Diskussionsoplæg:
Hvordan står det til med bekæmpelsen af hvidvask af penge

med bidrag fra Jan Damsgaard, Jonas Hedman and Kalle Johannes Rose
CCG, CBS

Resumé:

Nu hvor Danmarks Finansbranche er kommet op på det internationale niveau for anti-hvidvask af penge (AML) (og andre) compliancestandarder, er det tid til at se på systemet på en holistisk måde og stille spørgsmål om effektivitet, procesoptimering og omkostninger. Compliance er vigtigt, da det teoretisk set sikrer et rent finansielt system og giver effektiv støtte til politiet i blandt andet bekæmpelse af organiseret kriminalitet.

Vores pointe i denne korte indledning er, at det globale AML-compliancesystem ikke gør meget for at afskrække professionelle aktører fra hvidvaskaktivitet. For i øjeblikket bruger vi for meget tid på de 'små' fisk, og ikke de 'store aktører'. Systemet medfører dog betydelige omkostninger for bankerne og dermed samfundet som helhed (en hurtig og uformel udregning anslår de årlige omkostninger til compliance i banker, der opererer i Danmark, til knap DKK 7 mia. om året).

Som vi har argumenteret for i nogen tid, skal systemet gendesignes, så det er tilstrækkeligt risikobaseret, og således at store dele af det automatiseres. Dette vil både reducere omkostningerne og sikre en bedre brug af compliance-medarbejdere, når de fokuserer på risikovægtede undersøgelser.

Vi kommer med en række anbefalinger om teknisk automatisering nedenfor, men en vigtig forudsætning vil være, at både lovgivningen og de finansielle myndigheders retningslinjer bliver harmoniseret på tværs af de nordiske lande.

Præambel

Efter Danske Banks hvidvaskskandale – og lignende problemer hos Nordea, Swedbank og andre – var der generel bestyrtelse over, at sådan noget kunne være sket i et velfungerende land som Danmark. Det generelt høje niveau af tillid i det danske samfund betød, at det havde en lav prioritet, formentlig kombineret med en manglende forståelse for, at hvidvask af penge (herefter angivet ML) er et globalt fænomen, der ikke respekterer lokale normer. Efter at have foretaget de nødvendige investeringer i processer og mennesker, er det nu tid til at tænke på, hvordan man løfter systemet op til næste niveau, så at det bliver meget bedre, hurtigere og billigere. Danmark – og dets generelt høje digitaliseringsniveau – kan i princippet være den ideelle læreplads på AML-området, hvis institutionerne tillader det. Som det så ofte sker, kan en krise katapultere et land fra at være efternøler til at blive leder inden for et område, forudsat at det træffer de rigtige valg.

Opgavens omfang og baggrund

ML opstår, når kilderne til midler skal skjules af den ene eller anden grund. Dette betyder, at vi for at kunne definere et effektivt forsvar mod ML skal have en ordentlig forståelse eller taksonomi for efterspørgslen efter ML-tjenester. Ingen forstår helt, hvor stort problemet egentlig er, men skøn over størrelsen af den illegale økonomi spænder fra 1 % til 5 % af et givet BNP. Med det globale BNP på omkring 100 billioner USD, varierer de mængder, der globalt og hvert år skal 'vaskes' fra 1 billion

USD til 5 billioner USD. Uanset det rigtige tal, er det et betydeligt beløb, der lægger et alvorligt pres på alle AML-systemer rundt om i verden. Efterspørgslen efter disse ML-tjenester vil komme fra organiserede kriminelle grupper, der opererer professionelt over hele verden. Deres primære indkomststrøm vil være fra narkotikahandel, men mange af deres andre indkomstkilder vil være mindst lige så skadelige (hvis ikke mere) for samfundet: Handel med illegale stoffer, illegal våbenhandel, menneskeligt slaveri, seksuel udnyttelse af børn, afpresning og bedrageri, miljøkriminalitet og på det seneste cyberkriminalitet.

Der vil være yderligere kilder til midler, som ikke er det direkte udbytte fra traditionel kriminel aktivitet, nemlig underslæb med statsmidler, skatteunddragelse, valutakontrol og alvorlig korruption, der ofte stammer fra lande med svage institutioner. Beløbene kommer oveni de ovenfor nævnte[1]. Der er også spørgsmålet om bekæmpelse af terrorfinansiering (CTF), som blev føjet til AML-systemet efter 9/11-angrebene i USA. Men i modsætning til nogle af de politiske aktører for dette CTF-initiativ, så tvivler vi på, at de finansielle institutioner er de rigtige til at stoppe det, og argumenterer for, at en bedre tildeling af midler til politiet kan give samfundet et meget bedre afkast – men mere om det senere.

Folk spørger ofte om, hvor stort problemet er i forhold til de danske banker, eller de nordiske banker mere generelt, og det ærlige svar er, at ingen helt ved det. For at give en indikation, henviser den seneste vurdering fra den Danske Nationale Risikovurdering af Hvidvask til en FN-beregning, som anslår den til omkring 68 mia. kr. årligt[2]. Men givet det konstante pres på systemet, er det næsten irrelevant at anslå det potentielle omfang, da vi ved, at hvidvask-professionelle vil gøre brug af muligheden i det øjeblik, forsvarsværkerne svækkes (som det skete tidligere).

For at opsummere er problemet, vi står over for, at der hvert år er billioner af amerikanske dollars (eller tilsvarende i andre respektive valutaer), som skal omdannes til legitime midler, så de kan være til nytte for deres modtagere. Og givet størrelsen af den konstante kapitalstrøm, betyder det også, at der vil være et konstant pres på alle forsvarsværker globalt, og søger disse kriminelle aktører konstant efter det svageste led.

Effektivitet og gennemslagskraft i det nuværende system

En måde at vurdere effektiviteten af et AML-forsvar er at se på markedsprisen for professionelle hvidvasktjenester. Det er klart, at der ikke er et åbent marked for den slags tjenester, og der findes et stort spektrum med hensyn til hvilke mængder, der håndteres. Vi ved dog fra forskellige europæiske politikilder (og andre), at for meget store beløb er markedsprisen et sted i intervallet 8 % (eller mindre). Det er klart, at prisen for mindre beløb stiger, men overstiger ofte ikke 20%. Det betyder, at efter fradrag af omkostningerne (bestikkelse osv.) ved aktiviteten, er den eventuelle opdagelsessandsynlighed tæt på nul. Men vi tror, at det, vi bliver nødt til at acceptere, både er, at markedet er meget effektivt, og at de professionelle ikke frygter at blive opdaget. Vi får dog 'fat i' folk i processen. Mange af dem kan imidlertid betegnes som små og/eller uerfarne og er sandsynligvis dem, der ikke vil forårsage meget skade på samfundet (og som vi derfor ikke er virkelig interesserede i). Vi bemærker dog, at processen påfører kunderne betydelige omkostninger i form af meget højere transaktionsomkostninger (åbning af konti, flytning af større beløb eller fremskaffelse af bevis for indtægter/omkostninger). Det pålægger også bankerne betydelige omkostninger i form

[1] Desuden vil der være problematiske kilder til kapital, der skyldes omgåelse af valutakontrol, men dette er mere et problem i Asien, da store mængder kapital forsøger at forlade Kina.
[2] DEN NATIONALE RISIKOVURDERING AF HVIDVASK (2022); p. 15.

af meget højere complianceomkostninger for AML og andet. I appendiks A opsummerer vi nogle hurtige og uformelle beregninger, der anslår de årlige omkostninger til compliance-arbejde for banker med virksomhed i Danmark til lidt under DKK 7 mia. årligt. Efter min mening er det et bemærkelsesværdigt beløb, og sandsynligvis står det ikke i et fornuftigt forhold til den skade, der forårsages af dem, vi sandsynligvis vil opdage (små eller uerfarne, som nævnt ovenfor).

Vi argumenterer ikke for, at vi skal reducere vores fokus på at forhindre mistænkelige transaktioner. Men vi argumenterer for, at vi som samfund (globalt) bliver nødt til at udvikle løsninger, der er meget bedre, billigere og hurtigere (effektive og med gennemslagskraft). Et skridt i denne retning vil være at få en bedre forståelse af efterspørgselssiden, med andre ord de kriminelle, der gør brug af hvidvasktjenester. En anden er at bruge de data, vi har, meget bedre, forbedre vores empiriske modeller på mange forskellige måder og dele data (hvilket, vi mener, kan gøres uden at overtræde eksisterende lovkrav).

Vores overordnede målsætning må være at designe et finansielt system, der på den ene side er meget effektivt, men på den anden side ikke lader sig misbruge af tvivlsomme aktører til at hvidvaske penge fra kriminelle eller andre ulovlige eller problematiske kilder.

Banker som en forlængelse af politimyndighederne?

Før vi dykker ned i de tekniske detaljer vedrørende bedre detektionsmodeller, vil vi vende tilbage til en tanke, vi henviste til tidligere, da vi talte om terrorfinansiering.

Begyndende med beslutninger fra G7 og efterfulgt af internationale aftaler og standarder koordineret gennem FATF (Financial Action Task Force) i Paris, har politikerne globalt givet alle banker en væsentlig rolle i retshåndhævelsen ved at få dem til at følge pengene og opdage mistænkelige betalingsaktiviteter. Dette skal dog endnu ikke understøttes ved at give bankerne det vidtrækkende ansvar, der er nødvendigt for at udføre arbejdet effektivt. Ikke at give dem vidtrækkende beføjelser er klart det rigtige at gøre, da vi ikke ønsker, at bankfolk skal være politibetjente. Men på den anden side gør det dem også ineffektive i forhold til nogle af deres opgaver, da de ikke har adgang til de samme data, værktøjer og rettigheder/beføjelser som retshåndhævende myndigheder.

Derfor kan det til tider og med specifikke opgaver (f.eks. finansiering af terrorisme) være mere fornuftigt at betænke politimyndighederne og potentielt finansiere dem med en afgift fra bankerne (der er mindre end complianceomkostningerne for den specifikke opgave). Den enkle idé er, at afkastet til offentlig sikkerhed kan være højere, når man bruger penge på politiet end på banker. Det er klart, at politiet så vil være ansvarligt for samtlige aktiviteter, selvom de finansieres gennem en bankafgift.

NÆSTE SKRIDT

Skal lovgivningen harmoniseres på tværs af Norden?

Den første anbefaling, vi kommer med, er af ikke-teknisk karakter: at harmonisere lovgivning og håndhævelse af compliance på tværs af Norden. Dette arbejde bør strømlines og man bør foretage et større nordisk samarbejde, hvor de forskellige systemer og lovgivning bliver standardiseret.

Historisk set har hvert land sin egen juridiske ramme, der er styret af EU-regulering. I det seneste EU AML-direktiv har de enkelte medlemslande mindre fortolkningsrum, hvilket naturligvis vil fremtvinge

en vis standardisering. Når det er sagt, bør målet være at udvikle tekster så identiske med hinanden som muligt, ikke mindst da vi også ønsker at opnå en standardisering af de forskellige finansielle regulatorers regelsæt og handlinger sammen med private offentlige (og akademiske) partnerskaber (OPP'er), skattemyndigheder på tværs af Norden. I det lange løb kan dette tjene som en plan for en bredere europæisk samarbejdsramme. Dette har flere vigtige fordele:

- Banker, der opererer på tværs af Norden, opererer typisk med én regelbog, hvilket betyder, at de kan være (tæt på) at overtræde reglerne i det ene eller det andet land. Dette betyder også, at visse aktiviteter muligvis skal gentages med høje omkostninger til følge på tværs af de forskellige lande.
- Det vil give mulighed for standardisering af processer og it-systemer, hvilket også kan føre til centralisering af visse aktiviteter på tværs af grænserne.
- I betragtning af landenes ringe størrelse er videnspuljen af personer, som indgående kender den nationale lovgivning, og som enten kan udarbejde regler eller rådgive om dem, også meget begrænset. En standardisering af lovgivningen vil give mulighed for en væsentlig udvidelse af videnspuljen, forbedre debatten og dermed også kvaliteten af den rådgivning, der kan gives.

Forbedre datadeling

I appendiks C diskuterer vi indgående de juridiske aspekter af deling af relevante AML-data på tværs af banker i Danmark. Vi konkluderer, at vi ikke ser nogen grund til, at dette ikke skal ske, så en effektiv vurdering af transaktioner (og kunder) kan finde sted. Her vil danske bankers datacentre som Bankdata, BEC eller SDC være et praktisk sted at starte, men som sagt, dette kan og bør standardiseres og automatiseres.

Hvordan kan man forbedre detektion?

Som allerede omtalt er problemet, vi står over for, at offentligheden (via banktjenester) investerer et betydeligt beløb i at detektere ulovlige betalinger og aktører, mens denne indsats har sandsynligvis ringe indflydelse på de faktiske AML aktiviteterne (målt ud fra markedspriser).

Dette sker, fordi den nuværende empiriske tilgang til detektion mangler en 'udfaldsvariabel'. Derfor kan vi ikke køre en regression eller en maskinlæringsmodel uden en fundamentalt anderledes tilgang (som vi foreslår nedenfor). Branchen hjælper sig selv ved at stole på såkaldte 'scenarier', som i al væsentlighed er tidligere tilfælde af ML, som man har observeret. Disse scenarier er også meget begrænsede i antal (typisk <130) og er sandsynligvis også kendt af den 'anden side'. Under alle omstændigheder er de af begrænset betydning. Vi skal også huske på, at større banker har langt flere ressourcer og dermed sandsynligvis har højere standarder end nogle af de (mange) mindre banker i Danmark i forhold til ML-processer.

Når det er sagt, er der efter min mening mange måder at foretage en trinvis ændring på med hensyn til effektiviteten af detektionsalgoritmerne, hvis blot vi tillader eksperimenter med forskellige tilgange.

Nøglen vil være at flytte vores detektion fra individuelle observationer (hvor vi naturligvis vil støde imod grænserne for privatliv og GDPR-lovgivningen) til aggregering indenfor mindre områder. Her dropper vi alle personligt identificerbare oplysninger og erstatter dem med en områdeindikator for, hvor den private person bor, eller i tilfælde af virksomhed, hvor vedkommende opererer. Denne aggregering indenfor mindre områder fungerer rigtig godt, og tidligere har det givet os mulighed for

at opbygge en referencemodel for kriminalitetsforudsigelse for Storbritannien. Disse mindre områder fungerer så godt, fordi folk selv vælger at tilslutte sig grupper, der minder om dem selv i forhold til, hvor de vælger at bo (du ligner meget din(e) nabo(er)). Dette giver os igen mulighed for at forstå den socioøkonomiske struktur, præferencer og velstandsforhold i ethvert område – alt hvad vi behøver at vide for at få en god forudsigelsesmodel. Og da oplysningerne nu er fri for databeskyttelse problemer har vi et format, der giver os mulighed for at dele data mellem banker og mellem myndigheder og banker. Dette kan også være en måde at tage det meget vigtige arbejde i det danske JIMLIT-initiativ videre til næste niveau og hjælpe med at automatisere det.

De nordiske lande, som er blandt de mest digitalt kyndige og velorganiserede samfund, ville være et perfekt laboratorium for eksperimenter på dette område. De har været trendsættere i forhold til meget digital innovation, og det vil være naturligt, hvis de også fører an på dette område. Vi tror, at udbyttet for samfundet ville være enormt.

Banktilsynsmyndighedens centrale rolle

For at lykkes med et hvilket som helst innovationsinitiativ på dette område er det altafgørende, at banktilsynsmyndigheden er med på det. Banker vil ikke innovere ud over de klare retningslinjer, som tilsynsmyndigheden har fastsat, da de ikke ønsker at blive irettesat. På den anden side har banktilsynsmyndigheden typisk ringe appetit på at fremme innovation, og det er der mange grunde til, ikke mindst da tilsynsmyndigheden opererer inden for lovens og andre reglers grænser, som typisk ikke giver mulighed for at eksperimentere. Desuden giver Folketingets lov om Finanstilsynets sandkasse ikke plads nok til, at sandkassen kan bruges til dette formål (AML-test). Derfor er vi fastlåst i en negativ stationær tilstand mellem en risiko-utilbøjelig administration, banker, der blot vil overholde reguleringen, og en industri, der sælger løsninger til overpris, men kun leverer begrænsede ændringer på området.

Det betyder kort sagt, at hvis vi virkelig ønsker at forbedre effektiviteten og gennemslagskraften i AML-procedurer i banker, er vi nødt til at tænke over, hvordan vi kan bemyndige – og endda instruere – tilsynsmyndigheden til systematisk at tillade eksperimenter i banker. For at opnå dette skal vi også sikre lige adgang til en – lad os kalde det Sandkasse 2.0 – og til en vis grad potentielt endda fritage banker for visse risici, de tager i processen i en begrænset periode.

Pre-clearance, føderale systemer og digitale valutaer (CBDC'er)

På mellemlangt sigt ville et alternativ være at forhånds-cleare aktørerne og give dem såvel som deres transaktioner en ren sundhedsattest på forhånd. Velegnede er de såkaldte føderale (*federated* på engelsk) systemer – og vi diskuterer anti-hvidvask-anvendelsen af dem i detaljer i bilag B – hvor vi stoler på en anden banks beslutning om arten af en transaktion eller kunde. Dette kunne nemt implementeres i de ovennævnte bankdatacentre og vil spare de deltagende banker for betydelige pengebeløb, da de kan ophøre med en gentagelse af aktiviteter. Der er spørgsmålet om ansvar, men i praksis vil risikoen i velfungerende systemer være lille. Desuden skal vi huske på, at i et risikobaseret system er fejl uundgåelige (de forekommer også i øjeblikket, men i det nye system vil vi være åbne omkring dette), og på kort sigt kan eventuelle potentielle bøder og tab blive dækket af besparelserne ved at undgå dobbeltarbejde. Et sådant system vil også kræve en god feedback-loop, som vil være let at implementere. Et sådant system kan derefter overføres til centralbankudstedte digitale valutaer (CBDC'er, såsom e-kronen eller e-EURO), hvis og når de bliver udstedt.

Appendiks A: Hvad danske pengeinstitutter bruger på compliance og AML

I det følgende forsøger vi at estimere de sandsynlige årlige omkostninger ved 'Compliance og AML' hos banker i Danmark (dvs. den danske drift af både lokale og internationale banker). Vi baserer vores analyse på tallene fra Danske Bank, da det er den eneste bank, der offentliggør sådanne tal som en del af deres regnskab. Det betyder naturligvis, at vi er udsat for en række skævheder, som heldigvis går i den modsatte retning og til dels vil ophæve hinanden. På den ene side er det sandsynligt, at Danske Bank måske investerer mere end de andre på netop dette område i øjeblikket, blandt andet for at rette op på historiske mangler. At basere det udelukkende på Danske Banks tal vil derfor betyde, at vi sandsynligvis overvurderer det samlede beløb, der er brugt i Danmark. På den anden side mangler vi de nødvendige regnskabsdata for nogle mindre banker (36 i alt), og vi udelukker dem derfor i vores analyse. Det betyder, at vi vil undervurdere det samlede beløb.

Under alle omstændigheder er formålet med denne øvelse at give et groft skøn over de sandsynlige udgifter til "Compliance and AML" og ikke at give et punktestimat. Så hvordan nåede vi frem til vores omtrentlige resultat?

Data
De regnskabsdata, der er brugt til disse beregninger, er hentet fra Orbis. Orbis kategoriserer finansielle institutioner efter forskellige konsolideringskoder, der er som følger:

- C1: Opgørelse fra en moderbank, der integrerer opgørelsen af sine kontrollerede datterselskaber eller filialer uden ikke-konsolideret partner
- C2: erklæring fra en moderbank, der integrerer erklæringerne fra sine kontrollerede datterselskaber eller filialer med en ikke-konsolideret partner
- C*: yderligere konsolideret opgørelse
- U1: erklæring, der ikke integrerer erklæringerne fra de mulige kontrollerede datterselskaber eller filialer af den pågældende bank uden konsolideret partner
- U2: erklæring, der ikke integrerer erklæringerne fra de mulige kontrollerede datterselskaber eller filialer af den pågældende bank med en konsolideret partner
- U*: yderligere ikke-konsolideret opgørelse

Til denne analyse har vi valgt at bruge konsolideringskoderne C1, C2 og U1, da vi er interesserede i det aggregerede bankforbrug.

De variabler, vi har udtrukket for perioden 2017–2020, er:

- Antal ansatte
- Samlede aktiver i USD
- Indlån og kortfristet finansiering i USD

Data for 2021 var stadig ufuldstændige på tidspunktet for vores analyse, og er derfor ikke inkluderet her.

Som vi nævnte ovenfor, indeholder Orbis ikke regnskabsdataene fra en række mindre banker, og det gør heller ikke noget andet datasæt, som vi har adgang til. Således kan vi på dette tidspunkt kun anerkende denne udeladelse og gå videre:

År	2017	2018	2019	2020	2021
Antal banker i vores dataset	79	82	79	75	71
Samlet antal virksomheder, der har en banklicens	100	96	95	90	89

Tabel 1: Det faktiske antal danske pengeinstitutter sammenlignet med antallet af pengeinstitutter, som vi trækker på fra databasen. Dette omfatter både danske banker og filialer af udenlandske banker. Det faktiske antal pengeinstitutter i Danmark er hentet fra FinansDanmark: https://finansdanmark.dk/tal-og-data/institutter-filialer-ansatte/

Så vi ser, at problemet sandsynligvis vil være større, end disse beregninger kan redegøre for.

Estimatet

	2017	2018	2019	2020	2021
USD	284.354.499	388.173.981	710.920.847	898.994.895	823.092.383
DKK	1.875.404.082	2.452.260.012	4.742.021.203	5.874.278.071	5.178.693.147

Tabel 2: De danske pengeinstitutters AML- og compliance-forbrug beregnet ud fra tal fra Danske Bank med den årlige valutaveksling fra Danmarks Nationalbank: https://nationalbanken.statbank.dk/nbf/100249.

Appendiks B: Føderal risikobaseret system til bekæmpelse af hvidvask af penge

Bekæmpelse af hvidvask er en centraliseret opgave, som hver bank udfører. For eksempel kontrollerer betalers og betalingsmodtagers banker den samme transaktion, hvilket er en del af bankernes forpligtelser, hvis de fortsat skal overholde reglerne. I et føderal system har aktører tillid til hinanden, da hver aktør opfylder sine forpligtelser, herunder risikovurderinger, Kend din kunde (KYC) og transaktionsovervågning. En illustration af, hvordan et føderal risikobaseret system fungerer, er lufthavnssikkerhed. Københavns lufthavn behøver ikke at tjekke alle transferpassagerer, der ankommer fra Berlin, fordi København stoler på, at Berlin har foretaget et grundigt sikkerhedstjek. Derfor har Københavns Lufthavn ingen grund til at gentage denne proces.

Et andet eksempel er WAYF (Where Are You From), som gør det muligt for personer med legitimationsoplysninger, for eksempel fra et nordisk universitet, en myndighed eller en offentlig institution, at logge ind i hinandens systemer. Hvis Aarhus Universitet for eksempel har tillid til studerende og Copenhagen Business School (CBS) har tillid til Aarhus Universitet, så kan CBS give Aarhus-studerende adgang til sine systemer uden at løbe nogen sikkerhedsrisiko. Et system, der bruger WAYF-principperne, er EDUROAM, som gør det muligt for akademikere og studerende, som er betroet på én institution, at logge ind på alle andre deltagende akademiske institutioners Wi-Fi-systemer.

Lad os give en illustration af, hvordan et føderal risikobaseret anti-hvidvask system kunne fungere med hensyn til betalinger. Mange transaktioner er lokale Business-to-Business eller Business-to-Consumer og involverer ofte transaktioner mellem hinanden. Så hvis bank A har tillid til bank B, som igen har tillid til sin kunde X, så kan denne tillid overføres via legitimationsoplysninger til bank A. Når kunde X foretager en transaktion med nogen af Bank A's kunder, behøver hverken Bank A eller B at kontrollere transaktionen. Bemærk, at et føderal system allerede er på plads på centralbankniveau.

Denne del af et anti-hvidvask-system vil fokusere på at begrænse uønskede transaktioner, der skader samfundet. Et føderal risikobaseret AML-system kan gøre dette. Denne type system skal kunne klare to niveauer. Det første niveau omfatter de finansielle aktører, der i dag indirekte (kriminel part bruger en eksisterende kunde hos en finansiel aktør) og direkte (kriminelle er klienter hos en finansiel aktør), anvendes som hvidvasktjenesteudbydere. Det andet niveau er de transaktioner, hvor nogle vil være uønskede. Et distribueret risikobaseret AML-system bør indeholde følgende nøgleelementer:

1. Intra-bank risikovurdering: Banken bør foretage en grundig risikovurdering for at identificere og evaluere potentielle hvidvaskrisici på tværs af forskellige forretningsområder, produkter, tjenester og geografiske placeringer og give dem en bedømmelse (1 = ingen risiko, 5 = meget risikabelt).
2. Kend din kunde (KYC): Banken har typisk allerede implementeret robuste og gennemsigtige (for andre banker) KYC-procedurer for at indsamle oplysninger om kunder og deres transaktioner, og vurderet niveauet af hvidvaskrisiko forbundet med deres transaktioner og givet dem en bedømmelse (1 = ingen risiko, 5 = meget risikabelt).
3. Transaktionsovervågning: Banken bør løbende overvåge transaktioner for at opdage og markere enhver mistænkelig aktivitet, for eksempel ændringer i transaktionsmønstre, og give dem en bedømmelse (1 = ingen risiko, 5 = meget risikabel).
4. Indberetning og undersøgelse: Banken bør kunne indberette mistænkelig aktivitet til de relevante myndigheder og foretage undersøgelser efter behov.

5. Feedback: Relevante myndigheder og banker skal oplyse transaktionsoplysninger.

Element 1-3 er nøglen til oprettelse af transaktionsoplysninger. Det er transaktionen, ikke kunden, der er i fokus i et føderal transaktionsovervågningssystem.

Appendiks C: Forordning om datadeling og bekæmpelse af hvidvask af penge

Fra inkorporeringen af det 4. AML-direktiv (4AMLD) i EU er der blevet lagt stor vægt på den betydelige indvirkning, som datadeling mellem finansielle institutioner kan have på forebyggelsen af ML. Tilgangen til datadeling i Danmark er dog fortsat noget forsigtig. En forklaring på dette kan findes, hvis vi ser på de enkelte aktører og deres indbyrdes samspil. Med hensyn til de finansielle institutioner er sanktionsniveauet for overtrædelse af privatlivsforordningen (uanset om det er GDPR eller EU's charter om grundlæggende rettigheder) ret højt. Fordi de regulatoriske grænser mellem AML-regulering og GDPR er uklare, kan de finansielle institutioners adfærd forklares med den simple frygt for sanktionering fra tilsynsmyndigheden. Ydermere, er der uenigheder om, hvorvidt bankerne, grundet bankhemmelighedsreglen, kan dele information om kunder med hinanden, hvis balancen mellem AML-reguleringen og GDPR skulle tillade dette.

På den anden side har de kompetente myndigheder i Danmark også haft en meget reaktiv holdning til datadeling. De kompetente myndigheders adfærd i Danmark kan til dels forklares med uklarheden i EU-forordningen i sig selv, som indtil den nylige EF-Domstols dom af 22. november 2022 ikke har været klar rent juridisk. Men forklaringen skal også findes i en generel mangel på kompetencer eller forståelse for risikobaseret regulering. Hvis de kompetente myndigheder havde en omfattende forståelse af den risikobaserede tilgang til regulering, ville de have været i stand til at adressere datadeling på en proaktiv måde, simpelthen fordi uklarheden mellem privatlivsregulering og AML-regulering er forårsaget af den risikobaserede tilgang. Som følge heraf har den reaktive tilgang fra de nationale kompetente myndigheder øget frygten for sanktioner i den private sektor, hvilket mindsker incitamentet til at dele data.

Den lovgivningsmæssige uklarhed – eller snubletråd – mellem privatlivsbestemmelser, bankhemmelighedsregler og AML-regler er forårsaget af den risikobaserede tilgang til regulering, som er ny, især i civilretlige lande. En nylig dom fra EF-Domstolen specificerer grænserne mellem privatlivets fred og AML-regulering og præciserer, at data, der er omfattet af privatlivsbestemmelser (såsom GDPR) generelt kun kan overtrædes, hvis der er en legitim grund til at gøre det.[3] En sådan legitim begrundelse gives i AML-forordningen, hvis der er en aktuel risiko for hvidvask af penge. Begrundelsen er, at privatlivets fred er beskyttet, medmindre kriminalitet er åbenbar. Efter dette risikobaserede princip bør datadeling være mulig under to omstændigheder:

1. Hvor risikoen for hvidvask er åbenbar.
2. Hvor data ikke omfatter oplysninger, der er beskyttet af GDPR eller EU's charter om grundlæggende rettigheder.

Med hensyn til datadeling er især to tilgange blevet diskuteret, men hindret af den reaktive tilgang på grund af regulatorisk tvetydighed: deling af risikobedømmelse af kunder og deling af generiske data for at sammenligne anti-hvidvask-metodologi. Med hensyn til den første tilgang bør en deling af en risikobedømmelse på ingen måde forstås som en deling af privatlivsbeskyttede data, da risikobedømmelsen blot repræsenterer de finansielle institutioners egen opfattelse og vurdering af den tilgængelige information og iboende risici. Der bør derfor som standard ikke være nogen hindring for at dele sådanne data. I det andet tilfælde ville deling af generiske data medføre enorme

[3] EF-Domstolen C-37/20 af 22. november 2022.

fordele for samfundet og lette tilpasningen af metoden og evalueringen af risikoen for hvidvask af penge på tværs af finansielle institutioner, hvorefter en divergens i sammenligning kunne tjene som en rødt flag-indikator for enten kunden eller metoden. Hvis de indeholdte data ikke omfatter private oplysninger, bør deling af modeller og data til fordel for at føre en bedre tilgang til forebyggelse af hvidvask af penge ikke anses for at være i strid med GDPR eller EU's charter om grundlæggende rettigheder. Der er dog stadig en del uklarheder vedrørende samspillet med bankhemmelighedsreglerne i Lov om Finansiel Virksomhed.