser for markedet, da det vil være konkurrenceforvridende for de personer og virksomheder, som legalt handler varerne og ydelserne. Det samme gør sig gældende for brancher, hvor der er en stor grad af ”sort” økonomi, eksempelvis visse dele af servicebranchen.

Hvidvaskemodi, hvor det kriminelle udbytte sendes til udlandet, medfører, at der ikke bliver svaret skatter og afgifter af de kriminelle midler. Det har ligeledes den betydning, at pengene ikke umiddelbart bliver genintroduceret i den danske økonomi.

5. Metode og data i risikovurderingen

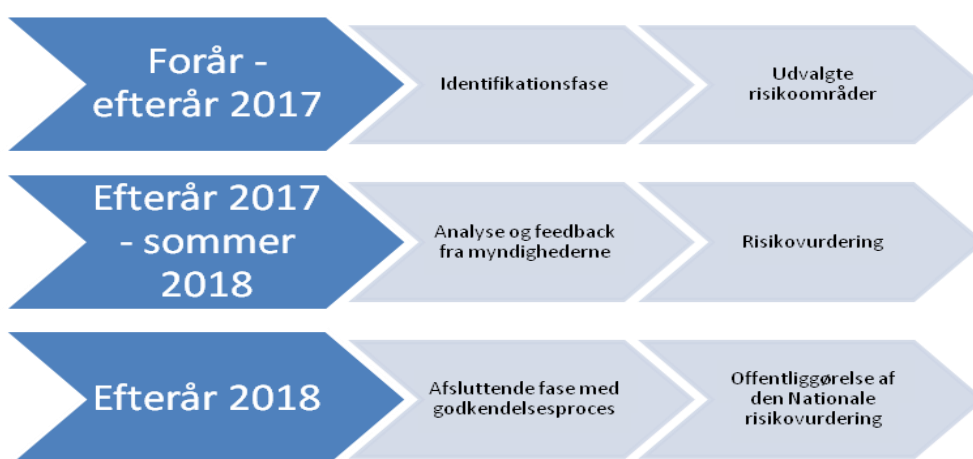
Denne nationale risikovurdering af hvidvaskområdet adskiller sig på flere punkter fra den tidligere risikovurdering. Først og fremmest har SØIK videreudviklet den risikomodel, der er anvendt til analyse og vurdering af hvidvaskrisikoen inden for hvert enkelt risikoområde. Risikomodellen, som er vist på side 15, indeholder parametre relateret til både trusler og sårbarheder og er videreudviklet for at give et bedre indblik og øget transparens i vurderingerne af de analyserede områder. SØIK har herudover inddraget langt flere samarbejdspartnere fra den private og offentlige sektor end i den tidligere risikovurdering, hvilket har styrket grundlaget og derved umiddelbart gjort vurderingen mere relevant og anvendelig for de underretningspligtige. Herudover har SØIK hentet inspiration fra udenlandske risikovurderinger samt FATF's vejledning (FATF 2013b) vedrørende udarbejdelse af risikovurdering på hvidvask- og terrorfinansieringsområdet.

Arbejdet med den nationale risikovurdering kan overordnet inddeles i to faser:

- 1) *identifikation* af trusler og sårbarheder i forhold til risikoen for hvidvask og
- 2) *analyse* af trusler og sårbarheder med henblik på at forstå risiciene og vurdere sandsynligheden for at hvidvask forekommer.

Nedenstående Figur 2 viser et overblik over processen i forbindelse med udarbejdelse af risikovurderingen:

Figur 2 Overblik over processen



Arbejdet med den nationale risikovurdering har været en omfattende proces, hvoraf identifikationsfasen forløb i foråret og frem til efteråret 2017. På baggrund af de identificerede risikoområder blev analysefasen påbegyndt og forløb frem til sommeren 2018. Herefter blev slutfasen med en godkendelsesproces påbegyndt og afsluttet i efteråret 2018.

Identifikation af trusler og sårbarheder

Definitionen af en trussel forstås som en person, gruppe eller aktivitet, der potentielt kan gøre skade mod staten, samfundet, økonomien mv. En sårbarhed kan udnyttes af en trussel eller facilitere trusselens aktiviteter. Sårbarheder kan således være svagheder i det danske system til bekæmpelse af hvidvask, men det kan også være et produkt eller en service, der bevirker, at en sektor er særligt udsat.

Med henblik på at identificere trusler relateret til risikoen for hvidvask er der først set på forhold i omverdenen, der kan have betydning for omfanget af og metoderne til hvidvask (se side 17). Dernæst er der set på tendenser i den profitmotiverede kriminalitet (se side 20), da hvidvaskpotentialet afhænger af udviklingen inden for specifikke kriminalitetsformer: bedrageri, skatte- og momssvig, narkotikakriminalitet mv. Det er ikke muligt at undersøge fordelingen af de forbrydelser, der går forud for hvidvaskprocessen (førforbrydelserne), da den nuværende lovgivning ikke gør det muligt at identificere samtlige sager i Danmark, hvor hvidvask har fundet sted.

De to afsnit om henholdsvis omverdensforhold og tendenser i den profitmotiverede kriminalitet er baseret på oplysninger fra en lang række kilder, herunder Europol, Det Kriminalpræventive Råd, Danmarks Statistik, Rigspolitiet og Rockwoolfondens Forskningsenhed. Herudover inddrages oplysninger fra underretninger sendt til Hvidvasksekretariatet i SØIK samt registeroplysninger om politianmeldelser inden for økonomisk kriminalitet.

Identifikationen af sårbarheder er sket i samarbejde med tilsynsmyndighederne: Finanstilsynet, Erhvervsstyrelsen, Spillemyndigheden og Advokatsamfundet. Herudover har Finans Danmark, Dansk Ejendomsmæglerforening (DE), Danske Revisorer (FSR), Finans og Leasing samt Forsikring og Pension bidraget med oplysninger på vegne af deres medlemmer. Skattestyrelsens afdeling for Særlig Kontrol har bidraget med oplysninger fra den enhed, der undersøger sager med konkret mistanke om momskarruselsvig og kædesvig.

Processen i forhold til identifikation af sårbarheder forløb fra foråret til efteråret 2017, jf. ovenstående Figur 2, og der kan derfor være yderligere sårbarheder, som efterfølgende er blevet relevante, men som ikke blev fremhævet i selve identifikationsfasen. Eksempelvis er SØIK efterfølgende blevet opmærksom på flere områder, som er identificeret som værende mulige risikoområder, fx AIF/FAIF fonde. Dette område er dog ikke inkluderet i denne risikovurdering, men vil blive inkluderet og vurderet i en kommende national risikovurdering, såfremt det er relevant. Herudover skal det bemærkes, at forsikrings- og pensionsområdet blev fremhævet som værende særligt sårbart over for misbrug til hvidvask. Den efterfølgende risikovurdering af området har dog vist, at med de nuværende kontrolforanstaltninger og love omkring udbetaling af pensions- og forsikringsmidler synes

det meget lidt sandsynligt, at hvidvask skulle kunne forekomme. Dette område er derfor udeladt fra risikovurderingens analyse.

Herudover har politikredsens afdelinger for organiseret kriminalitet, deriblandt afdelinger hos Grønlands Politi og Færøernes Politi, bidraget med oplysninger om, hvilke trusler og sårbarheder der aktuelt kan relateres til risikoen for hvidvask i Danmark. Oplysningerne er indhentet via interviews og stammer primært fra efterforskninger af førforbrydelser til hvidvask af kriminelt udbytte.

På baggrund af identifikationen af trusler og sårbarheder, som blev foretaget i foråret til efteråret 2017 behandles følgende risikoområder i risikovurderingen:

- ✓ Legale virksomhedskonstruktioner
- ✓ Pengeinstitutter
- ✓ Betalingsinstitutter
- ✓ Pengeoverførselsvirksomheder
- ✓ Valutavekslingsvirksomheder
- ✓ Fysisk transport af valuta
- ✓ Spilsektoren
- ✓ Fast ejendom
- ✓ Høj-værdi-varer
- ✓ Leasing
- ✓ Service providers
- ✓ Rådgivere
- ✓ Virtuelle valutaer

Analyse af trusler og sårbarheder

Til brug for analysen af trusler og sårbarheder er der udviklet en risikomodel med i alt fem parametre: Omfang, tilgængelighed, attraktivitet, opdagelsesrisiko og sandsynlighed for retsforfølgelse og dom. Disse parametre vægter alle lige højt i den samlede vurdering af, om hvidvaskrisikoen inden for hver enkelt risikoområde er henholdsvis lav, middel eller høj.

Med risikomodellen som udgangspunkt er hvert enkelt identificeret område derefter analyseret og vurderet indgående med hensyntagen til tidligere erfaringer og ny information som er tilvejebragt fra politikredsene, andre myndigheder og interesseorganisationer.

De analyserede og vurderede risikoområder er alle fremsendt til relevante tilsynsmyndigheder og skattemyndighederne. De har derved haft mulighed for at give feedback og kvalificere argumenter i de relevante kapitler inden for deres område. Analysen bygger således på værdifuld ekspertise og viden fra myndighederne, som er kombineret med politiet og anklagemyndighedens viden og erfaringer fra straffesager.

Tabel 1 Risikomodel til risikovurdering af hvidvaskkanaler

	Parameter	Risiko <i>Lav</i>	Risiko <i>Middel</i>	Risiko <i>Høj</i>
Trussel	Omfang³	Begrænset <i>Hvidvaskmuligheden benyttes så vidt vides ikke eller kun af en lille kreds i kriminelle miljøer</i>	Moderat <i>Hvidvaskmuligheden benyttes af et moderat antal personer i kriminelle miljøer</i>	Stort <i>Hvidvaskmuligheden benyttes af mange personer i kriminelle miljøer</i>
	Tilgængelighed	Svært <i>Svært tilgængeligt, kræver betydelig planlægning, viden og/eller teknisk ekspertise</i>	Moderat <i>Forholdsvis tilgængeligt, kræver moderat planlægning, viden og/eller teknisk ekspertise</i>	Nemt <i>Let tilgængeligt, kræver lidt eller ingen planlægning, viden og/eller teknisk ekspertise</i>
Sårbarhed	Attraktivitet	Uattraktiv <i>Det er svært at forblive anonym, metoden opfattes som usikker og/eller dyr at anvende</i>	Moderat attraktiv <i>Det er relativt let at forblive anonym, metoden opfattes som rimelig sikker og/eller mindre dyr at anvende</i>	Meget attraktiv <i>Det er meget let at forblive anonym, og metoden opfattes sikker og/eller billig at anvende</i>
	Opdagelsesrisiko	Høj <i>Der er passende kontrolinstanser, og det er sandsynligt, at det opdages, hvis der forekommer forsøg på hvidvask</i>	Middel <i>Der er begrænsede kontrolinstanser, og det er mindre sandsynligt, at det opdages, hvis der forekommer forsøg på hvidvask</i>	Lav <i>Der er svage eller ingen kontrolinstanser, og det er svært at opdage, hvis der forekommer forsøg på hvidvask.</i>
	Sandsynlighed for retsforfølgelse og dom	Høj <i>Lovgivningen er fuldt ud tilstrækkelig til at forfølge potentielle hvidvaskere, og politiet og øvrige myndigheder har ressourcer og kompetencer til at gøre det</i>	Middel <i>Lovgivningen er tilstrækkelig til at forfølge potentielle hvidvaskere, men politiet og øvrige myndigheder har begrænsede ressourcer og kompetencer til at gøre det</i>	Lav <i>Lovgivningen er mangelfuld i forhold til at forfølge potentielle hvidvaskere, og politiet og øvrige myndigheder mangler ressourcer og kompetencer til at gøre det</i>

³ Det bemærkes, at denne parameter indeholder oplysninger om førforbrydelser til hvidvask via det område, der er i fokus, og om andre forhold i omverdenen af betydning for omfanget, f.eks. udviklingen i kriminelle miljøer og den øgede digitalisering.

6. Omverdensforhold

Flere faktorer i samfundsudviklingen er medvirkende til at bestemme omfanget og typen af kriminalitet og hvidvask. I det følgende ses der derfor nærmere på lovgivningsmæssige, internationale, økonomiske, teknologiske, og sociale faktorer, som kan have betydning for motivation og muligheder for at begå hvidvaskkriminalitet.

Hvidvasklovgivningen, hvidvaskdirektivet og hvidvaskstrategien

Trusselsbilledet i forhold til hvidvask og terrorfinansiering ændrer sig konstant, hvilket har spillet en rolle i forbindelse med tilblivelsen af EU's 4. hvidvaskdirektiv, som bygger på FATF's (Financial Action Task Force) anbefalinger.

Direktivet muliggør ikke, at medlemsstaterne kan lempe deres lovgivninger, men sætter fokus på, at der skal indføres mere skærpede regler end dem, som EU har påkrævet. Implementeringen af det 4. hvidvaskdirektiv udmøntede sig i stramminger i den danske lovgivning og på denne baggrund trådte der (i juni 2017) en ny og skærpet udgave af hvidvaskloven i kraft. Der er desuden i sommeren 2018 indført en ny bestemmelse i straffeloven om hvidvask, jf. afsnittet "Hvad er hvidvask?" ovenfor.

I juni 2018 blev det 5. hvidvaskdirektiv vedtaget i EU. Direktivet sætter bl.a. fokus på kriminelles brug af elektroniske penge og virtuel valuta (Den Europæiske Unions Tidende 2018). Regeringen har derudover indgået en ny hvidvaskaftale den 19. september 2018, som bl.a. indeholder mulighed for forhøjet bødestraf, en fasttrack-ordning, udvidelse af fit og proper-krav og forbud mod anvendelse af 500-eurosedlen i Danmark (Finans Danmark 2018 og Erhvervsministeriet 2018).

Internationalt samarbejde

Danmarks medlemskab i EU skaber international mobilitet og giver mulighed for at søge arbejde i udlandet, drive virksomhed i flere lande og flytte penge over landegrænser, men den frie bevægelighed inden for EU stiller samtidig krav om et stærkt samarbejde mellem landenes myndigheder i efterforskningen og retsforfølgningen af borgere, der begår grænseoverskridende kriminalitet. Danmarks position i EU's retssamarbejde har ændret sig de seneste år, efter at Danmark stemte nej til tilvalgsordningen for det retlige samarbejde i 2015 og som konsekvens heraf forlod Europol pr. 1. maj 2017. Dansk politi har dog fortsat adgang til oplysninger i Europol via forbindelsesofficerer, ligesom Danmarks status i Eurojust⁴-samarbejdet ikke har ændret sig. I takt med at flere retsakter på området for retlige og indre anliggender ændres i de kommende år, vil Danmark på grund af retsforbeholdet ikke længere kunne deltage i samarbejdet på samme vilkår, hvilket kan risikere at besværliggøre Danmarks praktiske samarbejde med øvrige EU-lande om sager vedrørende bl.a. sporing, beslaglæggelse og konfiskation af udbytte fra kriminalitet (Sørensen 2018). Danmark er imid-

⁴ Eurojust er et EU- samarbejde mellem de nationale anklagemyndigheder i sager med grænseoverskridende kriminalitet.

lertid fortsat med i samarbejdet om bekæmpelse af økonomisk kriminalitet under Financial Action Task Force (FATF) under OECD og i Egmontsamarbejdet⁵.

Økonomiske faktorer

Danmark har en åben økonomi, der er meget afhængig af samhandel med udlandet, og som samtidig påvirkes let af udefrakommende faktorer og internationale, økonomiske tendenser.

Beskæftigelsen er på nuværende tidspunkt på sit højeste i mange år, og danskerne har flere penge til forbrug end tidligere (Økonomi- og Indenrigsministeriet 2018). I takt med, at ledigheden er faldet, modtager færre offentlig forsørgelse, og samtidigt er skatten blevet lavere. Incitamentet til at begå visse former for økonomisk kriminalitet (herunder svindel med sociale ydelser, skatteunddragelse og sort arbejde) vurderes derfor at være mindre end i årene under finanskrisen⁶. Det skal samtidig bemærkes, at værdien af sort arbejde i 2016 skønnedes at udgøre mellem 34 og 59 mia. kr. svarende til mellem 1,7 og 2,9 procent af den danske BNP (Andersen, L. H. 2017).

Økonomi- og Indenrigsministeriet vurderer, at manglen på arbejdskraft på grund af væksten har lagt et pres på det danske arbejdsmarked. Presset vurderes at være formindsket ved forøget udenlandsk arbejdskraft, men spiller fortsat en rolle og vil kunne bremse den økonomiske vækst på længere sigt. Ifølge De Økonomiske Råd (2018) ses der tegn på, at jobmuligheder for ufaglærte og i mindre omfang også for faglærte vil svækkes i takt med en stigning i andelen af udenlandsk arbejdskraft, da en stor andel af den gruppe beskæftiges i lavtlønnede jobs. Dette kan påvirke incitamentet hos denne gruppe til at begå økonomisk kriminalitet, herunder sort arbejde.

Sociale faktorer

OECD forventer, at antallet af personer på verdensplan, som lever i sårbare kontekster, fortsat vil stige – fra 1,6 mia. til 3 mia. svarende til 32 % af verdens befolkning i 2050 (OECD 2016). Stigningen vil med stor sandsynlighed få betydning for flygtninge- og migranttilstrømningen til Europa fremover.

Det er vanskeligt at vurdere konsekvenserne af flygtninge- og migranttilstrømningerne, da disse er afhængige af den politiske udvikling i Danmark, Europa og på verdensplan. Danmark indførte den 4. januar 2016, som følge af den store flygtninge- og migranttilstrømning, midlertidig grænsekontrol sammen med en række andre europæiske lande (Udlændinge- og Integrationsministeriet 2017). Grænsekontrollen, og det øgede antal flygtninge og migranter, har skabt et mere attraktivt marked for menneskesmugling. Migrantsmugling er blevet en meget profitabel og udbredt aktivitet for or-

⁵ Egmont er et FN-samarbejde om bekæmpelse af økonomisk kriminalitet og terrorfinansiering mellem 155 ud af FN's 192 godkendte lande.

⁶ En ny undersøgelse fra Rockwool Fonden Forskning (2018) viser dog, at beskæftigelsen blandt de 25-54-årige fortsat er væsentligt under niveauet fra årene før krisen.

ganiseret kriminalitet i EU (Europol 2017). Udover transport af migranter er dokumentforfalskning en kriminel nøgleaktivitet, som er linket til migrationskrisen. Det er estimeret, at migrantsmuglingsnetværk samlet set i EU genererede mellem 4,7 og 5,7 mia. euro i profit i 2015. Profitten er dalet siden 2016 med minimum 2 mia. euro, hvilket er i overensstemmelse med det dalende antal migranter (Europol 2017).

Socialt bedrageri og bedrageri vedrørende arbejdsløsheds-kasser har en alvorlig påvirkning på den danske velfærdsstruktur, særligt hvis der er tale om organiseret eller omfattende bedrageri med offentlige ydelser. Socialt bedrageri, primært begået mod arbejdsløsheds-kasser, har siden 2015 været en af de kriminalitetsformer hvor anmeldelsestallet er faldende (Politi 2017). Tendensen hænger formentligt sammen med, at der i Danmark på nuværende tidspunkt ses lav arbejdsløshed (Danmarks Statistik 2018), hvilket kan bidrage til et lavere incitament til at begå socialt bedrageri.

Teknologiske faktorer

Udviklingen og brugen af de teknologiske ressourcer bidrager til at skabe grundlag for nye former for økonomisk kriminalitet og udvikling af eksisterende kriminalitet. Kriminalitetstyper, der tidligere krævede fysisk kontakt mellem kriminelle og forurettede, kan i dag finde sted over internettet. Ved hjælp af internettet kan kriminelle aktører hurtigt skabe kontakter og netværk, hvormed forskellige kompetencer og muligheder kan udnyttes. Som følge af den teknologiske udvikling opstår der derfor mulighed for nye forretnings- og kriminalitetsformer såsom hacking, tyveri af oplysninger og salg eller udnyttelse af data. Der bliver via brug af internettet delt mere personlig information om brugerne, herunder adfærd, færdene og præferencer (Pedersen, Rene 2017).

Potentialet for især økonomisk it-kriminalitet (kreditkortsvindel m.m.) er stort, bl.a. fordi 77 % af den danske befolkning mellem 16 og 89 år har anvendt internethandel til køb af tøj, rejser, oplevelser og dagligvarer, og tendensen er stigende (Forsvarets Efterretningstjeneste 2017). Handel med ulovlige genstande som narkotika og våben via sociale medier eller Dark Web er ligeledes en af de voksende og populære kriminalitetsformer. Især inden for handel på Dark Web ses en stigende tendens, hvor handlerne ofte foregår ved, at der betales med virtuel valuta for varerne.

Den teknologiske udvikling er dog ikke kun negativ, den giver ligeledes politiet nye muligheder. Politiet har bl.a. fået udviklet et nyt IT-system, POL-INTEL, som samkører oplysninger fra flere forskellige registre, som politiet normalt har adgang til (DR 2018). POL-INTEL er et stærkt opslagsværktøj, som muliggør mere effektive efterforskninger, da søgemulighederne er mere avancerede end i de hidtidige systemer.

7. Tendenser i den profitmotiverede kriminalitet

Som beskrevet i afsnittet, der vedrører omverdensforhold, ses der flere samfundsfaktorer som påvirker kriminalitetsudviklingen, både i Danmark og i resten af verden. Grænsefladerne mellem hvidvask, internetrelateret og profitmotiveret kriminalitet bliver konstant mere udvaskede, og der ses ofte overlap mellem de forskellige typer af kriminalitet, som går forud for hvidvaskprocessen.

De underretninger, som Hvidvasksekretariatet modtager vedrørende mulig hvidvask, kan give en indikation på, hvilke typer af forførbrydelser der begås, samt hvordan selve hvidvaskprocessen foregår efterfølgende. Andre typer af anmeldelser og kriminalitetsformer er dog også relevante at inddrage for at danne et fyldestgørende overblik over, hvilke tendenser, der dominerer inden for profitmotiveret kriminalitet og hvidvask.

Hvidvasksekretariatet fungerer som Danmarks FIU (Financial Intelligence Unit) og modtager underretninger om mulig hvidvask eller finansiering af terrorisme fra de i hvidvaskloven underretningspligtige virksomheder og personer. Hvidvasksekretariatet kan endvidere modtage underretninger fra myndigheder, virksomheder og borgere, som finder et forhold mistænkeligt og sender en underretning til Hvidvasksekretariatet, uden at være underlagt en underretningspligt. I 2017 modtog Hvidvasksekretariatet knap 25.000 underretninger, hvilket er 33 % flere underretninger end året før (Tabel 2).

Tabel 2. Antal underretninger sendt til Hvidvasksekretariatet.

2013	2014	2015	2016	2017
5.166	7.255	15.619	18.669	24.911

Stigningen i antallet af underretninger til Hvidvasksekretariatet skyldes formentlig et øget fokus på hvidvask og terrorfinansiering hos tilsynsmyndighederne og de underretningspligtige. Derudover blev det i 2014 et krav at underrette Hvidvasksekretariatet elektronisk, hvilket fik blandt andet pengeinstitutterne til at indføre systemer, der gør det lettere at underrette. Det kan ikke udelukkes, at stigningen i antallet af underretninger også skyldes, at den profitmotiverede kriminalitet er i vækst.

Størstedelen af de underretninger, der modtages i Hvidvasksekretariatet, kommer fra pengeinstitutter. Størstedelen af de underretninger, der videregives fra Hvidvasksekretariatet, oversendes til skattemyndigheden, da de ofte omhandler mistanke om svindel med indtægt eller offentlige ydelser.

Grænsen for kontantforbuddet blev i juli 2013 nedsat fra kr. 100.000 til kr. 50.000, for at mindske risiko for hvidvask via kontanthandler, hvilket også kan have medvirket til et øget fokus fra de underretningspligtige. Det kræves, at de underretningspligtige (erhvervsdrivende, revisorer, advokater

og pengeinstitutter) er opmærksomme på store kontantbeløb og mistænkelige indsættelser samt underretter herom for at hindre hvidvask via denne metode.

Hos de underretningspligtige er der stort fokus på compliance, herunder at opdage og videregive oplysninger om overtrædelser af hvidvaskloven. Eksempelvis er fokus på at opdage socialt bedrageri og skatte- og afgiftssvindel intensiveret hos kontrolmyndighederne. Skatteforvaltningen har blandt andet optimeret deres indsats på tilsynsområdet i 2018 ved at ændre struktur og opdele myndigheden i syv nye styrelser (Skatteforvaltningen N.d.).

Mistanke om hvidvask via online spilletjenester er en af de kriminalitetsformer, der ofte ses i de underretninger, som Hvidvasksekretariatet modtager. I takt med, at der kommer flere online spilletjenester, øges mulighederne for hvidvask via den metode. Tidligere har især handel med fysiske lotto- og oddskuponer været en metode, som blev benyttet i forbindelse med hvidvask af penge i narkosager, men dette ses nu også inden for andre typer af forførelser.

Aktører inden for profitmotiveret kriminalitet

Ifølge Det Kriminalpræventive Råd er den profitmotiverede kriminalitet generelt rykket fra gaden til cyberspace. Det er dog stadig de samme risikofaktorer og incitament, der gør sig gældende i forhold til at begå kriminalitet. Gerningsmændene til både internetrelateret og profitmotiveret kriminalitet har derfor overvejende de samme profiler, som de der begår kriminalitet i den fysiske verden (Kruize, Peter 2018).

Ifølge Hvidvasksekretariatets data er de kriminelle aktører, der opererer inden for hvidvaskområdet, ofte personer, som er i politiet og andre kontrolmyndigheders søgelys i forvejen i forbindelse med andre sagskategorier. Personer med relationer til rocker- og bandemiljøet figurerer dog relativt sjældent i hvidvaskunderretningerne, og det samme gør sig gældende for andre organiserede kriminelle grupperinger. Der ses en tendens til, at personer med udenlandske rødder, som har opholdt sig i Danmark i kort tid, indsættes som stråmand i komplekse selskabskonstruktioner. De fylder derfor en del i statistikken på underretningerne og dækker derved over de reelle bagmænd. Hvidvasksekretariatet udgiver kvartalsrapporter, hvor nye tendenser inden for hvidvask beskrives. Der deles desuden viden med politikredsene i form af information om potentielle kriminelle aktører, som er måludpeget ud fra flere kriterier på baggrund af de underretninger, som Hvidvasksekretariatet modtager.

Da der er internetadgang i stort set hele verden, og da mange processer hos myndighederne i Danmark er gjort digitale, ses det ofte, at kriminelle befinder sig i andre lande, imens kriminaliteten begås. Det medvirker til, at det er sværere for politiet at efterforske og for anklagemyndigheden at retsforfølge forbryderne. Det kan desuden være svært at afdække, hvem der reelt begår kriminalite-

ten, hvorfor det er vigtigt, at de underretningspligtige bidrager med deres oplysninger til at belyse området.

Nuværende kriminalitetstendenser

I Danmark ses der generelt et fald i kriminaliteten de seneste år, og især ungdomskriminalitet er faldet støt fra 25.125 mistanker/sigtelser i 2006 til 11.487 mistanker/sigtelser i 2016 (Kylvsgaard 2017). Til trods for det generelle fald i kriminaliteten er der siden 2016 sket en stigning i alle former for internetrelateret kriminalitet og berigelseskriminalitet, primært i form af (identitets)tyveri og misbrug af betalingskort. Det formodes, at det kun er omkring 36% af al internetrelateret berigelseskriminalitet, der anmeldes til politiet. Misbrug af betalingskort er den hyppigst anmeldte forbrydelse, men der er sandsynligvis et stort mørketal på området (Politi 2017).

Ifølge Politiets Nationale strategiske analyse (2017) ses der en signifikant stigning i antallet af anmeldelser om bedrageri fra ca. 8.000 anmeldelser i 2009 til ca. 44.000 anmeldelser i 2016. Her lægges bl.a. til grund, at handlen på internettet er steget markant i perioden, hvilket naturligvis har en indvirkning på stigningen i antallet af anmeldelser. I løbet af de første tre kvartaler i 2016 indrapporterede danske banker 970 tilfælde til FinansDanmark, hvor cyberkriminelle havde forsøgt at få adgang til danske netbanker ved at lokke oplysningerne fra bankkunder (Forsvarets Efterretnings-tjeneste 2017).

Københavns Politi har i samarbejde med resten af landets politikredse taget konsekvensen af den stigende internetrelaterede kriminalitet, og åbner i efteråret 2018 et nyt center, som får navnet Landsdækkende Center for IT-relateret Økonomisk Kriminalitet (LCIK). Centeret er oprettet med det formål at skabe et bedre overblik over udviklingen på området. Samtidig vil anmeldelse og visitation af alle sager, uanset hvor i landet gerningsstedet er, have opstart i centeret. Det er en nødvendighed med mere samling og ensretning i behandling af sagerne for at imødekomme det voksende antal af anmeldelser inden for kreditkortbedrageri, phishing, smishing, sextortion og BEC/CEO fraud på nettet.

IPR kriminalitet omhandler overtrædelse af lovgivning inden for ophavsretsloven, varemærkeloven, designloven, patentloven og distribution af produkter og ydelser. De hyppigst sete forbrydelser er salg af falske mærkevarer på sociale medier (Facebook) og ulovlig streaming af tv-kanaler, film eller serier. Det er en af de nyere kriminalitetsformer, og efter en periode med en forsøgsordning er der oprettet en central afdeling, som er forankret hos Statsadvokaten for Særlig Økonomisk og International Kriminalitet, hvor alle IPR sager behandles (Anklagemyndigheden 2018). Samling af sagerne skal sikre en bedre koordinering og efterforskning og give mulighed for at afdække eventuelle nye tendenser og trends.

Skatte- og momssvig, ulovligt arbejde, socialt bedrageri og hvidvask er sagskategorier, der ofte ses at hænge sammen i større og mere komplekse konstruktioner. Især sager om hvidvask via ulovligt arbejde, primært indenfor servicebranchen (rengøring, restauration mv.) ses hyppigt hos både politiet og skattemyndigheden. Herunder hører også risikoen for menneskehandel, som ligeledes er nævnt i afsnittet om omverdensforhold. Ifølge National strategisk analyse som Politiet (2017) udgiver, er antallet af anmeldelser om grov skatte- og momssvig mere end fordoblet i perioden 2009-2016. Idet antallet af anmeldelser afspejler myndighedernes indsats på området, er det vanskeligt at udtale sig om den reelle udvikling, da dette ikke nødvendigvis afspejler omfanget af kriminaliteten.

Som tidligere nævnt er brug af stråmænd, som er tilrejsende fra udlandet og opholder sig kortvarigt i Danmark, en tendens, der ses i relation til hvidvask og skatte- og momssvig. Det er ofte stråmænd fra Syd- eller Østeuropa, som rejser til Danmark for at få oprettet NemID og konto i en bank, hvorefter de forsvinder sporløst. De stifter virksomheder der ofte drives i en kort periode, hvor de drænes for økonomiske værdier og derefter erklæres konkurs. Der foregår ofte fiktiv fakturering til og fra virksomhederne som et led i hvidvaskkriminaliteten.

I Danmark er det både nemt og billigt at oprette og registrere en virksomhed. Siden 1. januar 2014 har det været muligt at oprette et iværksætterselskab (IVS), som er en særlig type anpartsselskab, hvor der gælder relativt lempelige regler i forhold til startkapital, hæftelse, revisionspligt m.m. Registreringsgebyret i forbindelse med oprettelse af selskabsformerne anpartsselskab (ApS) og IVS koster 670 kr. Herudover er der et krav om en startkapital på minimum 50.000 kr. ved etablering af et ApS, mens kravet kun er 1 kr. for et IVS⁷. Siden indførelsen af IVS'er har antallet af nye selskabsregistreringer været støt stigende, og for første halvår 2017 udgjorde nyetablerede IVS'er 39% af det samlede antal etablerede selskaber (Dansk Erhverv, Experian og Danske Revisorer 2017). Ca. halvdelen af de nyoprettede IVS'er er tilknyttet Hovedstadsområdet. Når et IVS er etableret, kan det efterfølgende omdannes til et ApS, såfremt visse betingelser er opfyldt. Dette er dog ikke et krav eller en forpligtelse, men blot en option til ejeren af IVS'et. En analyse fra Dansk Erhverv, Experian og Danske Revisorer (2017) viser, at et fåtal af IVS'erne bliver omregistreret til et ApS. For anpartsselskaber, herunder IVS'er, gælder herudover, at ejerne ikke hæfter personligt, da hæftelsen er begrænset til selskabets formue.

Revision kan være en kontrolinstans, da selskabet derved har en (uafhængig) revisor til at gennemgå selskabets regnskab, økonomi, struktur m.m. Udgangspunktet er, at selskaber skal have revideret deres regnskaber. Mindre selskaber kan dog fravælge revision, hvis de opfylder særlige betingelser vedrørende balancesum, nettoomsætning og antal medarbejdere. For offentliggjorte regnskaber pr. 30/6-2017 havde 3,9% af IVS'erne og 28,2% af ApS'erne fået revideret deres regnskaber (Dansk

⁷ Virksomheder dækker i denne forbindelse over alle typer af virksomheder og selskaber, mens selskaber dækker over selskabstyper uden personlig hæftelse, såsom IVS, ApS og A/S.

Erhverv, Experian og Danske Revisorer 2017). Bagsiden ved, at det er enkelt og billigt at oprette og drive eksempelvis et IVS kan være, at det er mere tilgængeligt og attraktivt for kriminelle aktører at udnytte denne selskabskonstruktion til hvidvask.

En analyse fra Erhvervsstyrelsen (2018) viser, at IVS'er i 2017 udgjorde omtrent 12 % af nye momsregistreringer, mens de samtidigt udgjorde ca. 33 % af de potentielle svigsvirksomheder, som af Skatteforvaltningen blev nægtet registrering efter skatte- og afgiftslovgivningen. Dog skal det bemærkes, at der fra myndighedernes side har været et øget fokus på nyoprettede IVS'er, og dette kan føre til, at kriminelle aktører i stedet overtager og omregistrerer allerede aktive selskaber. Dette vækker ikke umiddelbart samme grad af mistanke hos myndighederne, hvorfor selskabet potentielt kan udnyttes i en længere periode uden at komme i myndighedernes søgelys.

Fremadrettede kriminalitetstendenser

Center for Cybersikkerhed ved Forsvarets Efterretningstjeneste beskriver følgende fire aktiviteter som værende de primære trusler inden for IT-relateret kriminalitet; spionage via internettet, berigelseskriminalitet via internettet, aktivistiske aktioner via internettet og terrorhandlinger via internettet (Forsvarets Efterretningstjeneste 2017). Desuden ses hacking, primært cyberspionage, som en af de største trusler både nu og i fremtiden for Danmark.

Spionage og hacking begås både mod statslige/offentlige aktører og private selskaber. Truslen vurderes at være høj, og især Ransomware og DDoS angreb er populære metoder. Der har hidtil udelukkende været tale om tyveri af viden eller afpresning af penge og ikke risiko/fare for menneskeliv. I takt med teknologiens udvikling kan hacking af selvkørende biler eller andet udstyr, som opererer via wifi eller bluetooth, føre til fare for personers liv og helbred.

Det vil formentligt fortsat være de ovenfor nævnte tendenser som IPR, hacking og bedrageri, der vil gøre sig gældende inden for både økonomisk og internetrelateret kriminalitet. Der er også risiko for, at det fremadrettet vil være attraktivt at benytte virtuel valuta til hvidvask af udbytte fra kriminalitet, men på nuværende tidspunkt er det ikke set i mange sager. Virtuel valuta er stadig ikke anerkendt som brugbar valuta i det danske økonomiske system, hvorfor det stadig er relativt risikobetonet at anvende denne metode til hvidvask.

Fysisk transport af valuta er ligeledes en hvidvasktendens, som forventes at være stigende fremadrettet. Årsagen hertil er, at den finansielle sektor og de andre underretningspligtige bliver bedre til at efterleve deres registrerings- og underretningsforpligtigelser og derved gør det vanskeligere ubemærket at føre illegitime midler gennem det finansielle system.

Stråmandsselskaber og udenlandske direktører forventes at fylde i kriminalitetstendenserne fremadrettet, idet det er relativt nemt at oprette både NemID, selskaber og bankkonti med tilhørende kreditkort og netbank i Danmark. Dette vil dog blive påvirket af styrket myndighedssamarbejde og politiets egen indsats på området.

8. Fældende afgørelser for hæleri

Som nævnt i afsnittet ”Hvad er hvidvask?” var hvidvask indtil 1. juli 2018 ikke selvstændigt kriminaliseret, hvorfor hvidvask i udgangspunktet enten skulle straffes som en del af førforbrydelsen eller under hæleribestemmelsen i straffelovens § 290. For at afdække omfanget af hvidvasksager under straffelovens § 290 er der foretaget en analyse af fældende afgørelser for hæleri i 2016. Formålet med analysen er desuden, i det omfang det er muligt, at konkludere, hvilke førforbrydelser til hvidvask der har været tale om i de indhentede sager.

Metode

SØIK har via politiets sagsstyringssystem (POLSAS) indhentet alle sager med afgørelsesdato i 2016, som er afgjort med følgende gerningskoder: 76601 (Hæleri), 76602 (Hæleri - groft/forretningsmæssig), 76611 (Hæleri med hensyn til narkotika), 76612 (Hæleri med hensyn til narkotika – groft) og 76621 – (Hæleri med hensyn til våben/ammunition) 76622 (Hæleri med hensyn til våben/ammunition - groft). Herefter har SØIK, med hjælp fra Rigsadvokaten, rekvireret de relevante afgørelser (primært bødeforlæg og domme) fra politikredsene. Det skal bemærkes, at metoden er forbundet med en vis usikkerhed. Årsagen er, at det alt andet lige kræver, at datakvaliteten er tilstrækkelig og at POLSAS er opdateret med de korrekte gerningskoder. Gerningskoderne skal være tilført, når der er faldet afgørelse i en sag eller et sagskompleks. I tillæg til de indhentede sager fra POLSAS har SØIK bidraget med 3 sager, som vedrører 5 personer og 3 virksomheder.

På baggrund af de indhentede sager er dommene blevet gennemlæst, analyseret og vurderet ud fra en række objektive kriterier (fx antal forhold, afgørelsestype, strafflængde m.m.), for at kunne lave en deskriptiv analyse af de fældende afgørelser for hæleri i 2016. Derudover er der foretaget en subjektiv vurdering af, om sagerne indeholder elementer af hvidvask, og i givet fald hvilken hvidvaskkanal, der blev anvendt. På baggrund af listen af identificerede risikoområder, som den fremstod efter identifikationsfasen i 2017, er der foretaget en vurdering af, hvilken hvidvaskkanal der er anvendt i de indhentede sager.

Analyse

SØIK har indhentet oplysninger om 875 sager, der i 2016 førte til mindst én fældende afgørelse for overtrædelse af straffelovens § 290 om hæleri.

Sagerne angår 1.032 personer og tre virksomheder.⁸ Fordelingen af de involverede aktører ses af Tabel 3.

⁸ I alt 20 personer blev dømt for hæleri to gange i 2016, hvoraf antallet af unikke personer er 1.013.

Tabel 3. Personer og virksomheder, indgår i afgørelser om hæleri

Køn/ virksomhed	Antal
Mand	955
Kvinde	77
Virksomhed	3
I alt	1035

Hæleriafgørelser

Langt størstedelen (90%) af personerne er dømt for hæleri efter § 290, stk. 1, mens de resterende 10% af personerne samt de tre virksomheder er dømt for hæleri af særlig grov beskaffenhed, jf. § 290, stk. 2. Der er ligeledes 19 tilfælde, hvor en person er dømt for mindst et forhold af § 290, stk. 1, og mindst et forhold vedrørende hæleri af særlig grov beskaffenhed, jf. straffelovens § 290, stk. 2. Denne fordeling ses af Tabel 4

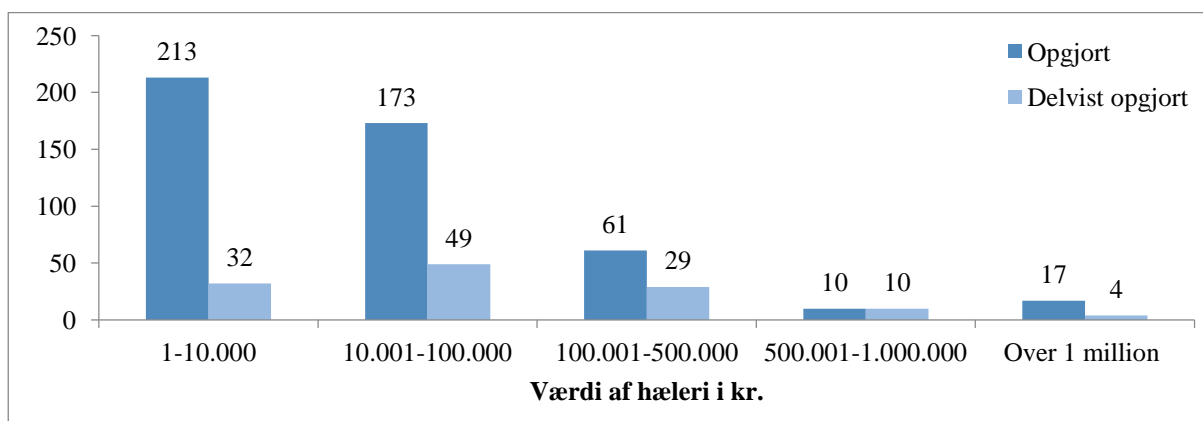
Tabel 4. Personer og virksomheder fordelt efter hæleriforholdet i afgørelsen

Afgørelse	Antal
§ 290, stk. 1	919
§ 290, stk. 2	97
§ 290, stk. 1 og 2	19
I alt	1035

Hæleriværdi

I mange af sagerne er værdien af hæleriet opgjort fuldt eller delvist. Der er stor forskel på værdien af det opgjorte, der spænder fra få hundrede kroner til mange millioner kroner. Dette vidner om stor forskel på sagernes omfang og karakter. Flere af afgørelserne med høj opgjort værdi af hæleriet har forbindelse til valutavekslingskontorer, hvor der er tale om egentlig hvidvask af midler, hidrørende fra kriminalitet. Det samme mønster afspejles også i bødestørrelserne, jævnfør Tabel 8. Hæleriværdien er illustreret i Figur 3

Figur 3. Antal personer og virksomheder fordelt efter værdien af hæleriet



I 31 sager er det nævnt, at hæleriet er af erhvervsmæssig eller professionel karakter, hvilket specifikt nævnes som skærpende omstændighed i forhold til straffelovens § 290, stk. 2. I 14 af sagerne er det nævnt, at hæleriet omhandler transport af midler til og fra udlandet.

Sagernes forhold

Det fremgår endvidere af sagerne, at 165 personer er dømt efter anklagerens subsidære påstand om hæleri, hvilket betyder at retten ikke har fundet det tilstrækkeligt bevist, at personen er skyldig i den principale tiltale i et forhold. Subsidære tiltaler forekommer i knap 2 ud af 3 tilfælde i forhold til afgørelser, hvor personerne er dømt for mindst et forhold af tyveri, jf. straffelovens § 276. Herudover fremgår det, at 130 personer tidligere er dømt for hæleri, hvilket især har relevans i forhold til udmåling af straf.

Det bemærkes, at personerne og virksomhederne oftest er dømt for mere end ét kriminelt forhold i samme sag. De øvrige forhold vedrører typisk andre lovovertrædelser end hæleri, herunder primært tyveri eller andre formueforbrydelser. Se denne fordeling i Tabel 5.

Tabel 5. Antal personer og virksomheder fordelt efter antallet af forhold⁹

Antal forhold i afgørelsen	Samtlige forhold	Hæleriforhold
1	282	708
2-5	341	244
6-20	313	74
21-50	87	5
51-100	8	0
+100	2	2
I alt	1033	1033

Afgørelsestype

Ovennævnte forhold påvirker selvsagt afgørelsestypen, der derfor sjældent kun er et udtryk for straffen for hæleriforholdene i sagerne. Tilsvarende gælder for strafflængden og/eller bødestørrelsen. Hæleriforholdet udgør i gennemsnit kun ca. 1/3 af det samlede antal forhold, der indgår i de domme, som er blevet analyseret. Se fordelingen efter afgørelsestype i Tabel 6.

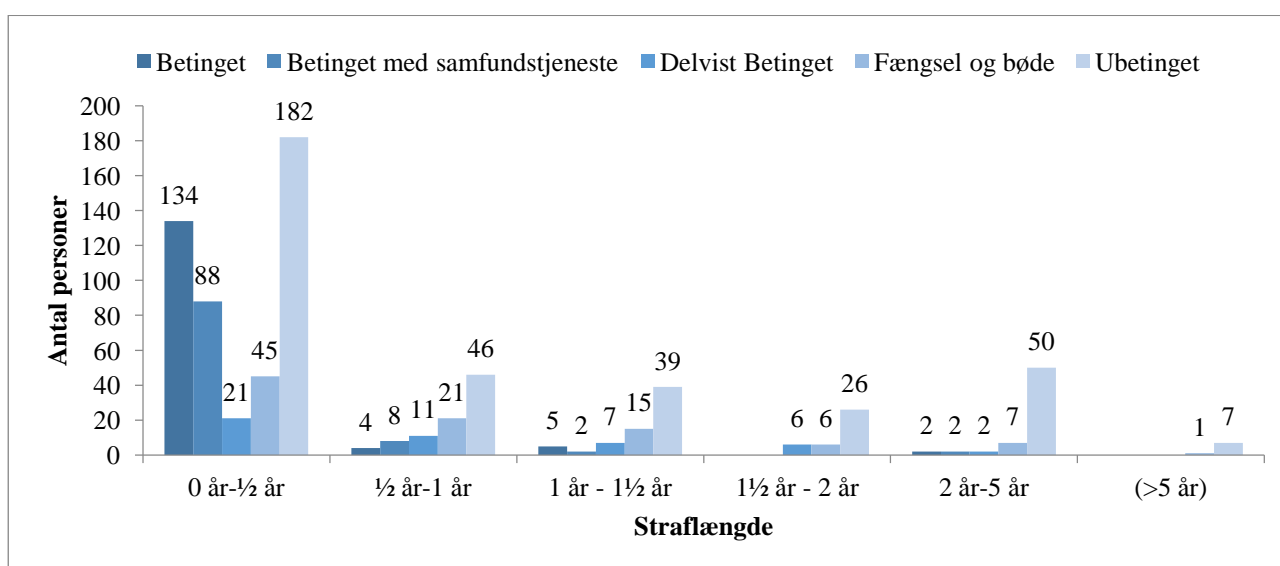
⁹ Der er 2 tiltalefrafald hvor der ikke er registret nogen forhold (0 forhold), disse er dog udeladt fra tabellen

Tabel 6. Personer og virksomheder fordelt efter afgørelsestype¹⁰

Afgørelsestype	Antal
Ubetinget	350
Ubetinget og bøde	95
Delvist betinget	47
Betinget	147
Betinget med samfundstjeneste	101
Bøde	267
Tiltalefrafald	3
I alt	1010

Straflængden er i dommene angivet i dage, måneder og år, alt efter straffens længde og karakter. For at få en sammenlignelig straffelængde på tværs af dommene, er dommene konverteret til dage, hvor 1 måned er lig med 30 dage, og et år er lig med 12 måneder (360 dage).¹¹ For delvist betingede domme er det den samlede straffelængde, der er angivet, og ikke den betingede del. I Figur 4 ses fordelingen på straffelængde og afgørelsestype.

Figur 4. Personer fordelt efter afgørelsestype og straffelængde



Langt størstedelen af de fængselsstraffe, der er idømt i sager, hvor der har været mindst et hæleri-forhold, er på under 180 dages fængsel (lig med ½ år). I de sager, hvor hele straffen er ubetinget, gælder det for lidt mere end halvdelen af de dømte, at de har fået en fængselsstraf på under 180 da-

¹⁰ De resterende 25 dækker blandt andet over sager hvor der er faldet dom, men hvor den tiltalte er uegnet til straf (behandlingsdom). Der ses også sager hvor der er givet en advarsel, eller hvor der ikke er nogen tillægsstraf, i forhold til tidligere afsagt dom i samme sagskompleks.

¹¹ Metoden er i overensstemmelse med Danmarks Statistiks metode vedrørende måling af straffelængde i deres statistikker vedrørende domme.

ge. Blandt de 8 personer, der er idømt fængselsstraffe over 5 år, er en direktør fra et valutavekslingskontor samt en person, som er dømt for omfattende overførsler til en pengeoverførselsvirksomhed.

Bødestørrelser

I Tabel 7 ses fordelingen af bødestørrelser. I tabellen indgår selvsagt kun de personer og virksomheder, som er pålagt en bødestraf, eventuelt kombineret med en fængselsstraf. Det samlede antal personer og virksomheder der har modtaget en bøde er 419. Den hyppigst udelte bødestørrelse er 1.501 kr. – 5.000 kr., mens der er meget få personer og virksomheder, som er idømt bøder på mere end 100.000 kr.

Tabel 7. Personer og virksomheder fordelt efter bødestørrelse

Bødestørrelse	Antal
500-1.500	52
1.501-5.000	191
5.001-10.000	85
10.001-25.000	56
25.001-100.000	27
100.001-1.000.000	2
Over 1 million	6
I alt	419

Hvidvaskkanaler

Som beskrevet i metodel delen er der foretaget en vurdering af, om sagerne indeholder et element af hvidvask, samt hvilken hvidvaskkanal der er benyttet. Nedenstående Tabel 8 viser en samlet oversigt over antallet af sager fordelt på hvidvaskkanal.

Tabel 8. Sager fordelt efter anvendt hvidvaskkanal

Hvidvaskkanal	Antal
Høj-værdi-varer	92
Pengeinstitutter	24
Pengeoverførselsvirksomheder	13
Handelsbaseret hvidvask	3
Valutavekslingsvirksomhed	2
I alt	134

Sammenfatning af hæleridomme

På baggrund af de indhentede 875 sager er det vurderet, at der i alt i 134 sager indgår et element af hvidvask. Langt de fleste af disse sager vedrører høj-værdi-varer. På trods af, at der er vurderet at være et element af hvidvask, handler mange af sagerne om besiddelse af tyvekoster. Dermed er høj-

værdi-varerne, i de fleste tilfælde, ikke brugt som metode til egentlig hvidvask af midler, som stammer fra en strafbar handling. De fleste af disse sager omhandler besiddelse af tyvekoster af høj værdi, som kan være erhvervet for kriminelle midler. Der er på den baggrund kun meget få af det samlede antal sager, som har et egentligt element af hvidvask. De sager, hvor der har været et element af hvidvask, er inddraget de steder i risikovurderingen, hvor det har været relevant.

I et forsøg på at kvantificere, hvilke førforbrydelser der har ført til dom for hvidvask, er der indhentet informationer om, hvad de andre forhold i dommene handler om. I praksis har det dog vist sig, at der i mange tilfælde ikke er sammenhæng mellem sagernes andre forhold og hæleriforholdet. Dette skyldes, at personer eller virksomheder, som modtager en dom for hæleri, ofte også er dømt for andre ikke nødvendigvis beslægtede forhold f.eks. narkotikakriminalitet, jf. straffelovens § 191, som det også er nævnt under analysen af afgørelsestype. Overordnet er det derfor ikke på baggrund af dommene muligt at konkludere, hvilke førforbrydelser der ligger til grund for et eventuelt hvidvaskforhold.

Der er enkelte sager, hvor hvidvask er straffet under straffelovens hæleribestemmelse § 290. Analysen af risikoområderne har ligeledes vist, at i sager der indeholder et element af hvidvask, er det ofte i forbindelse med førforbrydelsen, f. eks. databedrageri eller narkotikakriminalitet, at der er sket domfældelse. Det er for nuværende ikke muligt at udskille disse sager i politiets systemer. Dette skyldes bl.a. registreringspraksis, som kun gør det muligt at søge på gerningskoder (ofte kun en per sag eller sagskompleks), eller resumeet (sagens genstand), som politiet selv udfylder. Derudover er der søgenøgler, som kan tilknyttes til sagerne. Dog har der hidtil ikke været ret mange af disse, som er relevante i forhold til hvidvask.

9. Analyse og vurderinger (ikke offentligt tilgængelige)

Indholdet af analyserne, som angiver konkrete metoder og vurderer omfang, tilgængelighed, attraktivitet, opdagelsesrisiko samt sandsynlighed for retsforfølgelse og dom for hvert af de identificerede risikoområder, er her udtaget af hensyn til risikoen for, at disse indsigter kan misbruges.

Det identificerede og analyserede risikoområder inkluderer blandt andet:

- **Pengeoverførselsvirksomheder og alternative pengeoverførere**
- **Valutavekslingsvirksomheder**
- **Legale virksomhedskonstruktioner**
- **Fysisk transport af valuta over landegrænser**
- **Spilsektoren**
- **Pengeinstitutter**
- **Betalingsinstitutter og e-penge**
- **Kryptovaluta**
- **Fast ejendom**
- **Høj-værdi-varer**
- **Leasing**
- **Udbydere af tjenesteydelser til virksomheder (service providers)**
- **Rådgivere (advokater, revisorer, skatterådgivere og eksterne bogholdere)**

10. Litteratur

Advokatsamfundet. 2017. ”Advokatrådets vejledning om hvidvaskloven”. Advokatsamfundet, tilgået 18. oktober, 2018, https://www.advokatsamfundet.dk/Advokatregulering/Hvidvask/~/_media/Hvidvask/VEJLEDNING%20TIL%20HVIDVASKLOVEN%202017.ashx

Andersen, L. H., m.fl. 2017. *Danskernes liv med skatter, sort arbejde og gør det selv-arbejde*. Odense: Syddansk Universitetsforlag – med støtte fra Rockwool Fonden.

Anklagemyndigheden. 2018. ”Styrket indsats over for retligheds kriminalitet bliver samlet hos SØIK”. Anklagemyndigheden, tilgået 18. oktober, 2018, <https://www.anklagemyndigheden.dk/da/styrket-indsats-over-rettigheds-kriminalitet-bliver-samlet-hos-soik>

Basel Institute of Governance. 2016. ”Basel AML Index 2016”. International Centre for Asset Recovery, tilgået 18. oktober, 2018, https://index.baselgovernance.org/sites/index/documents/Basel_AML_Index_Report_2016.pdf

Betalingsrådet. 2016. ”Rapport om nye aktører på betalingsområdet”. Nationalbanken, tilgået 18. oktober, 2018, <https://www.nationalbanken.dk/da/publikationer/Documents/2016/08/Rapport%20om%20nye%20akt%C3%B8rer%20betalingsmarkedet.pdf>

CoinMarketCap. 2018. ”Top 100 Cryptocurrencies by Market Capitalization”. CoinMarketCap, tilgået 13. september, 2018, www.coinmarketcap.com

Danmarks Statistik. 2017. ”Mobilen er den foretrukne enhed til internetadgang”. Danmarks Statistik, tilgået 18. oktober, 2018, <https://www.dst.dk/da/Statistik/nyt/NytHtml?cid=24235#>

Danmarks Statistik. 2018. ”Fortsat stigning i beskæftigelsen”. Danmarks Statistik, tilgået 18. oktober, 2018, <https://www.dst.dk/da/Statistik/nyt/NytHtml?cid=26718>

Dansk Erhverv, Experian og Danske Revisorer. 2017. ”Analyse af Iværksætterselskaber”. Dansk Erhverv, tilgået 18. oktober, 2018, <https://www.danskerhverv.dk/siteassets/mediafolder/downloads/fakta/analyse-af-iværksætterselskaber-juli-2017>

De Økonomiske Råd. 2017. ”Dansk økonomi, forår 2017”. De Økonomiske Råd, tilgået 18. oktober, 2018, <https://dors.dk/vismandsrapporter/dansk-oekonomi-foraar-2017>

De Økonomiske Råd. 2018. ”Udenlandsk arbejdskraft bidrager til vores økonomiske velstand”. Altinget, tilgået 18. oktober, 2018, <https://www.altinget.dk/arbejdsmarked/artikel/de-oekonomiske-raad-udenlandsk-arbejdskraft-bidrager-til-vores-oekonomiske-velstand>

Den Europæiske Unions Tidende. 2015. “FORORDNINGER EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) 2015/847”. EUR-Lex, tilgået 18. oktober, 2018, <https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32015R0847&from=PT>

Den Europæiske Unions Tidende. 2018. “DIREKTIVER EUROPA-PARLAMENTETS OG RÅDETS DIREKTIV (EU) 2018/843”. EUR-Lex, tilgået 18. oktober, 2018, <https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32018L0843&from=EN%20>

Det Europæiske Råd. 2018. ”Kontrol med likvide midler, der føres ind i eller ud af EU: Rådet godkender aftale”. Det Europæiske Råd, tilgået 18. oktober, 2018, <http://www.consilium.europa.eu/da/press/press-releases/2018/06/27/controls-on-cash-entering-and-leaving-the-eu-council-endorses-agreement/>

DR. 2018. ”Nyt supervåben i politiet: Mand pågrebet for to voldtægter”. DR, tilgået 18. oktober, 2018, <https://www.dr.dk/nyheder/indland/nyt-supervaaen-i-politiet-mand-paagrebet-voldtaegter>

Elmark, Nils. 2017. ”Kun en tåbe frygter ikke neobankerne”. Finansforbundet, tilgået 18. oktober, 2018, <https://www.finansforbundet.dk/da/nyheder-aktuelt/Sider/Kunentaabefrygterikkeneobankerne.aspx>

Erhvervsministeriet. 2016. ”Troels Lund Poulsen strammer grebet om vekselkontorer”. Erhvervsministeriet, tilgået 18. oktober, 2018, <https://em.dk/nyheder/2016/16-09-14-troels-lund-poulsen-strammer-grebet-om-vekselkontorer>

Erhvervsministeriet. 2018. ”Ny hvidvaskaftale bringer bødeniveauet i Danmark i den absolutte top i Europa og effektiviserer tilsynet med bankerne”. Erhvervsministeriet, tilgået 18. oktober, 2018, <https://em.dk/nyheder/2018/09-19-hvidvaskstrategi>

Erhvervsstyrelsen. 2017. ”Reelle ejere”. Erhvervsstyrelsen, tilgået 18. oktober, 2018, <https://erhvervsstyrelsen.dk/reelle-ejere>

Erhvervsstyrelsen. 2018. ”Analyse af iværksætterselskaber 2018”. Erhvervsstyrelsen, tilgået 18. oktober, 2018, https://erhvervsstyrelsen.dk/sites/default/files/media/analyse_af_ivaerksaetterselskaber.pdf

EU-Kommissionen. 2017. “Report from the Commission to the European Parliament and the Council – on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities – Annex SNRA Part 2”. EU-Kommissionen, tilgået 18. oktober, 2018, http://ec.europa.eu/newsroom/document.cfm?doc_id=45653

EU-Kommissionen. 2018. “Strengthened EU rules to prevent money laundering and terrorism financing”. EU-Kommissionen, tilgået 18. oktober, 2018, http://ec.europa.eu/newsroom/just/document.cfm?action=display&doc_id=48935

European Banking Authority. 2014. “EBA Consumer Trends Report 2014”. EBA, tilgået 18. oktober, 2018, <http://www.eba.europa.eu/documents/10180/534414/EBA+Consumer+Trends+Report+2014.pdf>

Europol. 2015. “Why cash is still king”. Europol – Financial Intelligence Group, tilgået 18. oktober, 2018, <https://www.europol.europa.eu/sites/default/files/documents/europolcik%20%281%29.pdf>

Europol. 2017. “SOCTA – European Union, Serious and Organised Crime Threat Assessment, Crime in the age of technology”. Europol - Den Europæiske Union, tilgået 18. oktober, 2018, https://www.europol.europa.eu/sites/default/files/documents/socta2017_0.pdf

FATF. 2010. ”Money Laundering through Money Remittance and Currency Exchange Providers”. FATF, tilgået 18. oktober, 2018, [http://www.fatf-ga-
fi.org/media/fatf/ML%20through%20Remittance%20and%20Currency%20Exchange%20Providers
.pdf](http://www.fatf-gafi.org/media/fatf/ML%20through%20Remittance%20and%20Currency%20Exchange%20Providers.pdf)

FATF. 2013a. “The role of Hawala and other similar service providers in money laundering and terrorist financing”. FATF, tilgået 18. oktober, 2018, [http://www.fatf-
gafi.org/media/fatf/documents/reports/Role-of-hawala-and-similar-in-ml-tf.pdf](http://www.fatf-gafi.org/media/fatf/documents/reports/Role-of-hawala-and-similar-in-ml-tf.pdf)

FATF. 2013b. ”National Money Laundering and Terrorist Financing Risk Assessment”. FATF, tilgået 18. oktober, 2018, [http://www.fatf-ga-
fi.org/media/fatf/content/images/National_ML_TF_Risk_Assessment.pdf](http://www.fatf-gafi.org/media/fatf/content/images/National_ML_TF_Risk_Assessment.pdf)

FATF. 2013c. ”Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals”. FATF, tilgået 18. oktober, 2018, [http://www.fatf-
ga-
fi.org/media/fatf/content/images/Vulnerabilities_of_Legal_Professionals.pdf](http://www.fatf-gafi.org/media/fatf/content/images/Vulnerabilities_of_Legal_Professionals.pdf)

fi.org/media/fatf/documents/reports/ML%20and%20TF%20vulnerabilities%20legal%20professionals.pdf

FATF. 2015a. "Money Laundering Through the Physical Transportation of Cash". FATF, tilgået 18. oktober, 2018, <http://www.fatf-gafi.org/media/fatf/documents/reports/money-laundering-through-transportation-cash.pdf>

FATF. 2015b. "Guidance for a risk-based approach to virtual currencies". FATF, tilgået 18. oktober, 2018, <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf>

FATF. 2017. "Anti-money laundering and counter-terrorist financing measures – Denmark – "Mutual Evaluation Report". FATF, tilgået 18. oktober, 2018, <http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-Denmark-2017.pdf>

FATF. N.d. "Money Laundering". FATF, tilgået 18. oktober, 2018, <http://www.fatf-gafi.org/faq/moneylaundering/>

Finans Danmark. 2017. "Transaktioner - Se statistik på straksbetalinger og intradagstraktioner herunder". Finans Danmark, tilgået 18. oktober, 2018, <https://finansdanmark.dk/toerretal/institutter-filialer-ansatte/betalinger/transaktioner/>

Finans Danmark. 2018. "Ny hvidvaskstrategi og task force vil opruste indsatsen". Finans Danmark, tilgået 18. oktober, 2018, <https://www.finansdanmark.dk/nyheder/2018/ny-hvidvaskstrategi-og-task-force-vil-opruste-indsatsen/>

Finanssektorens Uddannelsescenter. 2014. "Digitale tendenser i finanssektoren – Neobanker". Finanssektorens Uddannelsescenter, tilgået 18. oktober, 2018, <http://ipaper.ipapercms.dk/FinansUdd/FUbrochurer/Digitaletendenser2014/Neobanker/?page=1>

Finanstilsynet. 2018. "Pengeinstitutternes størrelsesgruppering – Pengeinstitutterne fordelt efter størrelse 2018". Finanstilsynet, tilgået 18. oktober, 2018, <https://www.finanstilsynet.dk/~media/Tal-og-fakta/2017/Gruppeopdeling2018-xlsx.xlsx?la=da>

Forsvarets Efterretningstjeneste. 2017. "Trusselsvurdering – Cybertruslen mod Danmark". Forsvarets Efterretningstjeneste, Trusselsvurderingsenheden ved Center for Cybersikkerhed, tilgået 18. oktober, 2018, <https://fe-ddis.dk/cfcs/cfcsdocuments/cybertruslen%20mod%20danmark.pdf>

Kruize, Peter. 2018. ”Internetkriminalitet 2017 – Offerundersøgelse om identitetstyveri, bedrageri, afpresning og chikane i cyberspace”. Det Juridiske Fakultet, Københavns Universitet og Det Kriminalpræventive Råd, tilgået 18. oktober, 2018, <https://dkr.dk/media/13026/internetkriminalitet-2017-final.pdf>

Kyvsgaard, Britta. 2017. ”Udviklingen i børne- og ungdomskriminalitet 2006-2016”. Justitsministeriets Forskningskontor, tilgået 18. oktober, 2018, http://justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningsrapporter/2017/rapport_udviklingen_i_boerne_og_ungdomskriminalitet_2006-2016.pdf

Laursen, Anders & Kyed, Jon Hasling. 2014. Virtuelle valutaer. Danmarks Nationalbank, tilgået 18. oktober, 2018, http://www.nationalbanken.dk/da/publikationer/Documents/2014/03/Virtuelle_KVO1_2014.pdf

OECD. 2016. “States of Fragility 2016: Understanding Violence”. OECD, tilgået 18. oktober, 2018, http://www.keepeek.com/Digital-Asset-Management/oecd/development/states-of-fragility-2016_9789264267213-en#.WRnEfLtdC70#page8

Pedersen, Rene. 2017. ”IOT-producenterne er fuldstændig ligeglade med sikkerhed”. IDA Universe, tilgået 18. oktober, 2018, <https://universe.ida.dk/artikel/iot-producenterne-er-fuldstaendig-ligeglade-med-sikkerhed-35415/>

Politi. 2017. ”National strategisk analyse 2017”. Politi, tilgået 18. oktober, 2018, https://www.politi.dk/NR/rdonlyres/60D84675-DFA7-46FE-BDEC-6FE6545FC8AF/0/Rapport_NSA17_enkeltsider.pdf

Regeringen. 2016. ”Aftale om Danmarks tilknytning til Europol efter 1. maj 2017”. Regeringen, tilgået 18. oktober, 2018, <https://www.regeringen.dk/media/2740/aftale-om-europol-pdf.pdf>

Rockwool Fonden Forskning. 2018. ” Bag beskæftigelsesrekorden: Arbejdsmarkedets kernetropper fortsat langt under 2008-niveau”. Rockwool Fonden Forskning, tilgået 18. oktober, 2018, <https://www.rockwoolfonden.dk/app/uploads/2018/03/Kort-Nyt-Marts-2018-Bag-beskaeftigelsesrekorden.pdf>

Savona Ernesto U. & Riccardi Michele. 2015. ”From illegal markets to legitimate businesses: The Portfolio of Organised Crime in Europe”. Final Report of Project OCP – Organised Crime Portfolio, tilgået 18. oktober, 2018, <http://www.transcrime.it/wp-content/uploads/2015/12/ocp.pdf>

SKAT. 2017. "Kontrolaktiviteter i 2017 - Styrket regelefterlevelse på skatteområdet". SKAT, tilgået 18. oktober, 2018, www.skat.dk/getFile.aspx?id=133852

Skatteforvaltningen. N.d. "Om Skatteforvaltningen". Skatteforvaltningen, tilgået 18. oktober, 2018, <https://www.skatteforvaltningen.dk/om-skatteforvaltningen/>

Skatteministeriet. 2017. "Forslag til en stærkere myndighedsindsats mod organiseret svindel". Skatteministeriet, tilgået 18. oktober, 2018, <https://www.skm.dk/media/1554416/rapport-tvaerministeriel-arbejdsgruppe-moms-og-skattesvig.pdf>

Spillemyndigheden. 2018a. "Årsberetning 2017". Spillemyndigheden, tilgået 18. oktober, 2018, https://spillemyndigheden.dk/sites/default/files/filer-til-download/spillemyndigheden_-_aarsberetning_2017.pdf

Spillemyndigheden. 2018b. "Vejledning om væddemål og onlinekasino – Beskrivelse af krav til ansøgere til tilladelse om udbud af væddemål og onlinekasino". Spillemyndigheden, tilgået 18. oktober, 2018, https://spillemyndigheden.dk/sites/default/files/filer-til-download/vejledning_om_vaeddemaal_og_onlinekasino_-_juli_2018_.pdf

SØIK. 2015. "Hvidvask i Danmark – Den nationale risikovurdering 2015". Anklagemyndigheden, tilgået 18. oktober, 2018, <https://www.anklagemyndigheden.dk/sites/default/files/Documents/hvidvask-i-danmark-den-nationale-risikovurdering-%202015.pdf>

Sørensen, Catharina. 2018. "Retsforbehold kan blokere konfiskation af milliarder". Tænketanken Europa, tilgået 18. oktober, 2018, http://thinkeuropa.dk/sites/default/files/notat_retsforbehold_kan_blokere_konfiskation_af_milliardere.pdf

UBS. 2017. "Cryptocurrencies". UBS, Chief Investment Office Americas, Wealth Management, tilgået 18. oktober, 2018, <https://www.ubs.com/content/dam/WealthManagementAmericas/cio-impact/cryptocurrencies.pdf>

Udlændinge- og Integrationsministeriet. 2017. "Regeringen opretholder grænsekontrollen". Udlændinge- og Integrationsministeriet, tilgået 18. oktober, 2018, <http://uim.dk/nyheder/2017/2017-10/regeringen-opretholder-graensekontrollen>

Utrecht University. 2013. “The Economic and Legal Effectiveness of Anti-Money Laundering and Combating Terrorist Financing Policy”. Universiteit Utrecht, tilg et 18. oktober, 2018, [http://www2.econ.uu.nl/users/unger/ecolef_files/Final%20ECOLEF%20report%20\(digital%20version\).pdf](http://www2.econ.uu.nl/users/unger/ecolef_files/Final%20ECOLEF%20report%20(digital%20version).pdf)

Økonomi- og Indenrigsministeriet. 2018. ”Økonomisk Redegørelse - August 2018”. Økonomi- og Indenrigsministeriet, tilg et 18. oktober, 2018, https://oim.dk/media/20423/oekonomisk-redegoerelse-2-270818_web.pdf

Bilag 1: Begreber og definitioner

AIF/FAIF fonde: (Forvaltere af) Alternative investeringsfonde.

BEC/CEO fraud: (Business email compromise) Falske fakturaer eller falske e-mails, som synes ægte, sendes til den økonomiansvarlige eller bogholderen i et selskab. Afsender foregiver at være en chef eller en kollega, som beder medarbejderen om at betale fakturaen eller overføre et specifikt beløb til en nærmere anført konto, som tilhører den kriminelle.

Chip dumping: En eller flere pokerspillere i en turnering dumper deres chip hos en bestemt spiller (efter aftale), hvorved den ene spiller i turneringen har meget lav risiko og stor gevinst. Det kategoriseres som aftalt spil, men kan være svært at opdage.

DDos angreb: (Distributed denial of service) En hjemmeside overbelastes ved at en person styrer flere computer på én gang, og får dem til automatisk at forespørge den samme internetadresse i én uendelighed, således at hjemmesiden ikke kan benyttes.

E-wallet: en elektronisk pung, som giver mulighed for at udføre øjeblikkelige betalinger.

IPR: (Intellectual Property Rights) Kriminalitet, som omhandler krænkelse af mærkevarer (salg af falske mærkevarer) eller ulovlig streaming af tv-signal eller film.

Leasing (finansiel): Ved finansiel leasing er leasingtager ansvarlig for forhandling med leverandør og er, såfremt leasingaftalen indeholder en restværdi, ved leasinggivers påkrav forpligtet til ved leasingperiodens udløb at anviser køber til den leasede genstand. I finansiel leasing dækker leasingydelseerne tilbagebetaling af hele eller væsentligste dele af anskaffelsessummen.

Leasing: (operationel): Ved operationel leasing er leasinggiver ansvarlig for forhandling med leverandør og har risikoen for genstandens restværdi ved leasingperiodens udløb. Leasingydelseerne dækker ikke fuld tilbagebetaling af hele anskaffelsessummen.

Phishing: En svindler forsøger at franarre en persons brugernavn, adgangskode, kreditkort- eller bankoplysninger. Oftest foregår det ved, at brugeren får tilsendt en falsk mail som ser ud til at komme fra en virksomhed, som personen har tillid til. Personen afgiver frivilligt oplysningerne, uvidende om at det er en falske mail og at oplysningerne afgives til kriminelle personer, som efterfølgende misbruger dem.

Ransomware: En hjemmeside eller et IT-system infiltreres af en virus, der spærre eller krypterer al data. Ejeren afkræves derefter en løsesum i form af penge eller viden imod at data frigives igen.

Smishing: Phishing via SMS, hvor personen franarres koder, kortoplysninger eller lign.

Sextortion: Afpresning, hvor en gerningsmand har skaffet sig adgang til seksuelle billeder af en person, eller foregiver at have det. Gerningsmanden afpresser derefter vedkommende med at billederne offentliggøres, hvis vedkommende ikke betaler penge eller sender yderligere billeder til gerningsmanden.