

KVARTALS- RAPPORT

Hvidvasksekretariatet 2025

2



2. kvartal 2025

Kære samarbejdspartnere

I denne rapport kan du læse om, hvor mange underretninger Hvidvasksekretariatet modtog og videresendte i 2. kvartal 2025. Du kan læse om, hvordan de efterretningsoplysninger, som Hvidvasksekretariatet sender til Skatteforvaltningen, anvendes, og hvad de resulterer i. Herudover kan du læse om udvalgte sager om hvidvask, hvor der er rejst sigtelser eller faldet dom.

Der sker løbende nye tiltag på hvidvaskområdet. I dette kvartal er der vedtaget en lovændring, som betyder, at alle myndigheder i Danmark er underretningspligtige til Hvidvasksekretariatet. Internationalt har der været FATF-plenar, og såvel FATF's som EU's liste over risikolande er blevet opdateret. Det kan du læse mere om her.

For løbende at give de underretningspligtige et samlet overblik over lande, der fremgår af henholdsvis FATF's grå og sorte liste, samt EU-Kommissionens liste over højrisikotredjelande og ikkesamarbejdsvillige skattejurisdiktioner, har Hvidvasksekretariatet udarbejdet en samlet oversigt, som løbende vil blive opdateret. Oversigten kan findes på Hvidvasksekretariatets hjemmeside [her](#).

Europol har udgivet deres trusselsvurdering på området for organiseret internetkriminalitet, [Internet Organised Crime Threat Assessment 2025](#). Rapporten *Steal, deal and repeat: How cybercriminals trade and exploit your data* er en dybdegående analyse af, hvordan data er blevet kernen i en global, industrialiseret cyberkriminalitet, hvor cyberkriminelle aktører handler med og udnytter ulovlig adgang til data - herunder kommercialiserer disse varer og tjenester. Det har også konsekvenser på hvidvaskområdet, og særligt svindel med syntetiske medier kommer til at udfordre de kontrolprocesser, vi kender.

Hvidvasksekretariatet har fået ny leder. Erik Modin er tiltrådt, og ham kan du læse mere om her i rapporten.

God læselyst!

Med venlig hilsen

Hvidvasksekretariatet

Danmarks Finansielle Efterretningsenhed

Underretninger sendt til Hvidvasksekretariatet

I 2. kvartal 2025 modtog Hvidvasksekretariatet 23.330 underretninger. Det er et fald på 422 underretninger i forhold til 1. kvartal 2025, men knap 1.000 flere end i 2. kvartal 2024. Samlet set har Hvidvasksekretariatet modtaget flere end 94.500 underretninger det seneste år.

Tabel 1*. Antal underretninger sendt til Hvidvasksekretariatet i perioden fra 2. kvartal 2024 til og med 2. kvartal 2025.

Antal underretninger modtaget	2. kvartal 2024	3. kvartal 2024	4. kvartal 2024	1. kvartal 2025	2. kvartal 2025
I alt	22.395	24.045	23.436	23.752	23.330

*Tallene i tabellen er dynamiske og kan ændre sig fra kvartal til kvartal. Det skyldes, at der kan ske efterregistreringer for tidligere kvartaler, da den dato Hvidvasksekretariatet modtager underretningen, og den dato underretningen registreres i systemet, kan divergere.

De underretninger, Hvidvasksekretariatet modtager, fordeler sig på tre typer:

- *Suspicious Transaction Report (STR)*: Underretning om mulig hvidvask med transaktioner mellem personer eller selskaber, kontanthævninger eller kontantindsættelser.
- *Suspicious Activity Report (SAR)*: Underretning om mistænkelig aktivitet, adfærd eller hændelse, hvori der ikke indgår transaktioner.
- *Terror Financing Report (TFR)*: Underretning om mulig terrorfinansiering indeholdende mistænkelige transaktioner eksempelvis til og fra høj-risiko-lande.

Kategoriseringen af underretninger foretages af de underretningspligtige ud fra deres umiddelbare vurdering af mistanken. Ved modtagelse i Hvidvasksekretariatet foretages der screeninger på tværs, og selvom kategoriseringen er meget væsentlig for sekretariatets arbejde, er den ikke afgørende for oplysningernes anvendelse.

Fordelingen af underretninger på rapporttyper fremgår nedenfor. Antallet af underretninger om *mistænkelige transaktioner* (STR) udgør 19.028, svarende til cirka 82 pct. af alle underretningerne. Antallet er faldet med 938 i forhold til 1. kvartal 2025. Antallet af *underretninger om mistænkelige aktiviteter* (SAR) udgør 4.268 og udgør cirka 18 pct. Antallet er steget med 526 underretninger siden sidste kvartal. Antallet af *underretninger om mulig terrorfinansiering* (TFR) er faldet med ti underretninger i forhold til 1. kvartal 2025.

Sammenholdt med 2. kvartal i 2024 er antallet af *underretninger om mistænkelige transaktioner* (STR) steget marginalt, *underretninger om mistænkelige aktiviteter* (SAR) er steget med 27 pct., mens antallet af *underretninger om mulig terrorfinansiering* (TFR) er faldet med godt 50 pct.

Tabel 2*. Antal underretninger sendt til Hvidvasksekretariatet i perioden 2. kvartal 2024 til og med 2. kvartal 2025 fordelt på underretningstype.

Underretningstype	2. kvartal 2024	3. kvartal 2024	4. kvartal 2024	1. kvartal 2025	2. kvartal 2025
Underretninger om mistænkelige transaktioner (STR)	18.953	20.442	20.294	19.966	19.028
Underretninger om mistænkelige aktiviteter (SAR)	3.373	3.560	3.103	3.742	4.268
Underretning om mulig terrorfinansiering (TFR)	69	43	39	44	34
I alt	23.395	24.045	23.436	23.752	23.330

*Tallene i tabellen er dynamiske og kan ændre sig fra kvartal til kvartal. Det skyldes, at der kan ske efterregistreringer for tidligere kvartaler, da den dato Hvidvasksekretariatet modtager underretningen, og den dato underretningen registreres i systemet, kan divergere.

Antallet af underretninger kan ikke bruges til at estimere omfanget af hvidvask. En stigning i antallet af underretninger *kan* skyldes en stigning i hvidvaskaktiviteter, men også andre forhold, fx øget fokus på hvidvask, ændrede forretningsgange eller flere ressourcer hos de underretningspligtige.

Af tabel 3 fremgår antallet af underretninger fra hver kategori af underrettere. Tallene i parentes viser, hvor mange *aktive* underretningspligtige, der er oprettet i GoAML i den pågældende kategori pr. 30. juni 2025. At være registreret som *aktive* betyder, at en underretningspligtig er oprettet korrekt i GoAML. Det er ikke ensbetydende med, at de pågældende har sendt underretninger.

Det fremgår af tabellen, at størstedelen af underretningerne kommer fra *pengeinstitutter* og *spiludbydere*. Det tredjestørste antal underretninger kommer fra *udstedere af elektroniske penge og udbydere af betalingstjenester*. Blandt *udstedere af elektroniske penge og udbydere af betalingstjenester* har der været en stigning på 50 pct. i antallet af underretninger siden 1. kvartal 2025 og en stigning på cirka 30 pct. i forhold til det gennemsnitlige antal underretninger det seneste år. Denne stigning skyldes primært to underrettere, der har øget antallet af underretninger betydeligt. Disse underretninger handler typisk om mistænkelige transaktioner fortaget mellem Danmark og udlandet, herunder særligt Tyrkiet.

Blandt *Udbydere af virtuelle tegnebøger og veksling mellem virtuelle valutaer og fiatvalutaer* er antallet af underretninger også steget siden 1. kvartal 2025, fra 62 underretninger til 104. Underretningerne i denne kategori kommer primært fra en enkelt underretter og omhandler særligt mistænkelig aktivitet vedrørende kryptovaluta.

Ligeledes er der større stigninger i antallet af underretninger fra *revisorer, valutavekslingsvirksomheder og ejendomsmæglere* siden sidste kvartal.

Tabel 3*. Antal modtagne underretninger fordelt efter type underretter i perioden fra 2. kvartal 2024 til og med 2. kvartal 2025

Underretter	2. kvartal 2024	3. kvartal 2024	4. kvartal 2024	1. kvartal 2025	2. kvartal 2025
Pengeinstitutter (85)	17.291	18.417	17.767	17.907	16.841
Spiludbydere (77)	1.423	1.473	1.817	1.883	1.861
Udstedere af elektroniske penge og udbydere af betalingstjenester (63)	989	1.077	1.266	938	1.402
Revisorer (684)	1.021	970	734	593	865
Offentlige myndigheder (130)	712	812	744	717	650
Realkreditinstitutter (8)	232	463	569	1.030	903
Finansiell leasing (120)	218	181	140	203	203
Valutavekslingsvirksomheder (17)	340	443	238	263	364

Advokater (179)	56	63	65	90	43
Udbydere af virtuelle tegnebøger og veksling mellem virtuelle valutaer og fiatvalutaer (19)	32	48	34	62	104
Skatterådgivere, eksterne bogholdere mv. (339)	47	57	26	31	41
Andre (260)	14	18	9	15	7
Livsforsikringsselskaber og pensionskasser (30)	5	15	6	3	11
Ejendomsmæglere (750)	7	5	20	11	31
Service Providere** (55)	8	3	1	6	1
Investeringsforeninger og fonde (65)	0	0	0	0	0
Kunsthandlere og auktionshuse (12)	0	0	0	0	1
Sparevirksomheder (5)	0	0	0	0	0
Fondsmæglerselskaber (45)	0	0	0	0	1
Forsikringsformidlere (16)	0	0	0	0	1

*Tallene i tabellen er dynamiske og kan ændre sig fra kvartal til kvartal. Det skyldes, at der kan ske efterregistreringer for tidligere kvartaler, da den dato Hvidvasksekretariatet modtager underretningen, og den dato underretningen registreres i systemet, kan divergere. Yderligere kan underretningspligtige blive rykket til en anden branchekategori, hvis de er registreret under en branche, som de ikke tilhører.

***"Service Providere" dækker over udbydere af tjenesteydelser til virksomheder: selskabsoprettere, professionelle ledelsesmedlemmer, kontorhoteller mv.

Som det fremgår af tabellen, er der forskel på, hvor meget de forskellige typer af underretningspligtige underretter.

Mens nogle underretningspligtige har en fast praksis om at underrette ved mistænkelige transaktioner og aktiviteter, er der stadig underretningspligtige, som Hvidvasksekretariatet sjældent hører fra. Der findes også brancher, hvor kun få underretningspligtige har oprettet sig i GoAML. Det kan skyldes, at der ikke er tegn på hvidvask eller manglende opmærksomhed på risikoen for hvidvask.

Hvidvasksekretariatet gør opmærksom på, at du som omfattet af hvidvaskloven har pligt til at *underrette omgående*, hvis du har en mistanke om hvidvask eller terrorfinansiering, som du ikke kan afkræfte. Hvis du ikke har oprettet dig som bruger i GoAML forud for opdagelsen af en mistænkelig adfærd, er det vanskeligt at underrette Hvidvasksekretariatet omgående. Derfor opfordrer Hvidvasksekretariatet fortsat alle underretningspligtige til at oprette sig i GoAML, så du omgående kan sende en underretning, hvis du "er vidende om, har mistanke om eller rimelig grund til at formode, at en transaktion, midler eller en aktivitet har eller har haft tilknytning til hvidvask eller finansiering af terrorisme", som det fremgår af § 26, stk. 1, i hvidvaskloven.

Du kan læse mere om, hvordan du opretter dig i GoAML på vores hjemmeside Hvidvask.dk eller ved at klikke [her](#). Er du allerede oprettet, opfordrer vi til, at du holder dine kontaktoplysninger opdateret. Du kan læse mere om kontaktoplysninger [her](#).

I 2. kvartal 2025 blev der oprettet 96 nye underretningspligtige (unikke virksomheder) i GoAML, og det samlede antal aktive underretningspligtige, der er oprettet i GoAML er 2.959 pr. 30. juni 2025. Det svarer til, at godt 13 pct. af de minimum 22.000 underretningspligtige personer og virksomheder, der er omfattet af hvidvaskloven, har oprettet sig i GoAML.

Nyttiggørelse af efterretninger

Når Hvidvasksekretariatet videregiver oplysninger til en anden myndighed, fx en politikreds, sker det som en efterretning, der kan indeholde oplysninger fra mere end én underretning.

Af tabel 4 fremgår, hvor mange efterretninger Hvidvasksekretariatet har fremsendt til forskellige myndigheder. En efterretning kan indeholde én enkelt underretning eller en pakke af underretninger, som Hvidvasksekretariatet har analyseret og eventuelt beriget. Efterretningerne kan også indeholde andre underretningstyper end STR, SAR og TFR.

Tabel 4*. Antal efterretninger som Hvidvasksekretariatet har videregivet til forskellige myndigheder i perioden fra 2. kvartal 2024 til og med 2. kvartal 2025.

Modtagere	2. kvartal 2024	3. kvartal 2024	4. kvartal 2024	1. kvartal 2025	2. kvartal 2025
Skatteforvaltningen	2.062	1.074	2.920	3.013	2.119
Politiet (politikredsene og NSK)	522	545	575	528	514
PET: understøttelse af PET's operative virke	117	85	91	87	86
PET: andre administrative oplysninger	70	78	70	46	48
Anden offentlig myndighed	106	90	217	278	176
I alt	2.877	1.872	3.873	3.952	2.943

* Tallene i tabellen er dynamiske og kan ændre sig fra kvartal til kvartal. Det skyldes, at der kan ske efterregistreringer for tidligere kvartaler.

Den samme underretning kan indgå i forskellige pakker af efterretningsoplysninger og nyttiggøres i mange forskellige videregivelser. Af tabellen nedenfor fremgår det, hvor mange gange en underretning er videregivet til de enkelte myndigheder.

Tabel 5. Antal gange en underretning er videregivet til en myndighed i perioden fra 1. kvartal 2024 til og med 1. kvartal 2025.

Modtagere	2. kvartal 2024	3. kvartal 2024	4. kvartal 2024	1. kvartal 2025	2. kvartal 2025
Skatteforvaltningen	8.288	2.914	11.755	12.001	8.167
Politiet (politikredsene og NSK)	6.608	5.065	6.916	12.440	5.628
Anden offentlig myndighed	939	519	964	1.098	893
PET: understøttelse af PET's operative virke	346	184	236	264	232
PET: andre administrative oplysninger	139	296	161	185	171
I alt	16.320	8.978	20.032	25.988	15.091

* Tallene i tabellen er dynamiske og kan ændre sig fra kvartal til kvartal. Det skyldes, at der kan ske efterregistreringer for tidligere kvartaler. Det bemærkes endvidere, at oplysningerne i underretningerne ikke nødvendigvis bliver videregivet i den samme periode, som de er modtaget i. Det skyldes, at underretningerne kan vise sig først at være relevante at videregive i forbindelse med andre underretninger, der kommer til Hvidvasksekretariatet på et senere tidspunkt, eller i forbindelse med en efterforskning.

I 2. kvartal 2025 blev der 15.091 gange videregivet underretninger til politikredsene, PET, Skatteforvaltningen og andre offentlige myndigheder. Det er et fald på mere end 10.000 videregivelser i forhold til 1. kvartal 2025, men på niveau med antallet af videregivelser i 2. kvartal 2024.

Det relativt store antal videregivelser til Skatteforvaltningen skyldes blandt andet, at Hvidvasksekretariatet har øget automatiseringen af større dele af processen. Det markante antal af videregivelser til særligt politikredsene i 1. kvartal 2025 skyldes et større antal videregivelser i forbindelse med Hvidvasksekretariatets understøttelse af konkrete efterforskninger.

Særligt for politiet

Foruden de konkrete videregivelser til politiet bliver underretninger fra danske underretningspligtige udstillet i politiets it-system, POL-Intel. Det sker på en måde, hvor politiet kan identificere om konkrete personer, virksomheder, bankkonti eller lignende indgår i hvidvaskunderretninger. Politiet kan dog ikke se indholdet eller afsender af underretningerne. Hvis politiet på baggrund af et *hit* i POL-Intel ønsker at få adgang til indholdet i den pågældende underretning, skal politiet sende en begrundet anmodning til Hvidvasksekretariatet om at videregive underretningen. På den måde kan politiet få adgang til relevante oplysninger, såsom mistankegrundlaget og underliggende bilag, fx transaktionsoversigter. Politiet har således en særlig adgang, der giver dem mulighed for at identificere underretninger, der kan berige deres arbejde i igangværende efterforskninger og analyser, hvilket bidrager til en effektiv nyttiggørelse af Hvidvasksekretariatets oplysninger.

Beslaglæggelser

I 2. kvartal 2025 modtog Hvidvasksekretariatet 62 underretninger med mulighed for beslaglæggelse, herunder seks fast track-underretninger. Den samlede sum for de 62 underretninger var 29 millioner kroner. Fast track-underretningerne stod for 19 millioner kroner.

Ved modtagelse af en fast track-underretning skal Hvidvasksekretariatet inden udløbet af den efterfølgende bankdag træffe beslutning om, hvorvidt der i medfør af retsplejelovens § 807 f skal foretages en midlertidig beslaglæggelse af beløbet. En beslaglæggelse efter § 807 f er midlertidig og bortfalder efter en uge. Gennemføres en beslaglæggelse efter § 807 f, videregives oplysningerne fra underretningen til en politikreds eller NSK, som tager stilling til beslaglæggelse efter retsplejelovens § 802.

Oplysninger fra underretninger, hvor der er mulighed for beslaglæggelse, men som ikke falder ind under fast track-ordningen, videregives til en politikreds eller NSK, som tager stilling til en beslaglæggelse efter retsplejelovens § 802.

Skatteforvaltningens brug af oplysninger fra Hvidvasksekretariatet i 1. kvartal 2025

Ved mistanke om skatte- og momsunddragelse sender Hvidvasksekretariatet løbende efterretningsoplysninger til Skatteforvaltningen. En efterretningsoplysning kan indeholde oplysninger fra flere underretninger. Det sker blandt andet, når flere underretninger handler om den samme persongruppe eller de samme formodede svigshandlinger. Hvis underretningerne med mistanke om skatte- og momsunddragelse ved deres visitation i Hvidvasksekretariatet viser sig at være relevante for politiet, sendes de direkte til relevante politikredse og/eller NSK.

I 1. kvartal 2025 modtog Skattestyrelsen, som er SPOC (Single Point of Contact) i Skatteforvaltningen, 2.999 efterretningsoplysninger fra Hvidvasksekretariatet. Det er tre gange flere end i samme periode i 2024, hvor Hvidvasksekretariatet fremsendte 983 efterretningsoplysninger.

Når efterretningsoplysninger anvendes af Skattestyrelsen, er oplysningerne nyttiggjorte. I kontrolmæssig sammenhæng kan der være tale om nyttiggørelse med eller uden resultat. I 1. kvartal 2025 har Skattestyrelsen nyttiggjort 194 efterretningsoplysninger, hvoraf 162 er blevet nyttiggjort i sagsbehandlingen med ændring af skatte- og/eller afgiftstilsvaret. Af disse efterretningsoplysninger indgår 143 i sager, som efterfølgende er sendt til ansvarsvurdering. 32 underretninger er nyttiggjort uden resultat. En efterretningsoplysning, der er nyttiggjort uden resultat, er et udtryk for, at der er foretaget en kontrol på baggrund af den modtagne efterretningsoplysning, hvor kontrollen ikke har givet anledning til skatte- eller afgiftsmæssige ændringer.

Skattestyrelsens behandling af efterretningsoplysningerne har i 1. kvartal 2025 resulteret i et netto-provenu på knap 190 millioner kroner. I forhold til samme periode i 2024 er der tale om en stigning på 64 millioner kroner.

Skattestyrelsen igangsatte i 2023 et initiativ, som afsøgte mulighederne for at øge nyttiggørelsesgraden af de modtagne efterretningsoplysninger. Der blev i 2023 og 2024 på baggrund af en forsøgsordning arbejdet målrettet med at anvende efterretningsoplysninger i flere af Skattestyrelsens fagområder samt i de øvrige styrelser i Skatteforvaltningen, fx Toldstyrelsen og Motorstyrelsen. Skattestyrelsen vil samtidig etablere en proces med henblik på at kunne afrapportere på anvendelsen af efterretningsoplysninger til flere formål inden for Skattestyrelsens myndighedsområde med analytiske formål, fx måludpegning.

Efterretningsoplysningerne udgør et vigtigt bidrag til Skattestyrelsens muligheder for at målrette og effektivisere kontrolindsatsen mod den organiserede og systematiske skatteøkonomiske kriminalitet. Skattestyrelsens Kontrol- og Forretningsudvikling holder hver måned møde med Hvidvasksekretariatet for at drøfte trends og indhold. Derudover oplyser Hvidvasksekretariatet om forventningerne til det fremtidige antal oversendelser, ligesom antallet af allerede oversendte efterretningsoplysninger afstemmes med henblik på at sikre, at alle efterretningsoplysninger, som sendes til Skattestyrelsen, når frem.

Aktuelle hvidvasksager

Når Hvidvasksekretariatet videregiver oplysninger fra en underretning til en politikreds eller NSK, kan oplysningerne anvendes på følgende måder:

- Som grundlag for igangsættelse af en *ny efterforskning* vedrørende hvidvask eller anden kriminalitet.
- Til at underbygge en *igangværende efterforskning* og som muligt bevis i en straffesag.
- Som efterretninger, der kan indgå i politiets *samlede forståelse af kriminalitetsbilledet* eller risici inden for forskellige områder.

De underretninger, der anvendes i efterforskninger, kan resultere i, at der rejses tiltaler, hvis anklagemyndigheden vurderer, at det samlede bevismateriale kan føre til dom. I nogle tilfælde vil anklagemyndigheden rejse tiltale for førforbrydelsen, fx salg af narkotika eller grov skatte- og momssvig. I andre tilfælde vil der blive rejst tiltale for hvidvask efter straffelovens § 290 a.

Der er i 2. kvartal 2025 blandt andet rejst sigtelser eller faldet afgørelser i følgende sager om hvidvask:

- **Tre anholdt for hvidvask gennem skønhedsklinikker**

I juli måned blev to mænd og en kvinde anholdt og sigtet for hvidvask af ikke under 13 millioner kroner gennem skønhedsklinikker. I forbindelse med aktionen blev der foretaget ransagninger af i alt seks adresser i Aarhus, København og Sverige. Ransagningerne i Danmark er sket i samarbejde med Styrelsen for Patientsikkerhed, Lægemiddelstyrelsen samt Skattestyrelsen. Ransagningerne i Sverige er sket i samarbejde med svensk politi. Ved ransagningerne blev der beslaglagt store kontantbeløb i både dansk og udenlandsk valuta.

Sagen tager sit udspring i ODIN-samarbejdet, og den efterfølgende efterforskning i NSK er sket i tæt samarbejde med Styrelsen for Patientsikkerhed, Lægemiddelstyrelsen, Skattestyrelsen og Erhvervsstyrelsen. Du kan læse om sagen [her](#).

- **Dom for hvidvask af mere end 75 millioner kroner via Rumænien**

Fra juli 2018 til december 2019 hvidvaskede et firma i Hovedgård adskillige millioner kroner via Rumænien. I juni blev tre mænd dømt i sagen. En 58-årig mand blev idømt tre år og seks måneders ubetinget fængsel for grov hvidvask for mere end 75 millioner kroner. To medgerningsmænd på 26 år og 49 år fik hver to år og seks måneders fængsel.

I dommen blev der lagt vægt på, at den 58-årige mand var i kontakt med ukendte medgerningsmænd og ligeledes rekrutterede og vejledte den 26-årige, der var stifter og ejer af virksomheden, med henblik på at hvidvaske pengene gennem hans selskab. Han var ligeledes bevidst om størrelsen på de beløb, der blev hvidvasket og havde fuldmagt til en af de rumænske bankkonti.

Ifølge anklagemyndigheden ved NSK, som har ført sagen, blev store beløb kanaliseret gennem fiktive fakturaer og rumænske bankkonti, som tilhørte et rumænsk datterselskab. Herfra blev pengene sendt videre til adskillige bankkonti i både Danmark og udlandet.

- **Salon på Nørrebro har hvidvasket for over 20 millioner**

En 43-årig frisør blev idømt tre års fængsel for hvidvask i millionklassen via sin frisørsalon på Nørrebro. Det var en af frisørens venner, der ledte politiet i retning af salonen, da han blev stoppet med en rygsæk, som indeholdt 578.000 kroner i kontanter. Ved ransagningen blev der blandt andet fundet 400.000 kroner i kontanter, 14.500 kroner gemt under et ringbind i en skuffe og adskillige pengebundter med 500- og 1.000-kronesedler. Yderligere blev der fundet store kontantbeløb i en bil.

Frisøren fik ud over de tre års fængsel for grov hvidvask også en bøde på cirka 29 millioner kroner - svarende til det beløb, som blev hvidvasket i salonen. Manden, der kommer fra Syrien, undgår udvisning.

Du kan læse hele historien [her](#).

- **Ville afdrage på narkogæld: Mand i 20'erne dømt for at stille konti til rådighed**

En mand i 20'erne blev idømt otte måneders fængsel for hvidvask af cirka 700.000 kroner i perioden fra 2022 til 2024. Ifølge Nordjyllands Politi, der førte sagen, afbetalte manden på sin narkogæld ved at stille konti til rådighed for bagmænd, herunder også ved at have fået flere kammerater til at stille deres konti til rådighed for bagmændene. Det kriminelle udbytte stammede fra netbanksindbrud hos ældre borgere, og der var tale om kontanthævninger og videreoverførsler til udenlandske konti. Bagmændene er ikke identificeret.

- **Mand skal i fængsel for hvidvask af tocifret millionbeløb i byggebranchen**

En 27-årig mand blev idømt tre års fængsel for i halvandet år at have medvirket til at hvidvaske 23 millioner kroner via en fakturafabrik. Manden erkendte og forklarede i retten, hvordan han og en samarbejdspartner brugte konti fra såkaldte muldyr til at modtage sorte penge. Derefter blev der udarbejdet falske fakturaer i navnet på eksisterende virksomheder, så pengene fremstod lovlige. Det skriver mediet [Building Supply](#) med reference til artikel i [Sjællandske medier](#).

I retten fortalte han blandt andet om sit samarbejde med aktører i byggeriet, som fik ham til at hvidvaske penge for tømrere, håndværkere, VVS'ere med videre. Manden forklarede, at han konverterede pengene til kryptovaluta og sendte dem videre mod til gengæld at få to pct. af beløbet.

Mediet *Building Supply* har tidligere skrevet om falske faktura i byggebranchen. Se fx [Hvorfor er fakturasvindel så udbredt i byggeriet? Eksperter har et bud](#)

- **Person fra Vestgrønland sigtet for blandt andet hvidvask**

En person fra Vestgrønland blev på baggrund af oplysninger fra Hvidvasksekretariatet og underretningspligtige anholdt og sigtet for besiddelse af hash og hvidvask. I forbindelse med anholdelsen blev der foretaget ransagning, hvor politiet efterfølgende fandt 1,2 kilo hash. Ud over hashen blev der fundet et mindre pengebeløb i kontanter. Politiet efterforsker fortsat sagen.

- **Kolde kontanter: Vildt fund i Københavns Lufthavn**

En mand blev i juni sigtet for hvidvask, efter han i Københavns Lufthavn blev taget med ikke mindre end 250.000 kroner samt over 6.000 euro i sin bagage. Efter fundet blev sagen overdraget til politiet. Københavns Politi har efterfølgende sigtet manden for hvidvask. Du kan læse mere [her](#).

- **Dømt for hvidvask af penge der stammer fra bedrageri mod ældre borgere.**

I to sager håndteret af Sydøstjyllands Politi er to personer dømt for hvidvask af penge, der stammer fra kriminalitet mod ældre borgere.

I maj blev en 42-årig mand ved Retten i Kolding dømt for hvidvask og hæleri for et samlet beløb på 59.000 kroner. Pengene stammede fra et telefonbedrageri begået over for en ældre kvinde. Manden blev idømt 40 dages betinget fængsel med vilkår om 60 timers ulønnet samfundstjeneste og tilsyn af kriminalforsorgen i prøvetiden på et år. Dommen indeholdt ligeledes et forhold af spirituskørsel og kørsel uden førerret.

I juni blev en 33-årig mand ved Retten i Kolding dømt for to tilfælde af hvidvask og hæleri for et samlet beløb på 112.500 kroner. Pengene stammede fra telefonbedragerier begået over for ældre kvinder. Manden blev idømt 60 dages betinget fængsel med prøvetid i et år.

- **Hvidvask af penge der stammede fra bedrageri i samhandel**

I juni blev en 19-årig mand ved Retten i Kolding dømt for fem tilfælde af hvidvask og hæleri for et samlet beløb på cirka 19.000 kroner. Pengene stammede fra flere bedragerier i forbindelse med samhandel. Manden, der var 17 år på gerningstidspunktet, blev idømt 14 dages betinget fængsel med prøvetid på et år, samt tildelt en advarsel om udvisning.

- **Hawala-agent dømt for hvidvask af 29 millioner kroner**

En mand blev idømt tre års ubetinget fængsel og advarsel om udvisning for hvidvask af cirka 29 millioner kroner. Sagen er anket.

Københavns Politi efterforskede manden for at være en såkaldt hawala-agent i et større hvidvasknetværk, hvor flere bagmænd, muldyr, stråmænd i fakturafabrikker og andre hawala-agenter blev anholdt og sigtet. Politiet mistænkte manden, som havde en forretning på Nørrebro, for dagligt at modtage større kontantbeløb, som han via sit hawala-netværk flyttede til udlandet. Kontanterne blev herefter - mod betaling af et gebyr - udbetalt til forskellige netværk, der havde brug for kontanter.

- **Hollandsk statsborger dømt for hvidvask gennem dansk selskab**

En 45-årig hollandsk statsborger blev ved retten i Glostrup dømt for hvidvask af cirka 237 millioner kroner i en sag ført af NSK. Den 45-årige var ejer og direktør i et dansk selskab, der fungerede som fakturafabrik, og hvorigennem der blev overført cirka 237 millioner kroner. Der blev ved dommen lagt vægt på, at den 46-årige vidste, at han var direktør i selskabet samt at han fik løn for det, men at han ikke havde indsigt i driften og heller ikke søgte at få det. Den 46-årige bad således ikke om at få dokumenter eller andet vedrørende driften, og havde alene kontakt cirka hver anden måned med selskabets reelle leder. På den baggrund fandt retten at den 46-årige "i hvert fald må have indset muligheden for, at han ved sine handlinger foranledigede den i anklageskriftet beskrevne hvidvask, og at han accepterede denne mulighed for det tilfælde, at det faktisk forholdt sig på denne måde". Den 46-årige blev idømt fængsel i fire år og seks måneder samt udvisning for bestandigt.

- **Direktør dømt for hvidvask ved at overlade kontrollen af selskabets konto til medgerningsmand**

Den domfældte var direktør og ejer af et selskab, hvor han efter aftale overlod kontrollen med selskabets konto til en medgerningsmand, som derefter lod cirka 19 millioner kroner, der stammede fra kriminalitet, passere gennem kontoen. NSK har efterforsket sagen, og retten i

Randers fandt, at direktøren ved at have forholdt sig passivt til medgerningsmandens brug af kontoen samt ved at have overladt selskabets NemID/MitID til denne, havde accepteret risikoen for, at kontoen blev anvendt til kriminell aktivitet. Direktøren blev på den baggrund dømt for hvidvask af cirka 19 millioner kroner og idømt fængsel i to år og seks måneder, heraf seks måneder ubetinget. Der blev endvidere konfiskeret cirka 450.000 kroner, der var beslaglagt på selskabets konto, ligesom direktøren blev fradømt retten til at deltage i ledelsen af en erhvervsvirksomhed i to år.

- **25-årig mand dømt for hvidvask ved at have stillet sin private konto til rådighed for andre personer**

En 25-årig mand erkendte sagens faktiske omstændigheder, herunder at han over en periode på cirka to år havde modtaget cirka 2,5 millioner kroner på sin private konto, som han efterfølgende kanaliserede videre. Dette var sket efter instruktion fra en person, som den 25-årige kendte. Den 25-årige nægtede sig dog skyldig.

I sagen, der er ført af NSK, fandt retten i Roskilde den 25-årige skyldig, idet retten lagde vægt på hans egen forklaring om, at han hele tiden var nervøs for, at der kunne ske "noget", uden dog at præcisere, hvad dette var. Retten lagde ligeledes vægt på beløbets størrelse samt på, at den person, som fik kontoen stillet til rådighed, tilsyneladende havde adgang til meget dyre biler og smykker, uden at denne havde et tilsvarende indtægtsgrundlag. På den baggrund fandt retten det bevist, at den 25-årige utvivlsomt måtte have vidst, at der var tale om penge fra kriminelle forhold. Det var i sagen ikke bestridt, at der var tale om udbytte fra kriminell aktivitet. Den 25-årige blev idømt fængsel i et år og seks måneder, heraf tre måneder ubetinget.

- **Mand dømt for hvidvask ved at have foranlediget, at cirka 23 millioner kroner blev indbetalt på andre personers konti og derefter videreoverført**

En mand er i en tilståelsessag, ført af NSK, idømt tre års fængsel for i forening med en medgerningsmand at have hvidvasket cirka 23 millioner kroner. Hvidvasken var sket ved, at manden overtalte et antal personer til at stille deres bankkonti til rådighed for ham. Herefter indsatte og videreoverførte de to mænd samlet set cirka 23 millioner kroner på kontiene.

I tillæg er her et par yderligere sager om brud på hvidvaskloven for første kvartal 2025:

- **Regnskabsvirksomhed dømt for utilstrækkelig risikovurdering og risikostyring**

I slutningen af februar 2025 blev et anpartsselskab og dets direktør ved Retten i Randers idømt en bøde på henholdsvis 60.000 kroner og 6.000 kroner for overtrædelse af hvidvaskloven, da der hverken var udarbejdet en tilstrækkelig risikovurdering af virksomheden eller tilstrækkelige skriftlige politikker, forretningsgange og kontroller.

- **Regnskabsvirksomhed dømt for manglende kendskab til sine kunder**

I slutningen af februar 2025 blev et anpartsselskab og dets direktør ved Retten på Frederiksberg idømt en bøde på henholdsvis 50.000 kroner og 5.000 kroner for overtrædelse af hvidvasklovens regler om kundekendskab, idet virksomheden i ti kundeforhold ikke havde haft det tilstrækkelige kendskab til sine kunder.

Financial Action Task Force (FATF) plenar i juni

Hvidvasksekretariatet deltog i juni måned i det fælles FATF-MONEYVAL plenar, der blev afholdt i Europarådet i Strasbourg, hvor delegerede fra mere end 200 jurisdiktioner diskuterede centrale problemstillinger inden for hvidvask, terror- og proliferationsfinansiering (finansiering af masseødelægelsesvåben).

Et vigtigt resultat af plenarmødet var godkendelsen af MONEYVALs evaluering af Letland, den første evaluering i FATF's femte evalueringsrunde, der har et særligt fokus på, hvor effektivt landene bekæmper hvidvask, terror- og proliferationsfinansiering i forhold til de risici, landene står overfor.

Der blev derudover vedtaget flere ændringer til FATF-standarderne, herunder ændringer som skal forbedre sikkerheden og trygheden ved grænseoverskridende betalinger, og nye procedurer, der skal forhindre forkert anvendelse af de tiltag, der har til formål at beskytte non-profit organisationer mod misbrug.

Plenarmødet udmundede tilmed i vedtagelsen af flere rapporter og vejledninger fra FATF, der vil blive offentliggjort henover sommeren med det formål at gøre opmærksom på tendenser og trusler. Udgivelserne omfatter blandt andet en rapport om terrorfinansiering: [Comprehensive Update on Terrorist Financing Risks](#), en rapport om proliferationsfinansiering og sanktioner: [Complex Proliferation Financing and Sanctions Evasion Schemes](#) og en vejledning om finansiell inklusion: [Guidance on Financial Inclusion and Anti-Money Laundering and Terrorist Financing Measures](#).

Alle myndigheder er nu underretningspligtige

Pr. 1 juli 2025 trådte en lovændring i kraft, der gør alle myndigheder underretningspligtige. Hvidvasklovens § 28 lyder: "Får en tilsynsmyndighed i henhold til denne lov eller andre myndigheder kendskab til forhold, der giver grund til at tro, at disse kan have tilknytning til hvidvask eller finansiering af terrorisme, som er omfattet af underretningspligten i § 26, stk. 1, skal myndigheden underrette Hvidvasksekretariatet herom".

Alle myndigheder forpligtes hermed til at underrette om potentiel hvidvask og terrorfinansiering til Hvidvasksekretariatet. Samtidig er alle underretninger underlagt tavshedspligten i hvidvasklovens § 38 a.

Det er vigtigt at bemærke, at myndighederne skal underrette Hvidvasksekretariatet ved såvel *mis-tanke* som ved *kendskab* til hvidvask, terrorfinansiering med videre. Har myndighederne kendskab til lovovertrædelser, skal forholdet også anmeldes til politiet. En underretning til Hvidvasksekretariatet kan ikke gøre det ud for en eventuel politianmeldelse.

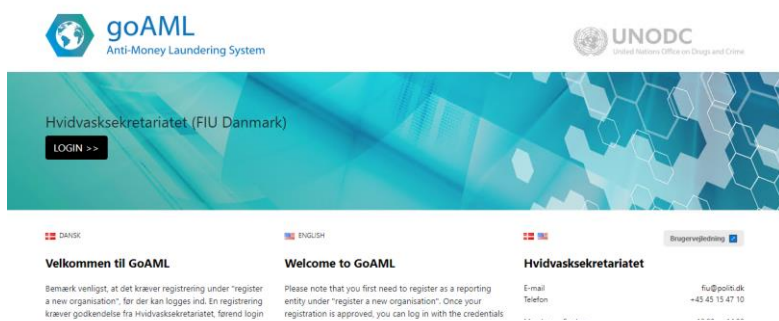
Hvidvasksekretariatet kan til enhver tid af egen drift videregive relevante oplysninger til kompetente myndigheder i Danmark. Tilsynsmyndigheder i Danmark kan ligeledes anmode Hvidvasksekretaria-

tet om oplysninger, idet Hvidvasksekretariatet kan imødekomme sådanne anmodninger, når de udspringer af bekymringer vedrørende mulig hvidvask af penge eller finansiering af terrorisme, og oplysningerne skal bruges til myndighedernes opgavevaretagelse.

Har du mistanke om hvidvask eller terrorfinansiering? Sådan underretter du:

En underretning er en oplysning med mistanke om mulig finansiell kriminalitet, som fx hvidvask eller terrorfinansiering. Underretningerne skal sendes direkte til Hvidvasksekretariatet via portalen GoAML.

Har du endnu ikke adgang til GoAML, er der hjælp at hente på vores [hjemmeside](#). Du er også meget velkommen til at kontakte os på telefon: (+45) 4515 4710 eller på vores mail: fiu@politi.dk.



Europol's trusselsvurdering for internetkriminalitet

Europol har udgivet deres trusselsvurdering på området for organiseret internetkriminalitet, [Internet Organised Crime Threat Assessment 2025](#) (IOCTA). Rapporten *Steal, deal and repeat: How cyber-criminals trade and exploit your data* er en dybdegående analyse af, hvordan data er blevet kernen i en global, industrialiseret cyberkriminalitet, hvor cyberkriminelle handler med og udnytter ulovlig adgang til data, herunder kommercialiserer disse varer og tjenester.

Kompromitterede data er blevet yderst værdifulde for en bred vifte af kriminelle aktører. Data kan i sig selv være værdifulde og misbruges til fx afpresning og i spionage-aktiviteter, ligesom de kan være midler eller værktøjer til at begå anden kriminalitet, fx identitetstyveri. Data som login-oplysninger, cookies og tokens udnyttes dog ikke blot til at tilgå konti og netværk, men kan også videresælges på markedspladser, så andre kriminelle kan udnytte dem til yderligere kriminelle aktiviteter. Det kan fx handle om 'datadumps' af legitimationsoplysninger, kreditkort-oplysninger, abonnementer på phishing-kits med videre. Udviklingen er i høj grad drevet frem af sociale manipulationsteknikker (social engineering), kunstig intelligens og markedspladser for kriminelle ydelser.

I 2024 støttede Europol en international operation mod LabHost32, en stor platform, der tilbød phishing-kits til salg. LabHost32 tilbød tilpassede phishing-kits, hosting-infrastruktur, interaktiv funktio-

onalitet til direkte kontakt med ofrene samt kampagne-oversigtstjenester for et månedligt abonnementsgebyr. I 2024 benyttes en række forskellige teknikker til at skaffe sig adgang til og stjæle og udnytter både menneskelige sårbarheder og tekniske sårbarheder i systemer. Disse teknikker anvendes af forskellige kriminelle aktører, som ofte kombinerer dem på en effektiv måde i deres kriminelle proces. Det gælder fx Initial Access Brokers, Data Brokers, Info-stealers, Phishing- og Social Engineering-kriminelle, Generative AI-baserede aktører og specialiserede aktører i online seksuel udnyttelse af børn og statsligt tilknyttede kriminelle netværk, som opererer som stedfortrædere for politiske eller geopolitiske formål (hybride-aktører).



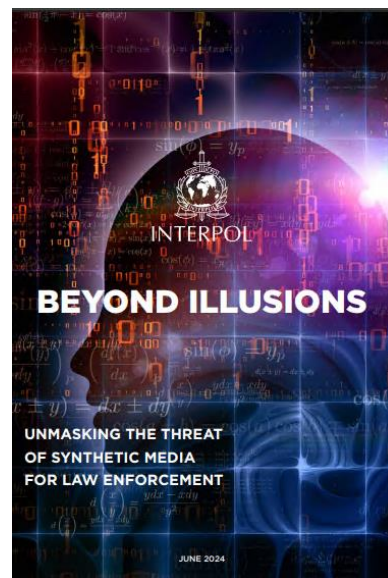
Udviklingen i kunstig intelligens, herunder den bredere anvendelse af store sprogmodeller og andre former for generativ kunstig intelligens, gør cyberkriminalitet mere sofistikeret, global og vanskeligere at bekæmpe. Kunstig intelligens forbedrer effektiviteten af social engineering-teknikker ved at skræddersy kommunikationen med ofrene og automatisere kriminelle processer.

Europols podcast har i denne sæson fokus på onlinestrukturernes betydning for udviklingen i kriminaliteten i Europa. I den seneste udgave diskuteres kunstig intelligens i forlængelse af trusselsvurderingen, IOCTA 2025. Du finder dette og alle øvrige afsnit [her](#).

Interpol om syntetisk medieproduktion

Interpol udgav sidste år rapporten *Beyond Illusions – Unmasking the Threat of Synthetic Media for Law Enforcement* med fokus på syntetisk medieproduktion, herunder deepfakes, AI-genereret stemme og tekst og dens betydning for retshåndhævelse internationalt. Selvom fokus er på betydningen for de retshåndhævende myndigheder, så er der gode beskrivelser og eksempler på anvendelser, hvis relevans rækker videre. Rapporten advarer om, at AI-drevne medier er blevet så realistiske og samtidig let tilgængelige globalt, at det kan være vanskeligt at skelne ægte fra manipulerede medier – og det er i den grad også relevant for alle aktører på hvidvaskområdet.

Rapporten definerer syntetisk indholdsproduktion som AI-genererede billeder, videoer, stemmer og tekst. Ifølge Interpol har fremkomsten af nyere, tilgængelige generative AI-platformer og "deepfake-as-a-service" forstærket produktionen, idet teknologien muliggør produktion med minimal teknisk viden og er dermed blevet tilgængelig for alle, herunder også kriminelle aktører. Kriminelle bruger blandt andet syntetiske medier til misinformation, svindel og forfalskning. Det er især problematisk, at materialet kan narre både mennesker og simpel automatiseret verifikation. Med teknologisk fremskridt forventes disse manipulationer at blive endnu sværere at afsløre og vil udgøre en langt større udfordring.



Rapporten adresserer fx risikoen for, at AI-skabte stemmer, videoer eller tekst kan bruges til avanceret identitetssvindel. De avancerede syntetiske medier (fx deepfake-videoer og AI-genererede identitetsbilleder) kan bruges til at *manipulere eller omgå* kend-din-kunde-verifikationsprocedurer. Det er især relevant i tilfælde af fjern-onboarding af kunder via videokald, automatisk dokumentgenkendelse via biometrisk software og ansigtsgenkendelse i apps og netbank.

Du kan læse hele rapporten fra Interpol [her](#).

Nye lande på FATF's og EU's liste over højrisikolande

FATF's [sorte liste](#) omfatter lande, som har alvorlige strategiske mangler i forhold til at bekæmpe hvidvask af penge, finansiering af terrorisme og finansiering af proliferation. FATF opfordrer alle lande til at udvise skærpet due diligence, og - i de mest alvorlige tilfælde - anvende modforanstaltninger for at beskytte det internationale finansielle system mod de risici, der udgår fra landet.

FATF's *grå liste* omfatter lande, som FATF har placeret under øget overvågning på baggrund af en vurdering af, at landene har en forhøjet risiko for hvidvask.

I modsætning til landene på FATF's *sorte liste*, har landene på den *grå liste* forpligtet sig til at løse de af FATF påpegede strategiske mangler inden for nærmere bestemte tidsrammer, ligesom landene aktivt er i dialog med FATF om deres respektive handlingsplaner. FATF opfordrer ikke til, at andre jurisdiktioner udvider deres due diligence-foranstaltninger i relation til landene på den *grå liste*, men at der tages hensyn til oplysningerne, når der udarbejdes risikoanalyser.

På FATF's sorte liste er Nordkorea, Iran og Myanmar. Der er som følge af plenarmødet i juni ikke nogen ændringer til den sorte liste, men der er flere ændringer til den grå liste. Kroatien, Mali, og Tanzania er taget af den grå liste efter vellykkede inspektionsbesøg, der bekræftede landenes gennemførelse af deres respektive handleplaner og heraf følgende forbedring af landenes indsats mod hvidvask. Samtidig er Bolivia og De Britiske Jomfruøer tilføjet til den grå liste og er nu en del af de jurisdiktioner, der er under øget overvågning af FATF.

På FATF's grå liste over lande under øget monitoring er Algeriet, Angola, Bolivia, De Britiske Jomfruøer, Bulgarien, Burkina Faso, Cameroun, Den Demokratiske Republik Congo, Elfenbenskysten, Haiti, Kenya, Kroatien, Laos, Libanon, Monaco, Mozambique, Namibia, Nepal, Nigeria, Sydafrika, Sydsudan, Syrien, Venezuela, Vietnam og Yemen. Du kan læse mere om FATF's grå liste [her](#).

EU-Kommissionen definerer også løbende højrisiko tredjelande, og den liste er også blevet opdateret.

Algeriet, Angola, Elfenbenskysten, Kenya, Laos, Libanon, Monaco, Namibia, Nepal og Venezuela er føjet til listen over højrisiko tredjelande, mens Barbados, Gibraltar, Jamaica, Panama, Filippinerne, Senegal, Uganda og De Forenede Arabiske Emirater er fjernet fra listen.

Den samlede liste kan tilgås [her](#), og du kan læse mere om listen [her](#).

Oversigt over risikolande

Hvidvask er i stadig stigende grad en grænseoverskridende udfordring, hvor kriminelle netværk udnytter internationale finansielle systemer til at skjule ulovlige midler. Den øgede aktivitet på tværs af landegrænser komplicerer indsatsen mod hvidvask, da transaktioner ofte involverer flere jurisdiktioner med varierende reguleringsniveauer og håndhævelseskapaciteter.

Derfor er det vigtigt med et særligt fokus rettet mod såkaldte højrisikolande, hvor svagheder i regulering eller kontrol skaber gunstige betingelser for hvidvask og terrorfinansiering.

På baggrund heraf har Hvidvasksekretariatet udarbejdet en oversigt over lande, der fremgår af henholdsvis FATF's grå og sorte liste samt EU-Kommissionens liste over højrisikotredjelande, for at give de underretningspligtige et samlet overblik. Oversigten er dynamisk, da lande løbende til- og fragår listerne, hvorfor der vil ske regelmæssig opdatering af oversigten. Oversigten kan findes på Hvidvasksekretariatets hjemmeside [her](#).

Hvidvasksekretariatet arbejder derudover på en større analyse af de lande, som fylder meget i de underretninger, der modtages fra de underretningspligtige. Formålet med landeanalysen er dels at forstå, hvorfor disse lande fylder meget i underretningerne, og om det er muligt at identificere tendenser og risici ud fra dette, dels at afdekke, om der findes lande, vi sjældent hører om, som potentielt kan udgøre en risiko for blinde vinkler.

Resultaterne af den samlede analyse af landene bliver en del af den kommende *Nationale Risikovurdering af Hvidvask*, som offentliggøres i løbet af 2026, således at underretningspligtige, myndigheder og øvrige aktører ligeledes bliver opmærksomme herpå.

Et eksempel på indholdet af landeanalysen

De Forenede Arabiske Emirater er blandt de lande, som fylder meget beløbsmæssigt i de underretninger, som Hvidvasksekretariatet har modtaget de seneste par år.

Hvidvasksekretariatet har analyseret en stikprøve af underretninger fra 2022 til 2024, der vedrører De Forenede Arabiske Emirater. En væsentlig del af de analyserede underretninger om De Forenede Arabiske Emirater omhandler skatteunddragelse, pyramidespil samt køb af ejendomme. Der er stor variation i, hvad underretningerne omhandler, men der ses et mønster, hvor personer og virksomheder overfører penge til De Forenede Arabiske Emirater uden at kunne forklare banken, hvorfor de sender midlerne der til. Derudover er der ingen af de analyserede underretninger, hvor banken har kunnet identificere ejeren af modtagerkontoen. Endvidere er der indikationer på, at flere benytter Dubai som mellemled, hvorefter midlerne føres videre til tredjelande (dog kun i få af de analyserede underretninger).

Ny leder i Hvidvasksekretariatet

I juni 2025 tiltrådte stillingen som chef for Hvidvasksekretariatet.

Erik har tidligere været leder af en efterretnings- og analyseenhed i National enhed for Særlig Kriminalitet (NSK). Han har en lang karriere bag sig som efterretnings- og analyseleder og har også haft et kortere ophold i den private sektor, hvor han arbejdede med bekæmpelse af hvidvask.

Gennem årene har Erik arbejdet med efterretning og analyse på både strategisk og operativt niveau. Netop balancen mellem det strategiske overblik og den konkrete indsats er en central del af Eriks ledelsesstil, hvor han i tidligere stillinger i politiet har haft fokus på at skabe effektfulde og målrettede indsatser. Erik ser meget frem til at bidrage til bekæmpelsen af hvidvask og terrorfinansiering i et tæt samarbejde med de mange aktører på området:

"Hvidvask er et stort og samfundsundergravende problem. Men ingen kan bekæmpe hvidvask alene, og jeg ser frem til at være med til at styrke samarbejdet mellem offentlige og private aktører." siger han.

Som chef for Hvidvasksekretariatet deltager Erik som Head of FIU i diverse internationale fora, herunder i Egmont og i FATF-regi samt i de strategiske nationale fora, der er etableret på hvidvaskområdet i Danmark.



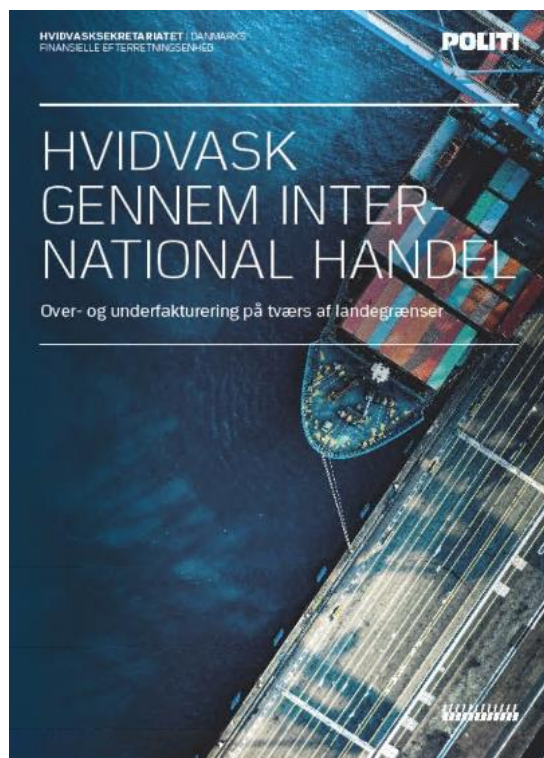
Ny temarapport: Hvidvask gennem International handel

Hvidvasksekretariatet har udgivet temarapporten [Hvidvask gennem international handel](#), hvor vi sætter fokus på, hvordan over- og underfakturering kan bruges som et modus i handelsbaseret hvidvask. Rapporten er udarbejdet i tæt samarbejde med Toldstyrelsen.

Over- og underfakturering fungerer ved, at varer eller ydelser handles til en pris, der er væsentligt højere eller lavere end den egentlige værdi. Uoverensstemmelsen imellem den handlede pris og den egentlige værdi af varen eller ydelser muliggør, at kriminelle aktører kan sløre oprindelsen af et beløb tilsvarende differencen mellem pris og værdi. Værdien af differencen bliver derved flyttet fra et land til et andet og på en måde, der er sløret for myndighederne.

Baseret på data fra Toldstyrelsen i 2023 estimerer Hvidvasksekretariatet, at mellem tre og 29 pct. af importen til Danmark *fra* tredjelande er potentielt over- og underfaktureret, mens det gør sig gældende for mellem fem og 40 pct. af eksport fra Danmark *til* tredjelande. Omregnet til kroner og ører svarer det til en samlet værdi på mellem 300 og 589 milliarder kroner af potentielt over- og underfakturerede import- og eksportvarer. Det er ikke et udtryk for, at der hvidvaskes for det beløb gennem international handel, men *alene et værdimæssigt estimat af potentiel over- og underfakturering*. Der kan være mange valide årsager til, at varer statistisk fremgår som over- og underfakturerede og afviger fra normalprisen. Det kan fx skyldes, at der er tale om varer af meget højere eller lavere kvalitet end gennemsnittet. Det kan du læse meget mere om i rapporten.

Formålet med temarapporten er at gøre opmærksom på over- og underfakturering som hvidvaskmodus, og den er primært henvendt til de virksomheder og personer, der i henhold til hvidvaskloven er underretningspligtige, samt de myndigheder, der deltager i bekæmpelsen af hvidvask. Rapporten er endnu en opfølgning på temarapporten [Handelsbaseret hvidvask](#) som Hvidvasksekretariatet udgav i december 2022. I 2024 så vi nærmere på den del af handelsbaseret hvidvask, der knytter sig til tredjepartsbetalinger i temarapporten [Hvidvask via tredjepartsbetalinger](#).



Finanstilsynet udgiver *God praksis for interne kontroller tilknyttet insiders*

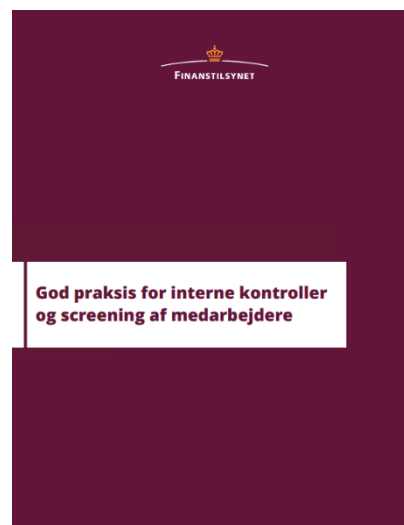
Det er en særskilt risiko, hvis man har medarbejdere, der bistår kriminelle. I de senere år er udfordringer med insiders i banker og andre virksomheder også dukket i Danmark. For at støtte finansielle virksomheder i at imødegå denne risiko præsenterer Finanstilsynet i et nyt notat en række tiltag, som udgør god praksis for interne kontroller og screening af medarbejdere i finansielle virksomheder. Notatet tager udgangspunkt i erfaringer fra forespurgte finansielle virksomheder, erfaringer fra Finanstilsynets inspektioner og internationale observationer. Notatet adresserer:

- Screening ved ansættelse og løbende ajourføring
- Håndtering af udsatte medarbejdere
- Kontrol ved onboarding af kunder
- Usædvanlig adfærd hos medarbejderen
- Opmærksomhed ved behandling af alarmer
- Foranstaltninger ved mistanke om misbrug af stilling

Virksomhederne er i henhold til hvidvasklovens § 8, stk. 1, forpligtede til at have skriftlige politikker, forretningsgange og kontroller, som skal omfatte blandt andet screening af medarbejdere og intern kontrol til effektiv forebyggelse, begrænsning og styring af risici for hvidvask og finansiering af terrorisme. Virksomhederne skal i den forbindelse have procedurer og interne kontroller, som sikrer mod at en medarbejder misbruger sin stilling.

Finanstilsynet bemærker, at det frem for alt er vigtigt, at virksomhederne er bevidste om deres egne sårbarheder, så de kan målrette deres indsats mod de områder, hvor det er nødvendigt at reducere eller helt fjerne en sårbarhed. Finanstilsynet fremhæver dog samtidigt, at screening af medarbejdere og interne kontroller ikke skal medvirke til en øget mistænkelighedskultur på arbejdspladsen, og at det forventeligt kun er et ganske lille fåtal af medarbejdere, der hjælper eller potentielt vil hjælpe kriminelle.

Du kan læse hele Finanstilsynets notat [her](#).



Terrorfinansiering i en international kontekst

Henover sommerperioden har FAFT og Europol udgivet en række relevante og aktuelle rapporter vedrørende terrorfinansiering, proliferationsfinansiering og terrorisme i EU, som kort præsenteres her. Særligt fremhæves den omfattende FAFT-rapport om terrorfinansiering, der er en samlet og opdateret version af tidligere udgivelser på området. Rapporten er udarbejdet af eksperter fra 18 medlemslande, herunder Danmark, samt fra en række øvrige internationale organisationer.

Fælles for rapporterne er, at de er skrevet i en international kontekst og dækker globale forhold. Rapporterne indeholder vigtig viden om risici, metoder, indikatorer, tendenser og forventet udvikling de kommende år.

FATF: Comprehensive Update on Terrorist Financing Risks

Rapporten er inddelt i fire sektioner. Sektion 1 beskriver faktorer, der kan påvirke risici for terrorfinansiering på forskellig vis. Dette kan være geografiske faktorer, eksempelvis konfliktområder eller i områder hvor terrororganisationer kan have større eller mindre territorial kontrol, ligesom korrupsion eller statslig støtte også kan have indflydelse. Truslen for terrorisme, typen af aktører og eksponering for propaganda kan også påvirke risici for terrorfinansiering.

Sektion 2 indeholder en detaljeret gennemgang af metoder, som aktørerne kan benytte til at frem-skatte, opbevare, overføre og anvende økonomiske midler til terrorfinansiering. Rapporten beskriver således, hvordan en lang række virkemidler og metoder kan udnyttes i en terrorfinansieringsproces, herunder ved brug af kontanter, pengeoverførselsvirksomheder, traditionelle finansielle services, digitale platforme, sociale medier, kryptovaluta og andre virtuelle aktiver, udnyttelse af naturressourcer samt via øvrige forskellige former for legale og ulovlige aktiviteter. Afsnittet er desuden suppleret med en række konkrete eksempler.

Sektion 3 fremhæver tendenser og udviklinger på området for terrorfinansiering. Der nævnes blandt andet forskellige geografiske og demografiske tendenser, ligesom teknologiuudvikling selvsagt er et centralt emne. Det fremgår desuden, at der fortsat er en decentralisering på terrorfinansieringsområdet, det vil sige, at terrorceller globalt i højere grad er selvfinansieret fremfor at modtage midler fra moderorganisationen. FATF vurderer ligeledes, at der er en større spredning i metoderne til at frem-skatte og overføre økonomiske midler i terrorfinansieringssammenhæng for at gøre det vanskeligere for myndigheder at opdage finansielle netværk. Herudover fremhæves blandt andet også stigende udfordringer i tilknytning til børn og unges eksponering for online propaganda, fundraising, udnyttelse af humanitær hjælp til terrorfinansierings-formål samt risici forbundet med klimaændringer.

Sektion 4 fremsætter en række policy-anbefalinger baseret på FATF-standarderne og pointerer i særdeleshed behovet for øget internationalt samarbejde og samarbejde mellem myndigheder og den private sektor. Afslutningsvis indeholder Bilag A en detaljeret liste over konkrete indikatorer på

terrorfinansiering inddelt i forskellige kategorier, eksempelvis kundeadfærd, geografiske risici, non-profit organisationer, nye teknologier eller i tilknytning til specifikke transaktioner eller finansielle produkter. Indikatorerne kan sjældent stå alene og bør ofte vurderes i en større kontekst, men Hvidvasksekretariatet anser indikatorerne for at være relevante i underretningspligtiges løbende transaktionsmonitorering og kundekendskab.

Du kan læse hele FATF-rapporten om terrorfinansiering [her](#).

Europol: European Union Terrorism Situation and Trend Report 2025

Rapporten indeholder et større overblik over sager, udviklinger og tendenser vedrørende terrorisme, samt finansiering heraf, inden for grænserne af EU i 2024. Der indgår således også flere forhold med relation til terrorfinansiering. Det fremgår blandt andet, at der er identificeret flere sager om terrorfinansiering med tilknytning til Islamisk Stat via økonomiske overførsler til familiemedlemmer, der opholder sig i syriske lejre.

Rapporten pointerer, at de økonomiske midler i sager om terrorfinansiering både kan være opnået på legal og illegal vis, og at de mest hyppige former for midlers oprindelse inkluderer almindelig indkomst samt online donationer og fundraising. Herudover nævner Europol også kryptovaluta og andre virtuelle aktiver, der kan benyttes til at omgå traditionelle finansielle systemer på tværs af grænser. Europol fremhæver, at der fortsat anvendes et mix af forskellige former for overførsler af økonomiske midler til finansiering af terrorisme, herunder traditionelle finansielle systemer, digitale banker, pengeoverførselsvirksomheder og kryptovaluta.

Du kan læse hele Europols rapport [her](#).

FATF: Complex Proliferation Financing and Sanctions Evasion Schemes

Proliferationsfinansiering er betegnelsen for finansiering af masseødelæggelsesvåben. Det kan omhandle forskellige former for finansiell støtte samt import og eksport af produkter, der enten direkte eller indirekte kan bidrage til at producere masseødelæggelsesvåben. FATF-rapporten udpeger Nordkorea som den største trussel i forbindelse med proliferationsfinansiering og identificerer særligt fire overordnede metoder, der kan benyttes til at omgå sanktioner målrettet proliferationsfinansiering:

- Brug af skuffeselskaber og tredjelande til at omgå sanktioner
- Sløring af ejerskab af virksomheder for at opnå adgang til det finansielle system
- Benyttelse af virtuelle aktiver og andre teknologier
- Udnyttelse af den maritime sektor

Du kan læse hele FATF-rapporten om proliferationsfinansiering [her](#).

Vil du vide mere?

Kinesisk milliardsvindel med tråde til Danmark

Et kinesisk netværk er afsløret i svindel for mindst 5,2 milliarder kroner i EU, og sagen trækker også tråde til Danmark. Netværket har tilsyneladende sendt varer fra Kina til blandt andet Danmark via havne i Sydeuropa. Importøren skal ifølge EU's regler først betale moms, når varerne ankommer til det land, der fremgår som slutmodtager. Derfor betales der ikke moms af varerne, når de ankommer til havnene i syd. Men varerne sendes aldrig længere end til lande i Sydeuropa, hvor de placeres på hemmelige lagre og sælges på det sorte marked. Profitten sendes retur til Kina.

Den Europæiske Anklagemyndighed (EPPO) udførte den 25. juni i år 101 ransagninger på tværs af Athen, Madrid, Paris og Sofia. Målene var alt fra toldmæglere til transportfirmaer, skatterådgivere og advokater – foruden rækken af kinesiske illegale logistikcentre. Der blev blandt andet beslaglagt valutaer, herunder kryptovaluta, for 43 millioner kroner, mere end 7.000 el-cykler, 11 ejendomme, 27 køretøjer, dyre ure og smykker samt våben. Ti personer blev arresteret, herunder to fra toldvæsenet.

EPPO har efterforsket sagen siden sidste år og rammer et omfattende kinesisk netværk, der nu er anklaget for at »oversvømme« EU-markedet med ulovligt importerede varer.

EPPO anslår, at EU-landene i den konkrete sag er blevet svindlet for mindst 5,2 milliarder kroner – men formentlig markant mere.

EPPO har siden 2021 haft til formål selvstændigt at efterforske og føre straffesager om økonomisk kriminalitet relateret til EU-midler. Du kan læse mere om sagen hos EPPO [her](#).



Dansk narkobande mistænkt for forsøg på indsmugling af næsten 1,7 ton kokain

Spanske og portugisiske myndigheder har slået til mod en dansk narkobande og anholdt i alt fire personer, heraf tre danskere, der er mistænkt for forsøg på indsmugling af næsten 1,7 ton kokain til en markedsværdi i Danmark på omkring 850 millioner kroner. De blev anholdt på deres båd. Samtidigt har spansk politi foretaget to ransagninger i Torremolinos, hvor der er beslaglagt 63.000 euro i kontanter og en række andre genstande.

DR Nyheder skriver, at politiet konkret har fundet en kobling mellem den danske narkobande og kriminelle i sydamerikanske narkokarteller, hvor kokainen menes at komme fra. Du kan læse mere om sagen [her](#).

EU-domstolen fastslår, at Maltas Golden Passport-program er ulovligt

I april slog EU-domstolen fast, at Maltas tildeling af statsborgerskab via investeringer er ulovlig. I en erklæring udtalte domstolen, at EU-retten kræver, at en vellykket ansøgning om statsborgerskab

skal være baseret på "en reel tilknytning til landet", og at Maltas program, der tilbyder statsborgerskab til gengæld for investeringer, "svarer til kommercialiseringen af tildelingen af statsborgerskab i en medlemsstat og dermed unionsborgerskab".

Court of Justice of the European Union:

"While the definition of the conditions for granting and losing the nationality of a Member State is a matter of national competence, that competence must be exercised consistently with EU law. The bond of nationality with a Member State is based on a specific relationship of solidarity, good faith and the reciprocity of rights and duties between the State and its citizens. Where a Member State grants nationality, and thus automatically Union citizenship, in direct exchange for predetermined investments or payments through a transactional procedure, it manifestly infringes those principles. Such 'commercialisation'

Ifølge Organized Crime and Corruption Reporting Project (OCCRP) er Malta den eneste tilbageværende EU-medlemsstat, der tilbyder statsborgerskab gennem investering, efter at Bulgarien og Cypern har afviklet deres programmer.

Du kan læse mere om sagen [her](#) og hos Court of Justice of the European Union [her](#).

Har du brug for at komme i kontakt med os?

Har du spørgsmål eller kommentarer til kvartalsrapporten, er du velkommen til at kontakte os via vores mail, som er fiu@politi.dk.

Du er også altid velkommen til at læse mere om hvidvask på www.hvidvask.dk. Her finder du også andre rapporter, fx årsrapporter, kvartalsrapporter og temarapporter fra Hvidvasksekretariatet. Materialet får du også adgang til, hvis du er oprettet i GoAML.



The screenshot shows the website of Hvidvasksekretariatet (National Unit for Serious Crime). The header includes the organization's name and a search icon. A navigation menu on the left lists: Genveje, Underret om hvidvask, Om Hvidvasksekretariatet, Udgifter, Ofte stillede spørgsmål, and Kontakt Hvidvasksekretariatet. The main content area features a section titled 'Nyheder fra Hvidvasksekretariatet' with three news items:

- 10. juni 2025**
Hvidvasksekretariatet
Ny temarapport: "Hvidvask gennem international handel"
Hvidvasksekretariatet sætter i denne udgivelse fokus på, hvordan over- og underfakturering kan bruges som et modus i handelsbaseret hvidvask.
- 28. maj 2025**
Hvidvasksekretariatet
Kvartalsrapport for 1. kvartal 2025
I denne udgave kan du blandt andet læse om, hvordan Hvidvasksekretariatet har fokus på svindel med velfærdydelse og hvidvask af midler, der stammer herfra, og om samarbejder med aktører på socialområdet.
- 2. april 2025**
Hvidvasksekretariatet
Vejledning til GoAML er blevet opdateret
Vi har opdateret vejledningerne til GoAML for at gøre det lettere for underretningsspligte at sende de lovpligtige underretninger ved mistanker om hvidvask.