

DANMARKS NATIONALBANK

26. JANUAR 2021 — NR. 1

Databaseret indsats styrker kampen mod hvidvask

- Nationalbanken har sammen med andre organisationer undersøgt mulighederne for at styrke indsatsen mod økonomisk kriminalitet ved hjælp af en udvidet datadrevet tilgang, der benytter detaljerede transaktionsdata.
- En udvidet risikobaseret metode på baggrund af flere datakilder afslører flere mistænkelige forhold tidligere og mere effektivt end i dag.
- Det fulde potentiale afhænger af brug af data på tværs af banker og myndigheder. En sådan sammenstilling vil kræve en lovændring.

Økonomisk kriminalitet, herunder hvidvask, har ikke alene alvorlige økonomiske konsekvenser, men også samfundsmæssige konsekvenser, fordi det skader tilliden til retsvæsenet og tilliden til den finansielle sektor.

Som et forsvarsværk i indsatsen mod økonomisk kriminalitet har den finansielle sektor ansat mere end 4.300 medarbejdere dedikeret alene til bekæmpelse af økonomisk kriminalitet og efterlevelse af lovgivningen.¹ Deres indsats resulterer i mere end 50.000 årlige indberetninger til myndighederne. Der har været tale om et støt stigende antal sager i de senere år. Trods sektorens betydelige ressourceindsats i den konstante kamp mod økonomisk kriminalitet lider systemet under nogle svagheder, der ikke lader sig løse inden for de nuværende rammer.

Nationalbanken har i samarbejde med Erhvervsstyrelsen, Statsadvokaten for Særlig Økonomisk og International Kriminalitet (SØIK), Finanstilsynet, Finans Danmark og en større bank undersøgt og vurderet mulige gevinster ved en udvidet datadrevet metode til at styrke kampen mod økonomisk kriminalitet, særligt i relation til hvidvask og momssvig.²

1 Se Finans Danmark, *Finanssektorens indsats mod hvidvask og terrorfinansiering – Afrapportering fra Finans Danmarks Hvidvask Task Force*, november 2019 ([link](#)).

2 I denne undersøgelse er sammenstilling af oplysninger fra den deltagende bank og offentlige myndigheder sket med dispensation fra erhvervsministeren. For yderligere detaljer, se boks 2 på side 7.

Data på nye måder

Mængden af data er vokset eksplosivt. Det anslås, at der i 2025 vil blive genereret mere end 450 exabyte data hver eneste dag. Det svarer til, at flere hundrede millioner almindelige computere dagligt fyldes med data. De enorme mængder data er meget forskelligartede, men nye og avancerede metoder gør det muligt at analysere dem på nye og mere effektive måder.

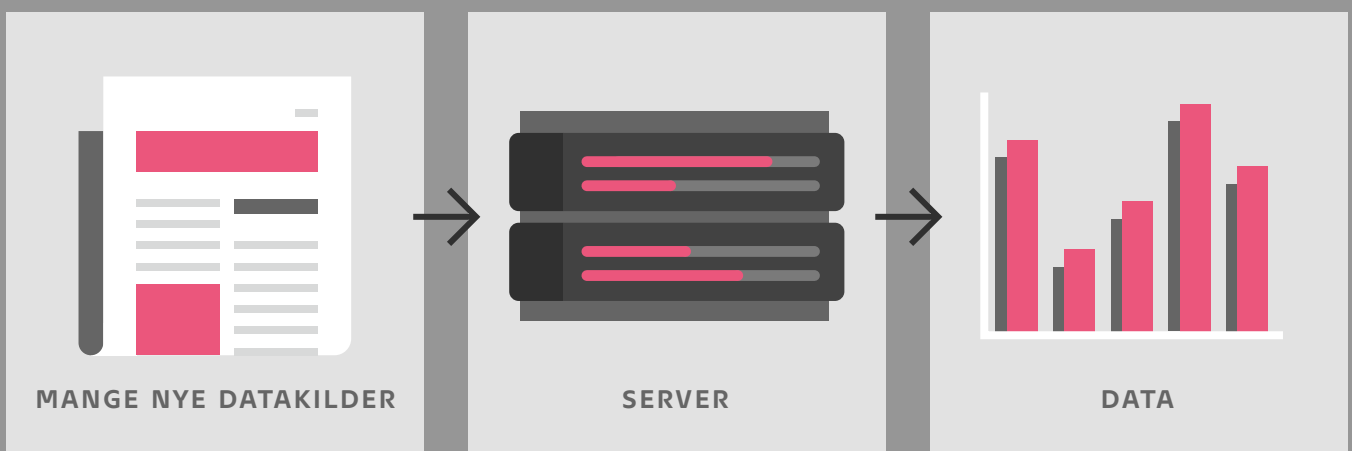
Nye typer af data og nye måder at indsamle data på kan bruges i forskellige sammenhænge i Nationalbankens løbende arbejde.

For at få mere viden og et bedre grundlag til at vurdere dansk økonomi sætter Nationalbanken fokus på de nye datatyper og metoder i en serie af udgivelser.

OM DENNE ANALYSE

Nationalbanken har i samarbejde med andre organisationer undersøgt en metode til at styrke indsatsen mod økonomisk kriminalitet. Metoden bygger på avancerede analytiske redskaber og inddrager flere datakilder, herunder detaljerede transaktionsdata. Den udvidede risikobaserede metode afslører flere mistænkelige forhold tidligere og mere effektivt end i dag.

Ny data giver ny viden



Denne analyse er et udtryk for Nationalbankens konklusioner på baggrund af den fælles undersøgelse.

Svagheder i det nuværende system mod hvidvask

I dag henledes opmærksomheden på mistænkelige transaktioner i de fleste banker af automatiske overvågningssystemer, der er baseret på foruddefinerede scenarier for mistænkelig adfærd. For eksempel udløses en alarm, hvis en kunde hæver større kontantbeløb flere gange inden for en kortere periode. Selv om disse scenarier kan tage hensyn til kunde-

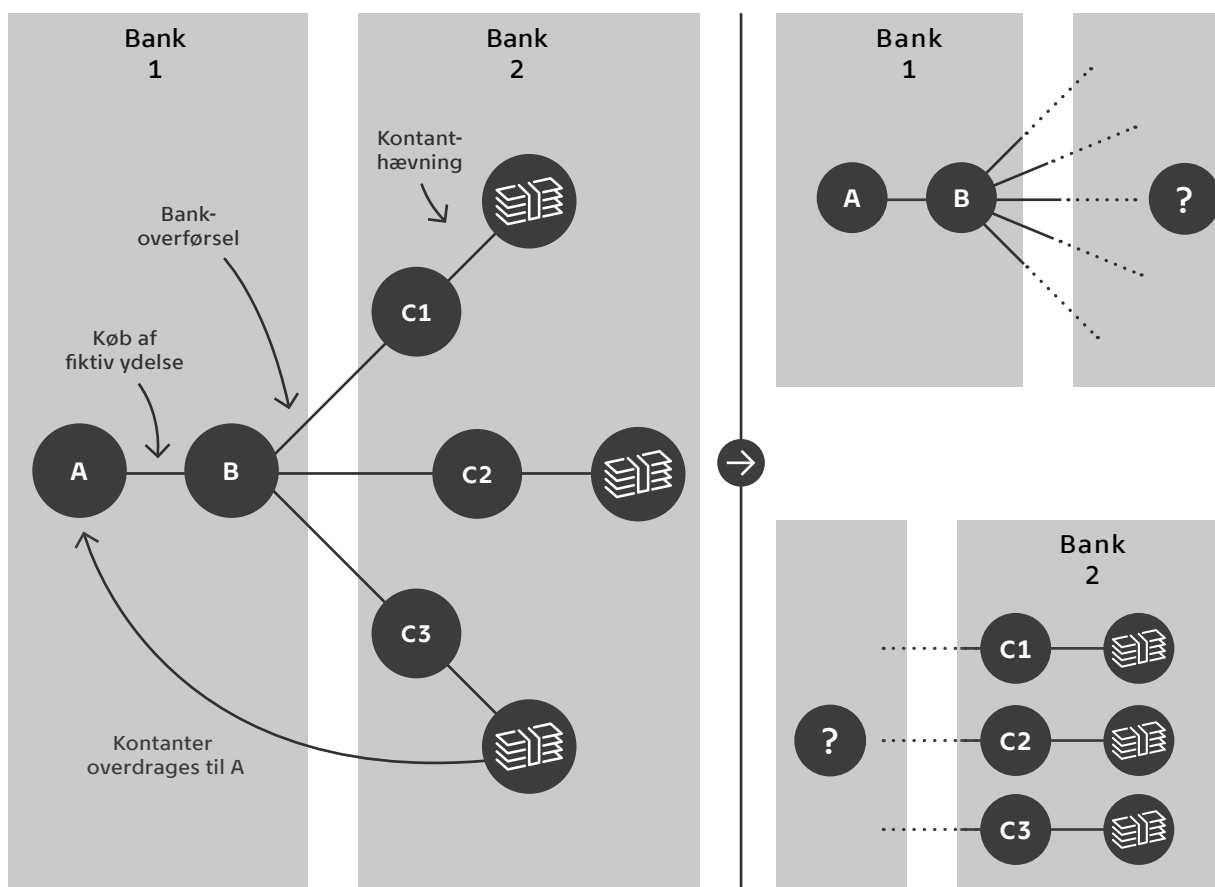
karakteristika, fx privat- eller erhvervskunde, så er de ikke tilstrækkeligt fleksible til præcist at spotte høj risikoadfærd hos bankernes kunder.

Det nuværende system har to væsentlige svagheder. For det første er arbejdet tidskrævende. For det andet har den enkelte bank kun adgang til egne kundedata.

Den betydelige ressourceindsats ses både i bankens arbejde og efterfølgende hos myndighederne. De foruddefinerede scenarier udløser et stort antal falske alarmer, som medarbejdere i bankens hvidvaskenhed efterfølgende manuelt må frasortere. Alarmer i forhold til transaktioner, der efter en manuel gennemgang fortsat vurderes at være mistænkelige, sendes til Hvidvasksekretariatet i SØIK.

Netværk, der opererer på tværs af banker, kan ikke identificeres med data fra enkelte banker

Figur 1



Anm.: A ønsker kontanter. For at få det køber A en fiktiv serviceydelse fra B og overfører det "aftalte" beløb til B. B fordeler beløbet ved at overføre til en række medlemsvorne, C. De medlemsvorne hæver siden hver især kontanter svarende til det overførte beløb. Kontanterne går retur til A minus det "gebyr", som B og C tager for deres "faktiske" serviceydelse. Bank 1 kan ikke se, at de overførte beløb hæves som kontanter. Bank 2 kan ikke udlede sammenhængen imellem kontanthævningerne, der hver især flyver under radaren. I den såkaldte "Operation Greed" blev et lignende system anvendt til hvidvask.

Hvidvasksekretariatet underkaster transaktionerne endnu et lag af kontroller, før sagerne eventuelt sendes til videre efterforskning hos den relevante myndighed, fx politiet. Det anslås, at kun 5 pct. af alle de automatisk udløste alarmer fra den deltagende bank i 2019 endte med at indgå i sager, der blev sendt til videre efterforskning samme år.³

Det store antal falske alarmer betyder, at det nuværende system slet ikke er gearret til at håndtere et stadigt stigende transaktionsvolumen og dermed et stigende antal mistænkelige transaktioner, der skal kontrolleres og måske efterforskes.

Den anden svaghed ved det nuværende system er, at det automatiske overvågningssystem i dag udelukkende trækker på den enkelte banks egne data. Banken har kun kendskab til egne kunder og er derfor ikke i stand til at vurdere den risiko, der er forbundet med en bestemt transaktionsmodpart, medmindre denne også er kunde i banken. På grund af denne begrænsning er det usandsynligt, at komplekse hvidvasknetværk, der involverer flere banker og konti, udløser en alarm hos den enkelte bank, jf. figur 1. Ydermere har bankerne heller ikke adgang til detaljerede myndighedsoplysninger fra fx virksomhedsregistret mv. Det nuværende system er derfor særligt sårbart over for kriminelle aktører, der bevidst benytter flere banker til at sløre deres spor. Derfor flyver mange hvidvasktransaktioner i dag under radaren.

En udvidet datadrevet tilgang kan forbedre opdagelse, effektivitet og hastighed i indsatsen mod økonomisk kriminalitet

Nationalbanken har i samarbejde med andre organisationer undersøgt og vurderet, om svaghederne i det nuværende system kan overvindes ved at gen-tænke og udvide den risikobaserede hvidvaskindsats ved i højere grad at udnytte berigede og detaljerede

transaktionsdata.⁴ Se boks 1 for yderligere detaljer om anvendte data og metoder i undersøgelsen.

Undersøgelsen viser på baggrund af flere uafhængige metoder, at dobbelt så mange mistænkelige transaktioner ville være blevet afsløret og med overvejende sandsynlighed indgå i sager, som Hvidvasksekretariatet ville have haft sendt videre til efterforskning.

Undersøgelsen viser også, at den udvidede datadrevne tilgang kan effektivisere bankernes nuværende manuelle kontrol.

I dag udløses der mange falske alarmer, der manuelt skal frasorteres af bankernes AML-medarbejdere. En datadrevet og risikobaseret metode gør det muligt at estimere en risikoscore for den bagvedliggende sandsynlighed for økonomisk kriminalitet i forbindelse med den enkelte alarm. På basis af disse scorer bliver det muligt i et risikobaseret system automatisk at frasortere alarmer med lav risikoscore, der rutinemæssigt ikke indgår i indberetninger til Hvidvasksekretariatet, og som sådan er at betragte som falske alarmer, jf. figur 2.

Når de alarmer, der udløses af den deltagende banks nuværende system, rangordnes efter risiko, viser undersøgelsen, at blot 1 pct. af de sager, der blev vurderet som værende efterforskningsegnete, og som derfor blev sendt til videre efterforskning, er baseret på de 27 pct. af alarmer med lavest estimeret risiko. Man kan derfor frasortere 27 pct. af de alarmer, der i dag indgår i manuelle kontroller, og fortsat finde 99 pct. af de sager, som sendes til videre efterforskning, jf. figur 2.

Disse tal viser, at der bruges uforholdsmæssigt mange ressourcer både i bankerne og hos myndighederne på at kontrollere alarmer, som i sidste instans vurderes at være knyttet til transaktioner med lav eller ingen risiko for økonomisk kriminalitet. I stedet kunne disse ressourcer i højere grad målrettes kontrol af transaktioner med høj risikoscore. Det ville mærkbart øge effektiviteten i bankernes manuelle

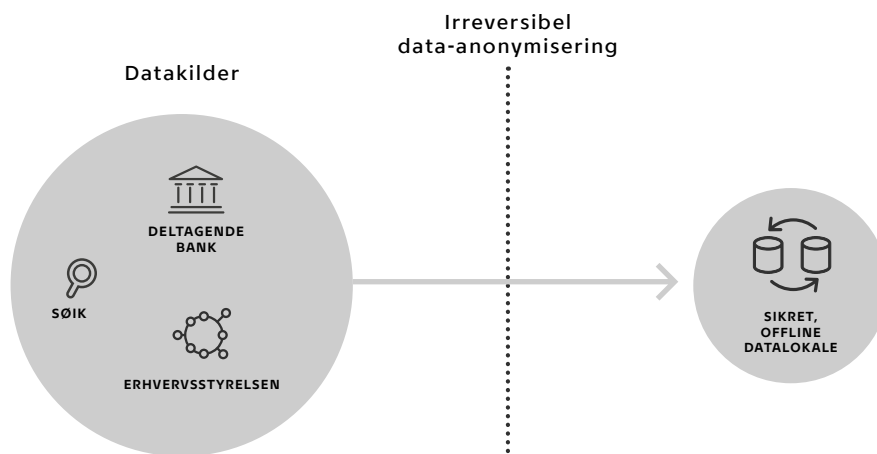
³ Den deltagende bank er repræsentativ for sektoren for så vidt angår mængden af sager, der sendes til SØIK, samt procentdelen af de pågældende sager, som ender med at blive sendt videre til efterforskning.

⁴ Med detaljerede transaktionsdata forstås informationer om alle typer af transaktioner, der registreres på bankkonti, fx kontanthævninger, MobilePay-overførsler, indenlandske og grænseoverskridende kreditoverførsler og korttransaktioner. Et datasæt, der omfatter alle transaktioner gennemført i Danmark i 2019, ville indeholde ca. 3,6 mia. transaktioner.

Anvendte data og metoder i undersøgelsen:

Data fra en enkelt bank blev beriget ved at sammenstille dem med data fra flere myndigheder. Data blev anonymiseret og undersøgt i et sikret lokale.

Boks 1



Undersøgelsen tog udgangspunkt i detaljerede transaktionsdata fra en større bank med oplysninger om flere end en milliard transaktioner gennemført over ca. 4 år. Transaktionsdataene fra den deltagende bank blev beriget med følgende oplysninger fra følgende aktører:

- Banken – oplysninger om alle alarmer, der var udløst af det nuværende overvågningssystem
- SØIK – oplysninger om, hvorvidt underretninger fra banken til Hvidvasksekretariatet indgik i sager, der blev sendt til videre efterforskning
- Erhvervsstyrelsen – oplysninger i form af et CVR-register beriget med regnskabsoplysninger for alle danske virksomheder og en grafdatabase, der bl.a. indeholdt information om forbindelser mellem disse virksomheder og væsentlige interessenter samt oplysninger om efterforskninger for momssvig fra Skattestyrelsen

Alle data blev efter sammenstilling anonymiseret, og den efterfølgende undersøgelse blev gennemført i et sikret datalokale af analytikere med sikkerhedsgodkendelse. Data og harddiske blev destrueret efter afslutning af projektet.

I undersøgelsen analyseres data ud fra to tilgange:

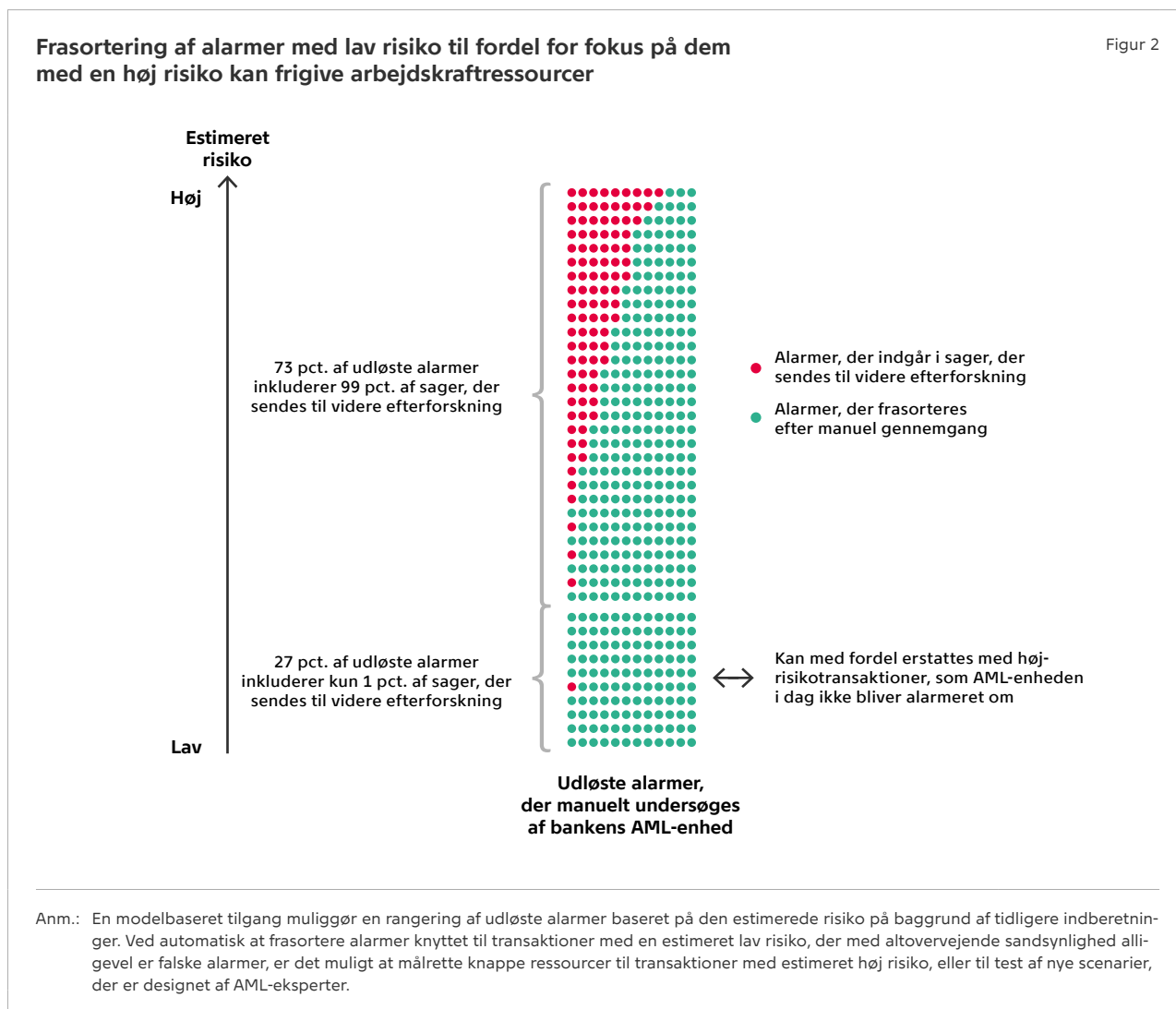
- Den ene tilgang er modelbaseret og tager afsæt i avancerede analytiske metoder og machine learning til at beregne sandsynligheden for, at en bankkunde vil indgå i en sag, som Hvidvasksekretariatet sender til videre efterforskning. Beregningen af sandsynligheden sker på basis af seneste og tidligere transaktioner og baggrundsinformation om bankens kunder holdt op imod, hvad der tidligere er blevet vurderet mistænkeligt af myndighederne.¹

Den anden tilgang er baseret på foruddefinerede scenarier. Disse scenarier tager afsæt i en sammenstilling af den enkelte banks data og data fra andre kilder med henblik på i samarbejde med AML-eksperter (anti-money laundering) at opstille scenarier, som vil udløse en alarm, der bør efterforskes.

De to tilgange supplerer hinanden. Den modelbaserede tilgang udnytter data til at genkende transaktionsmønstre (kundeadfærd) og afsløre transaktioner med høj risikoscore, dvs. risiko for at udløse en alarm, som AML-medarbejdere efterfølgende kontrollerer manuelt. Modellen er imidlertid afhængig af tidligere transaktioner og mønstre for at kunne genkende mistænkelig adfærd. Hvis visse typer af mistænkelig adfærd historisk ikke er blevet identificeret og behandlet på grund af manglende kontrol, vil modellen heller ikke fremadrettet kunne identificere disse typer af hvidvask.

I den scenariebaserede tilgang opstilles og udvikles i samarbejde med AML-eksperter nye scenarier til at opfange mønstre i transaktioner, der vurderes at pege mod bagvedliggende hvidvask. Disse scenarier kan forfines på basis af mønstre fundet via den modelbaserede metode og åbner op for, at AML-eksperter kan medvirke mere direkte i efterforskningen. Denne metode har mange sammenfald med det nuværende automatiske overvågningssystem. Den ekstra værdi opstår her ved en udvidet kombination af information fra flere kilder – banken og myndighederne – og særligt også muligheden for at kunne opstille scenarier, der udnytter datakilder på tværs af organisationer. Det kunne fx være ved mistanke om hvidvasknetværk som beskrevet i figur 1.

1. Disse machine learning-modeller er velegnede til at forudsige mistænkelig adfærd. Modellerne behøver ikke at være komplekse og svære at fortolke. Selv om modellens forudsigelsesevne ganske vist generelt øges med kompleksiteten, kan der også opnås tilfredsstillende resultater på baggrund af simple regressionsmodeller, forudsat at det sammenstillede datagrundlag er til stede. En middelvej er at opstille en kompleks model og lade modellen belyse, hvilke variable og mønstre der bidrager mest til modellens forudsigelsesevne. En analytiker kan derefter opstille en model, der er mere simpel og lettere at fortolke, og som udnytter indsigt fra de avancerede modeller.



kontrolproces.

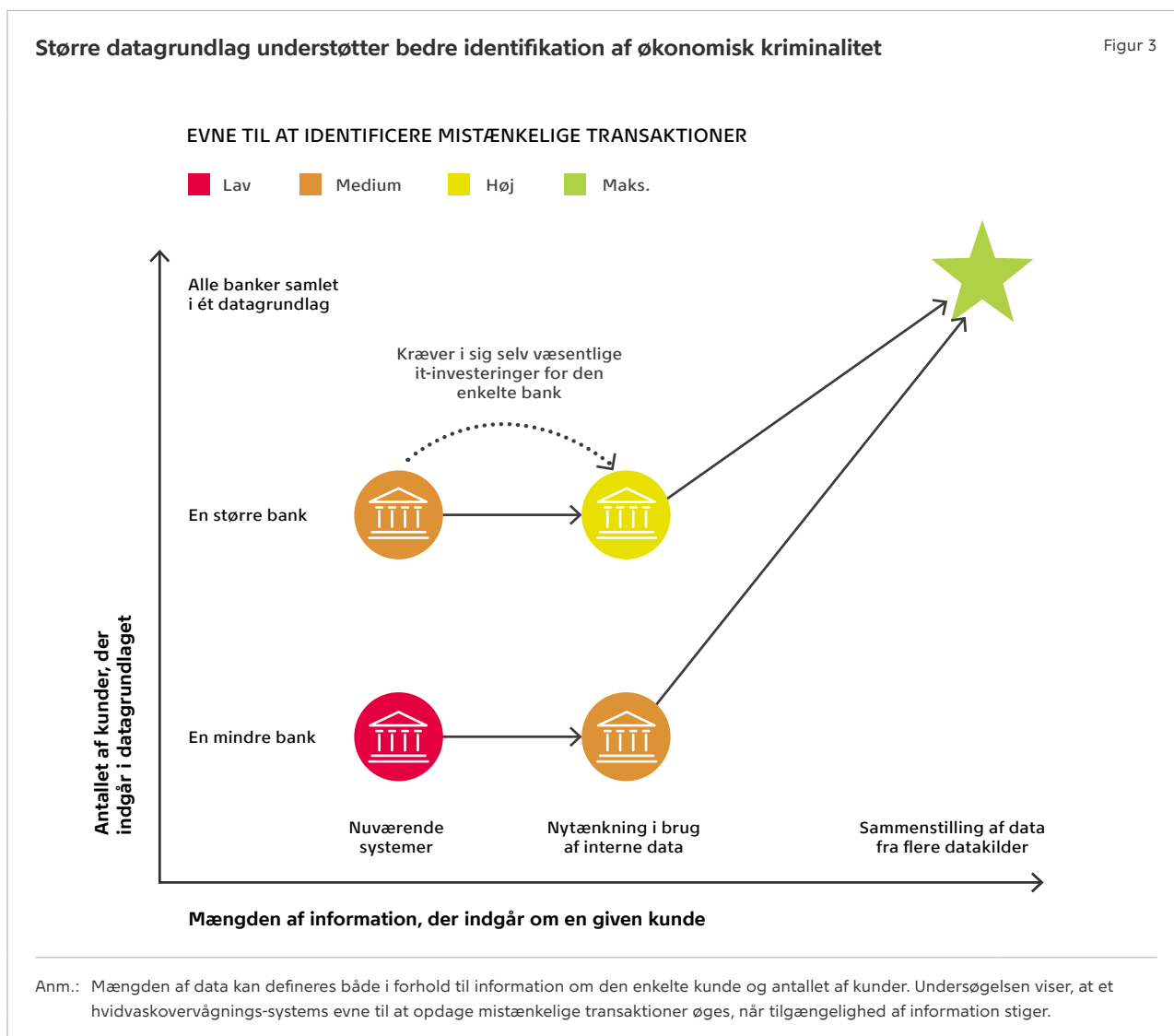
Den udvidede datadrevne metode opdager 84 pct. af de alarmer, der gav anledning til underretninger til Hvidvasksekretariatet, tidligere end i dag. Yderligere kunne mere end halvdelen opdages mere end 10 uger, før de ville udløse en alarm i det nuværende system.

Realisering af det fulde potentiale forudsætter sammenstilling af data fra flere kilder

Undersøgelsen viser, at der bruges mange ressourcer på falske alarmer, at mange mistænkelige transaktioner flyver under radaren i dag, og at dem,

der opdages, ofte opdages med forsinkelse. Et fælles system kan forbedre indsatsen mod økonomisk kriminalitet, men det forudsætter sammenstilling af data på tværs af banker og myndigheder af tre årsager.

For det første har bankerne i udgangspunktet ikke kendskab til transaktionsmodparten og kan derfor ikke i det nuværende system vurdere den risiko, der er forbundet med modparten. Det er en begrænsning, der udgør en stor hindring for at opdage komplekse netværk, der spænder over flere konti, kunder og banker, jf. figur 1. Desuden deles information ikke på tværs af bankerne, og dermed får kriminelle mulighed for at slette deres historik af mistænkelige transaktioner ved blot at skifte bank. Flere end halvdelen af underretningerne fra den deltagende bank omhandlede således en eller flere personer eller



virksomheder, der var indeholdt i underretninger fra andre banker og dermed allerede var kendt af myndighederne.⁵ Et fælles transaktionsmonitorerings- og analysesystem vil derimod samle viden på tværs af banker og være et bedre værn mod kriminel adfærd.

For det andet skaber en sammenstilling af data i et fælles system synergier, der ikke er mulige at opnå for en enkelt bank. Undersøgelsens resultater viser, at de potentielle gevinster ved en datadrevet metode

stiger i takt med den mængde data, der indgår i datagrundlaget. Dette forhold gør sig gældende både med hensyn til antallet af kunder i datasættet, og hvilke informationer der inddrages om den enkelte kunde, jf. figur 3. Sammenstilling af data på tværs af banker vil øge både antallet af kunder i datasættet og mængden af de tilgængelige informationer om den enkelte kunde og denne kundes relationer med andre kunder på tværs af banksystemet. Den information er særlig vigtig i forbindelse med kortlægning af netværk af kriminelle aktører.

⁵ Dette resultat kommer fra en anden undersøgelse lavet i samarbejde med Hvidvasksekretariatet i SØIK. Undersøgelsen viser, at 13 pct. Af de kunder, der optrådte i underretninger fra den deltagende bank, i samme periode også blev indrapporteret i underretninger fra andre institutioner.

For det tredje har små banker en væsentlig ulempe, idet de har få egne data til at lære at genkende mistænkelige mønstre ud fra. Denne ulempe bliver endnu mere udtalt, når det drejer sig om erhvervs-kunders transaktioner. Forskellen mellem små og store banker risikerer at forstærke strukturelle svagheder i kampen mod økonomisk kriminalitet, idet forskelle i ressourceindsats kan føre til, at de kriminelle "søger tilflugt" dér, hvor risikoen for afsløring er mindre.

Transaktionsdata kan også styrke indsatsen mod momssvig

Den Internationale Valutafond, IMF, skønner, at den danske stat hvert år går glip af momsindtægter for 10 mia. kr. på grund af momssvig.⁶ Undersøgelsen viser, at anvendelsen af transaktionsdata også kan understøtte afsløringen af momssvig, idet disse kan bruges til at anslå de beløb, virksomheder skal betale i moms til staten. Ved at sammenholde virksomhedernes faktiske momsindbetalinger med de anslåede beløb vil skattemyndighederne kunne målrette deres kontrolindsats mod virksomheder med markante afvigelser eller mod virksomheder, der ikke har ladet sig momsregistrere trods en omsætning, der overstiger grænsen for momsregistrering.

Myndigheder og finanssektor skal evaluere muligheder for en fælles løsning i kampen mod hvidvask og økonomisk kriminalitet

Undersøgelsen har vist, at en datadrevet tilgang baseret på berigede transaktionsdata kan forbedre indsatsen mod økonomisk kriminalitet væsentligt. Forudsætningen for at realisere det fulde potentiale er dog, at offentlige myndigheder og den finansielle sektor går sammen om at skabe rammerne for et

fælles transaktionsmonitorerings- og analysesystem.

I arbejdet med undersøgelsen blev det bevidst valgt ikke at fokusere på systemets funktion i praksis, krav i forhold til it-infrastruktur og det nødvendige lovgrundlag. Disse udestående spørgsmål, og hvad de hver især kræver med hensyn til ressourcer og lovgivningsmæssige rammer, bliver en opgave for en arbejdsgruppe ledet af Erhvervsministeriet. Gruppen vil omfatte medlemmer fra både myndigheder og den finansielle sektor.

Baggrund

Boks 2

Projektet udsprang dels af Nationalbankens løbende arbejde med indsamling og produktion af betalingsstatistik, dels af et øget fokus fra myndighederne på bekæmpelse af hvidvask og momssvig. Dertil kom, at Finans Danmarks Hvidvask Task Force lancerede sine 25 anbefalinger i december 2018, som også indeholdt sektorens forslag om øget samarbejde om it og håndtering af data som led i bekæmpelsen af økonomisk kriminalitet. Flere større sager om økonomisk kriminalitet har øget fokus på hvidvask og momssvig og medført, at der både fra politisk og bankernes side er opstillet en vision om, at Danmark skal være førende i kampen mod økonomisk kriminalitet.

Projektet har haft til formål at afdække, hvorvidt der inden for rammerne af et offentlig-privat partnerskab vil være forbedrede muligheder for at opspore og forebygge hvidvask og momssvig ved at sammenstille transaktionsdata og kundeoplysninger, såsom cpr- og cvr-numre samt formåls- og omfangsoplysninger, med data fra de relevante myndigheder. Datamaterialet består af kunde- og transaktionsoplysninger fra en større dansk bank, information om udfaldet af Hvidvasksekretariatets vurdering af hvidvaskunderretninger og ikke-offentlige oplysninger om moms- og erhvervsforhold, jf. figur 1.

⁶ IMF's landerapport, *Denmark: Technical assistance report – Revenue Administration Gap Analysis Program – The Value Added Tax Gap*, nr. 16/59, februar 2016.

UDGIVELSER



NYT

Nyt giver et hurtigt og tilgængeligt indblik i en Analyse, et Economic Memo, et Working Paper eller en Rapport fra Nationalbanken. Nyt udkommer løbende.



ANALYSE

Nationalbankens Analyseserie har fokus på økonomiske og finansielle forhold. Nogle af analyserne udkommer med fast frekvens, fx *Udsigter for dansk økonomi* og *Finansiel stabilitet*, der begge udkommer halvårligt. Andre analyser udkommer løbende.



RAPPORT

Nationalbankens Rapportserie er tilbagevendende rapporter og beretninger om Nationalbankens virke. Det er fx *Årsrapport* og *Statens låntagning og gæld*.



ECONOMIC MEMO

Economic Memo er en mellemting mellem en Analyse og et Working Paper og viser ofte forfatterens igangværende analysearbejde. Serien henvender sig primært til fagpersoner. Economic Memo udkommer løbende.



WORKING PAPER

Working Paper præsenterer forskningsarbejde udført af ansatte i Nationalbanken og samarbejdspartnere. Serien henvender sig primært til fagpersoner og folk med interesse for den akademiske tilgang. Working Paper udkommer løbende.

Analysen består af en dansk og engelsk version.
I tilfælde af tvivl om oversættelsens korrekthed gælder den danske version.

DANMARKS NATIONALBANK
LANGELINIE ALLÉ 47
2100 KØBENHAVN Ø
WWW.NATIONALBANKEN.DK

Thais Lærkholm Jensen
Chef for Data Analytics
and Science
tj@nationalbanken.dk

Bjarke Mørch Mønsted
Data Scientist
bmm@nationalbanken.dk

**Alessandro
Tang-Andersen Martinello**
Senior Data Scientist
alem@nationalbanken.dk

FINANSIEL STATISTIK

KONTAKT

Teis Hald Jensen
Kommunikations-
og presserådgiver

tehj@nationalbanken.dk
+45 3363 6066

SEKRETARIAT
OG KOMMUNIKATION



DANMARKS
NATIONALBANK