# Building Trust in a World of Deception

Experian research conducted by Forrester Consulting

# Velkommen til Experians svindelrapport 2026

**I de seneste år har vi set truslen fra svindel vokse markant. Svindel er blevet mere organiseret og industrialiseret, understøttet af stadigt mere avancerede værktøjer, som driver en kraftig stigning i både omfanget og kompleksiteten af angreb.**

Hele regioner er i dag blevet til deciderede megafabrikker for svindel rettet mod uskyldige mennesker verden over. Samtidig ser vi en voksende trussel fra statsgodkendte kriminelle organisationers involvering i disse koordinerede angreb – hvilket får nogle eksperter til at vurdere, at vi befinder os midt i svindelens guldalder.

At imødegå denne udfordring kræver et langt stærkere samarbejde. Den enkelte organisations indsats bliver markant mere effektiv, når den kombineres med andres. Organisationer, der deltager i Experians netværk af svindelbekæmpende konsortier, oplever ofte en betydelig reduktion i svindeltab, når de udnytter den kollektive intelligens, der deles på tværs af netværket.

Samtidig er det afgørende, at virksomheder tager de mest avancerede teknologier i brug inden for forebyggelse af svindel. Kunstig intelligens er blevet en central drivkraft i dette forsvar, hvor både machine learning og generativ AI åbner nye muligheder for bedre at identificere svindlere, hurtigere tilpasse sig nye trusler og mere effektivt administrere svindelsystemer – alt sammen med det formål at beskytte både virksomheder og deres kunder.

I årets undersøgelse, som er gennemført i samarbejde med Forrester Consulting, har vi spurgt omkring tusinde beslutningstagere inden for svindel fra ni lande om deres syn på de vigtigste tendenser, der påvirker forebyggelse af svindel. Jeg er overbevist om, at deres samlede indsigt vil hjælpe dig med at styrke din svindelstrategi i det kommende år.

Når du er klar til at indlede en dialog om vores komplette platform til forebyggelse af svindel, står både vores lokale og vores globale team af ekspertkonsulenter klar til at tage en samtale med dig.

**SHAIL DEEP**
COO Experian EMEA & APAC

# Indhold

FØRSTE DEL

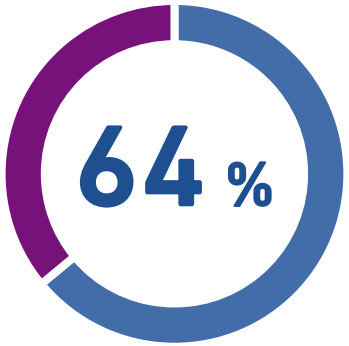
## Udfordringer og prioriteter



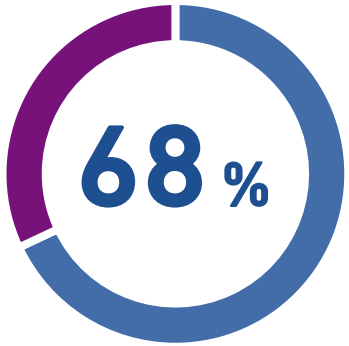
ANDEN DEL

## Teknologidrevne løsninger

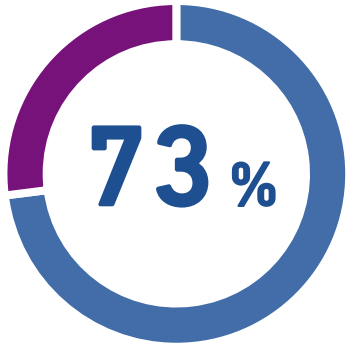
# Et snapshot af de vigtigste resultater



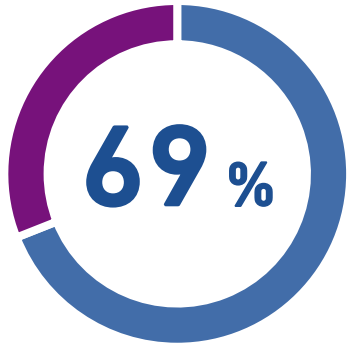

oplyser, at deres tab som følge af svindel er steget år for år.



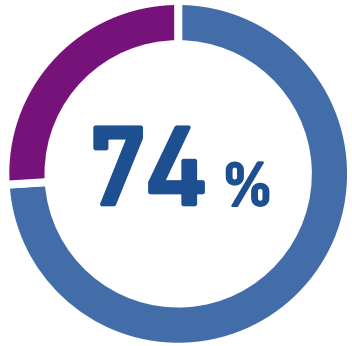

er enige i, at deres nuværende teknologistak ikke er tilstrækkelig til at imødegå en svindeltrussel i hastig forandring.




er interesserede i at investere i passive svindelkontroller som adfærds- og enhedsdata for at minimere friktion.




planlægger at integrere forebyggelse af svindel og vurdering af kreditrisiko i en overordnet risikostyringsstrategi.




er enige i, at de fleste virksomheder inden for de næste tre år vil indgå i netværk, hvor svindelintelligens deles på tværs.

Basis: 979 ledende beslutningstagere inden for svindel i EMEA og APAC
Kilde: Experian-undersøgelse udført af Forrester Consulting, juli 2025

FØRSTE DEL: udfordringer og prioriteter

# Indsigter fra frontlinjen

## Svindel er i dag både hurtigere og billigere at gennemføre end nogensinde før. Den dobbelte trussel fra stadigt mere organiserede, transnationale cyberkriminelle netværk og GenAI-drevne angreb har markant øget både omfanget og kompleksiteten af svindel.

Ifølge en nylig undersøgelse er svindelsyndikater i Sydøstasien blevet betegnet som "det mest magtfulde kriminelle netværk i moderne tid". De genererer årligt mellem 50 og 70 milliarder dollars og beskæftiger mere end 350.000 personer. Samtidig tilbyder de såkaldte *Fraud-as-a-Service*-leverandører på det mørke net et stadigt bredere udbud af produkter, der giver svindlere adgang til de nyeste værktøjer og den mest opdaterede kriminelle intelligens.

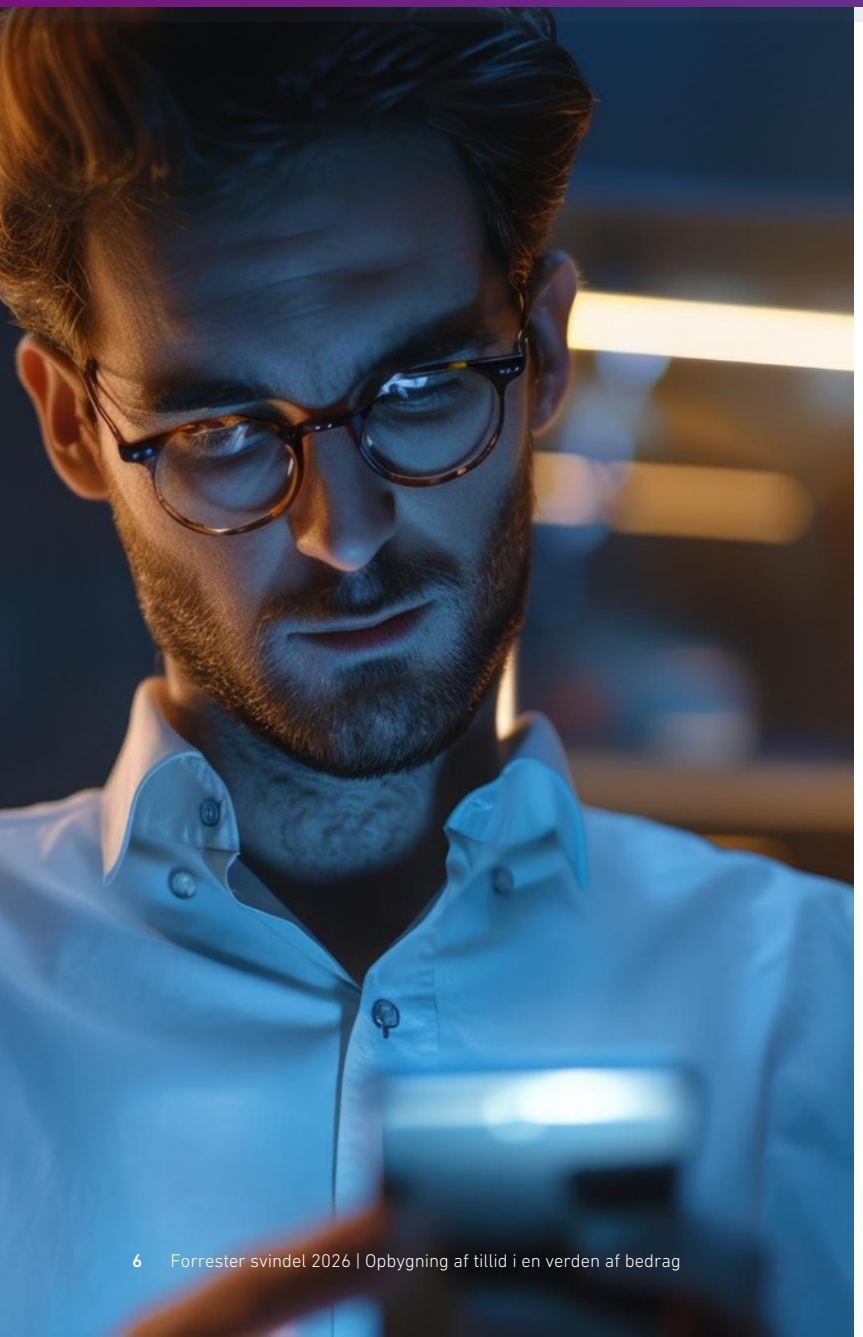
Vores analyser viser, at denne trussel påvirker virksomheder globalt. **Mere end to tredjedele (67 %) af de adspurgte forventer flere svindelangreb i 2026 end i de foregående år – en stigning på 10 procentpoint sammenlignet med året før.**

Som følge af denne udvikling oplever 64 % af virksomhederne, at deres tab som følge af svindel er steget sammenlignet med året før. Den samme andel angiver, at deres organisation har vanskeligt ved at følge med en svindeltrussel i hastig forandring. Konsekvenserne af denne bølge af svindel rækker imidlertid videre end direkte økonomiske tab: 67 % er enige i, at svindelsager også skader organisationens omdømme.

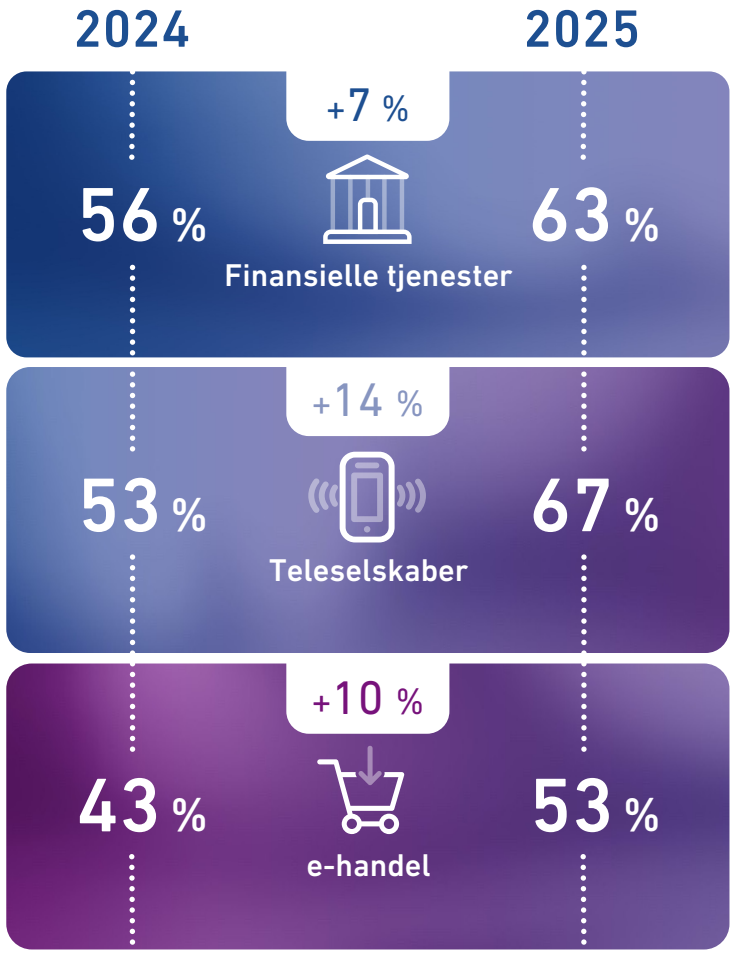
### Hvilke typer af svindel er steget mest?

Ser vi på de tre brancher, der indgik i undersøgelsen, har telesektoren oplevet den største stigning i det samlede antal svindelangreb, idet to tredjedele (67 %) rapporterer en stigning. Finansielle tjenesteydelser følger tæt efter med 63 %, mens lidt over halvdelen (53 %) af e-handelsvirksomhederne ligeledes er blevet ramt af flere svindelangreb.

**67 %** **forventer flere svindelangreb end sidste år**



## Andel af organisationer, der rapporterer en stigning i det samlede antal svindelangreb (2024 vs. 2025)




Basis: 979 ledende beslutningstagere inden for svindel i EMEA og APAC
Kilde: Experian-undersøgelse udført af Forrester Consulting, juli 2025

Sammenlignet med året før er social engineering, svindel relateret til loyalitets- og belønningsprogrammer samt identitetstyveri de hurtigst voksende trusler inden for finansielle tjenester og telesektoren. Det er ikke overraskende, at social engineering er i kraftig vækst, i betragtning af de muligheder, som GenAI tilbyder i dag.

Undersøgelsen indikerer samtidig, at svindlere i stigende grad retter fokus mod loyalitetsprogrammer og belønningsordninger – muligvis fordi disse ofte opfattes som mindre sikre end andre betalings- og identitetssystemer.

**Identitetsbekræftelse er blevet den vigtigste sikkerhedsperimeter og et primært mål for svindlere.** I takt med at legitime AI-agenter i stigende grad interagerer med digitale platforme side om side med bots og deepfakes, bliver evnen til præcist at autentificere og verificere kundens identitet helt afgørende.

Inden for e-handel har såkaldt friendly fraud og misbrug af refusionsordninger oplevet den største år-til-år-stigning. Angreb med syntetisk identitetssvindel er ligeledes steget, men i mindre omfang.

## Årlig stigning i typer af svindelangreb efter branche

### Finansielle tjenester

Stigning i samlede svindelangreb: **63 %**

Tab ved svindel stiger år for år: **64 %**

| | STEGET BETYDELIGT/MODERAT | STEGET EN SMULE/EN VIS GRAD | |
|---|---|---|---|
| Svindelangreb med identitetstyveri | 25% | 39% | 64% |
| Svindelangreb med loyalitet/belønning | 25% | 39% | 64% |
| Social engineering | 25% | 37% | 62% |
| Svindelangreb med kontoovertagelse | 25% | 35% | 60% |
| Svindelangreb med syntetisk virksomhed | 28% | 32% | 60% |

### Teleselskaber

67 % 66 %

| | STEGET BETYDELIGT/MODERAT | STEGET EN SMULE/EN VIS GRAD | |
|---|---|---|---|
| Pengekurerer | 26% | 36% | 62% |
| Svindelangreb med loyalitet/belønning | 22% | 39% | 61% |
| API-svindelangreb | 27% | 33% | 60% |
| Svindelangreb med syntetisk forbrugeridentitet | 18% | 42% | 60% |
| Svindelangreb med syntetisk virksomhed | 21% | 38% | 59% |

### e-handel

53 % 61 %

| | STEGET BETYDELIGT/MODERAT | STEGET EN SMULE/EN VIS GRAD | |
|---|---|---|---|
| Svindel med misbrug af tilbagebetaling | 22% | 39% | 61% |
| Angreb med venlig svindel | 27% | 33% | 60% |
| Svindelangreb med syntetisk identitet | 22% | 36% | 58% |
| Angreb med kontoovertagelse | 18% | 34% | 52% |
| Trekantssvindel | 17% | 32% | 49% |

Basis: 979 ledende beslutningstagere inden for svindel i EMEA og APAC
Kilde: Experian-undersøgelse udført af Forrester Consulting, juli 2025

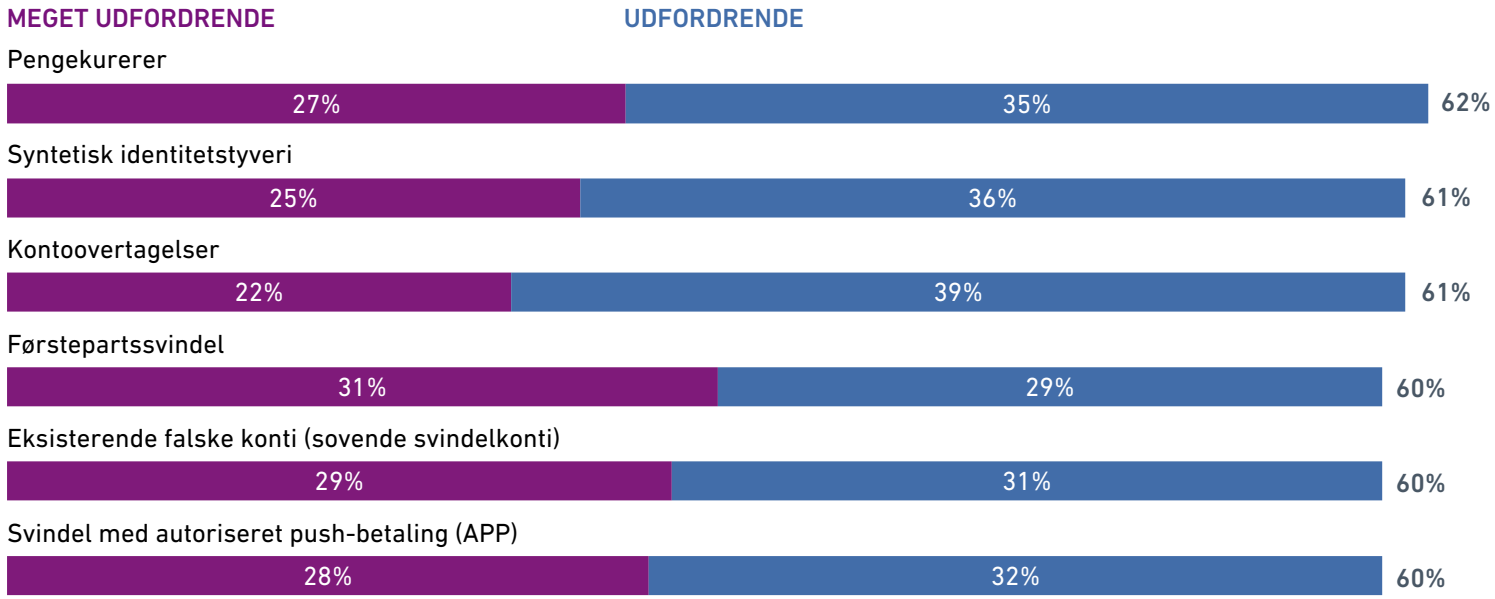
## Hvilke typer af svindel er mest udfordrende at opdage og forhindre?

Vores analyser viser, at pengekurerer er den sværeste form for svindel at bekæmpe, efterfulgt af syntetisk identitetssvindel og kontoovertagelse. Netop disse svindeltyper kræver adgang til supplerende svindelindikatorer, da de muliggør kontinuerlig og passiv overvågning af brugerdata for at identificere mønstre, der kan indikere svindel.

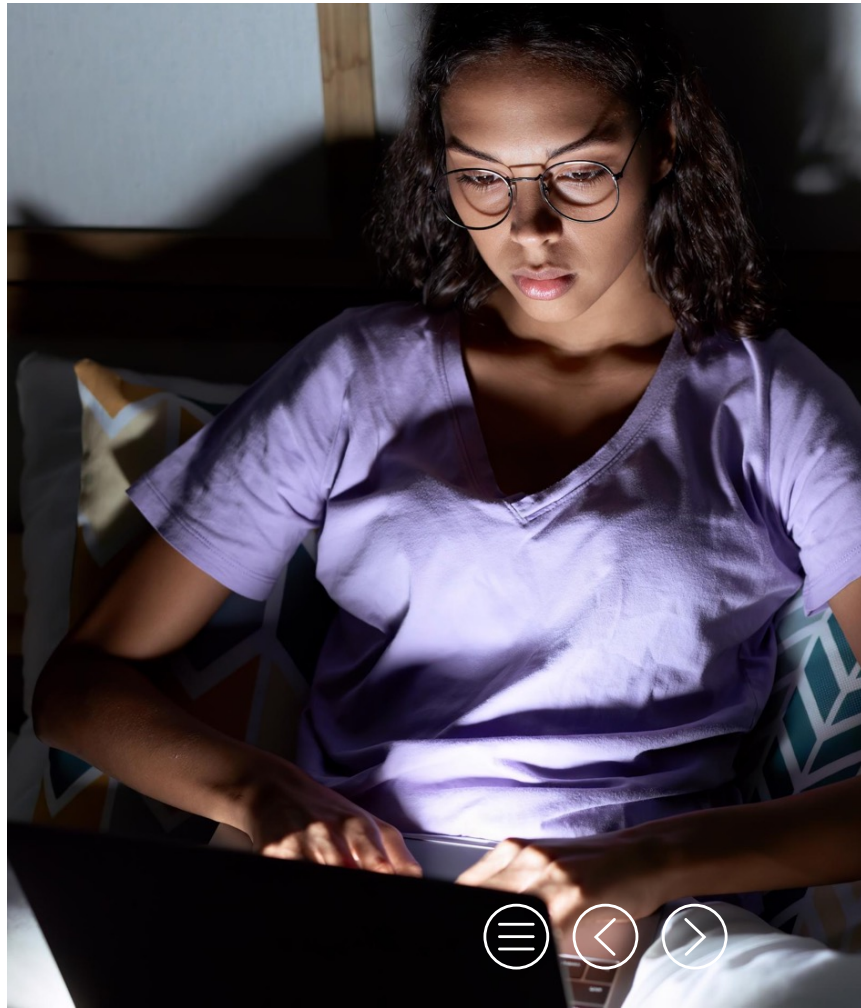
Traditionelle autentificeringsmetoder kan i dag relativt let omgås ved hjælp af GenAI-drevet social engineering og data fra det mørke net (the dark web). Svindeltyper, der er vanskelige at identificere, kan derfor kun forebygges ved hjælp af mere subtile enheds- og adfærdsbaserede signaler, som afslører afvigelser fra normal brugeradfærd. Set i lyset af, at kun en begrænset andel af respondenterne anvender avancerede autentificeringsværktøjer – 42 % benytter i dag enhedsdata, og blot 39 % anvender adfærdsbiometri - er det forståeligt, at disse former for svindel fortsat udgør en betydelig udfordring.

Uden adgang til disse værktøjer vil mange virksomheder opleve stigende svindeltab, i takt med at svindlere får adgang til systemer via kompromitterede legitimationsoplysninger. Samtidig er overvågning af det mørke net (the dark web) blevet et vigtigt element i svindelbekæmpelsen for at holde overblik over, hvilke data der er i omløb, og hvilke svindeltaktikker der aktuelt anvendes.

### Hvilke typer af svindel er mest udfordrende at opdage og forhindre?




Basis: 979 ledende beslutningstagere inden for svindel i EMEA og APAC
Kilde: Experian-undersøgelse udført af Forrester Consulting, juli 2025



# De største udfordringer ved svindel

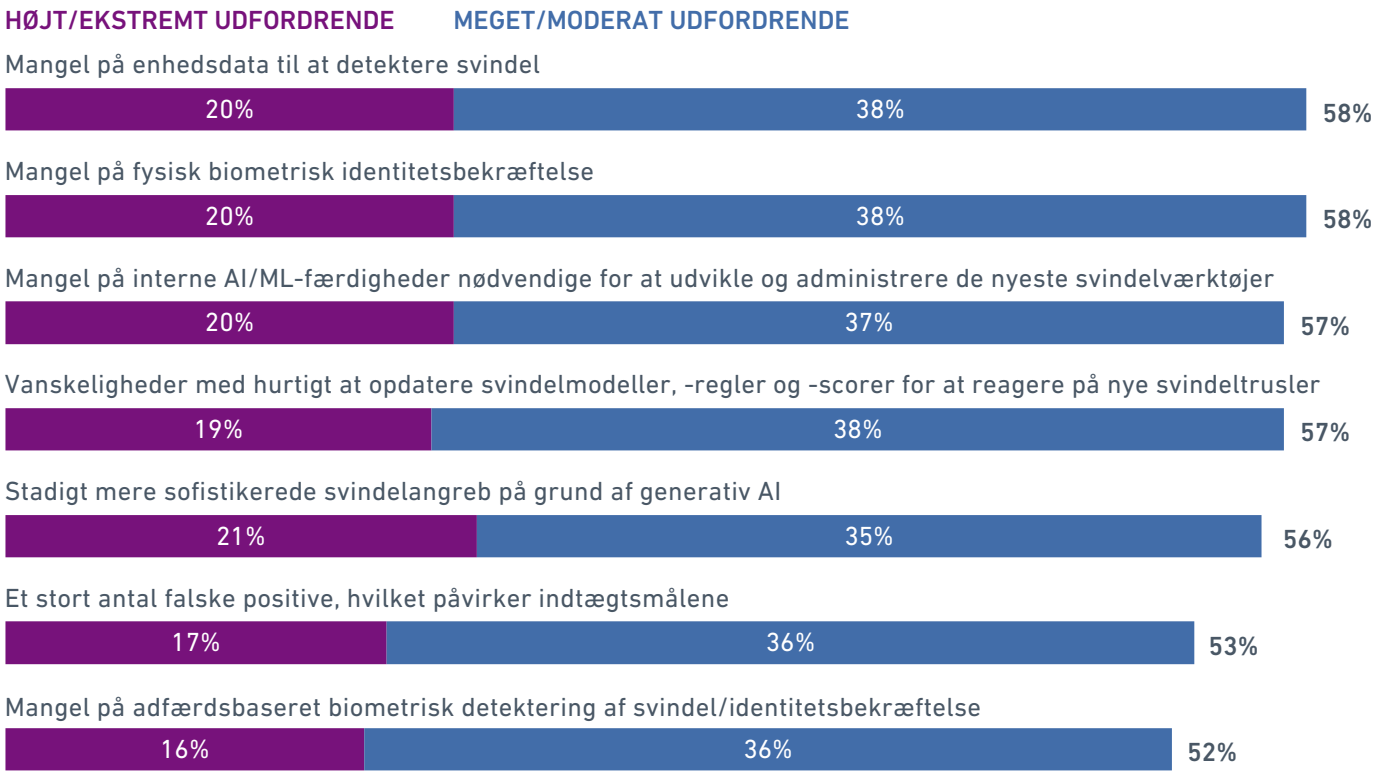
**De tre største udfordringer, der begrænser organisationers evne til at opdage og forhindre svindel, relaterer sig alle til manglende kapabiliteter. Enhedsdata og fysisk biometri identificeres som de væsentligste mangler, tæt fulgt af behovet for AI- og ML-ekspertise til at omsætte disse signaler til præcise og pålidelige beslutninger om svindel.**

Vores analyser peger på, at mange virksomheder befinder sig i et kapabilitetsmæssigt vakuum: Deres eksisterende svindelsystemer er ikke længere tilstrækkelige til effektivt at kontrollere svindel, men samtidig mangler de ressourcer og kapacitet til at implementere de avancerede værktøjer, der er nødvendige. Spørgsmålet om, hvorvidt man skal udvikle løsninger internt eller købe dem eksternt, er ikke nyt, men den hastige udvikling i stadig mere sofistikerede svindelangreb har markant øget presset.

**Virksomheder har brug for effektive løsninger nu – ikke om et år eller mere, hvilket ofte er den tid, det tager at udvikle en intern løsning.** Samtidig er det blevet afgørende for fremtidig vækst at finde den rette balance mellem interne kompetencer og teknologiske løsninger i mødet med en stadigt voksende svindeltrussel. Det er værd at bemærke, at næsten tre fjerdedele (71 %) af de adspurgte angiver, at de investerer mere i svindelteknologi end i menneskelige svindelanalytikere.

**68 %** er enige i, at deres nuværende teknologilandskab ikke er tilstrækkeligt til at håndtere en svindeltrussel i hastig udvikling

## De største udfordringer, der begrænser evnen til at detektere og forhindre svindel




Basis: 979 ledende beslutningstagere inden for svindel i EMEA og APAC
Kilde: Experian-undersøgelse udført af Forrester Consulting, juli 2025

## GenAI ændrer svindellandskabet markant

Ser man på de faktorer, der driver den voksende svindeltrussel, fremstår GenAI som den centrale katalysator, der forbinder enorme mængder data fra det mørke net med hundredtusinder af tvangsrekrutterede svindlere. Mørke LLM'er som WolfGPT og WormGPT har gjort det muligt for stort set alle med en internetforbindelse at udføre en bred vifte af sofistikerede svindelangreb.

Som følge af den hastige forbedring i kvaliteten af falske dokumenter og deepfake-billeder angiver 64 % af respondenterne, at deres eksisterende kend-din-kunde- og identitetsbekræftelsesprocesser ikke er i stand til at opdage GenAI-genereret materiale.

Når ægte kundedata kombineres med syntetiske billeder og dokumenter, bliver identifikation endnu mere kompleks. Og i takt med at stadig mere avancerede værktøjer bliver bredt tilgængelige til stadig lavere omkostninger, vil udfordringen kun vokse. **Faktisk er 60 % enige i, at vi fortsat kun har set toppen af isbjerget, når det gælder AI-drevet svindel.**

AI

**66 %** **af svindeleksperter er enige i, at GenAI er den største udfordring for svindelforebyggelse nogensinde**

Et konkret eksempel på denne hurtige udvikling er, at deepfakes nu kan simulere hjerteslag. Indtil for nylig blev mikroskopiske variationer i hudfarve forårsaget af puls betragtet som en pålidelig metode til at afsløre deepfakes. Nyere, mere avancerede deepfakes er imidlertid i stand til at replikere dette signal, hvilket gør dem markant sværere at opdage.

Der er ingen tvivl om, at fremkomsten af GenAI markerer et skelsættende vendepunkt i forebyggelsen af svindel. Grænsen mellem det ægte og det falske er i stigende grad udvisket, og konsekvenserne er fortsat vanskelige at forudsige. 60 % af respondenterne er enige i, at deres svindeltab er steget markant siden GenAI's gennembrud.

Samtidig angiver en tilsvarende andel (58 %), at de har vanskeligt ved at afgøre, om GenAI har været involveret i et angreb, hvilket gør det udfordrende at kvantificere den samlede effekt.

### Bør deepfakes være ulovlige?

61 % af vores respondenter er enige i, at alle former for deepfakes bør gøres ulovlige af hensyn til samfundet. Lovgivere verden over arbejder på at formulere regler for deepfakes, men det nuværende fravær af en klar juridisk ramme betyder, at truslen i vid udstrækning forbliver ukontrolleret.

Danmark er blandt de få lande, der har reageret relativt hurtigt på problemstillingen. Her er der for nylig fremsat forslag om ændringer i ophavsretsloven, som skal sikre, at alle har ret til deres egen krop, ansigtstræk og stemme.

Italien har ligeledes taget markante skridt ved officielt at kriminalisere skabelse og distribution af skadelige deepfakes som led i sin nye nationale AI-lovgivning. Denne lov, som er den første af sin art i EU, indfører fængselsstraffe for personer, der ulovligt producerer eller deler AI-genereret eller manipuleret indhold – herunder deepfakes. Sanktionerne skærpes yderligere, hvis teknologien anvendes til at begå forbrydelser som svindel eller identitetstyveri.

Selvom dette er skridt i den rigtige retning, mangler der fortsat bred juridisk præcedens. Indtil der foreligger mere omfattende regulering, kan alle i praksis skabe en deepfake på få sekunder. Spørgsmålet er derfor, om stemme- og video-deepfakes bør gøres ulovlige.

# Prioriteter for det kommende år

I takt med den stigende sofistikering af svindeltrusler er det naturligt, at den højeste prioritet for det kommende år er at gennemføre en strategisk gennemgang af de nuværende svindelløsninger (70%). Systemer, der har været i drift i årtier, bliver hurtigt forældede, og virksomheder efterspørger i stigende grad mulighed for at inddrage flere og mere avancerede svindelsignaler i deres vurderinger.

Denne revurdering hænger tæt sammen med den næst- **og tredjevigtigste prioritet: at migrere svindelløsninger til skyen (68%) samt at investere i nye svindelværktøjer (68%).**

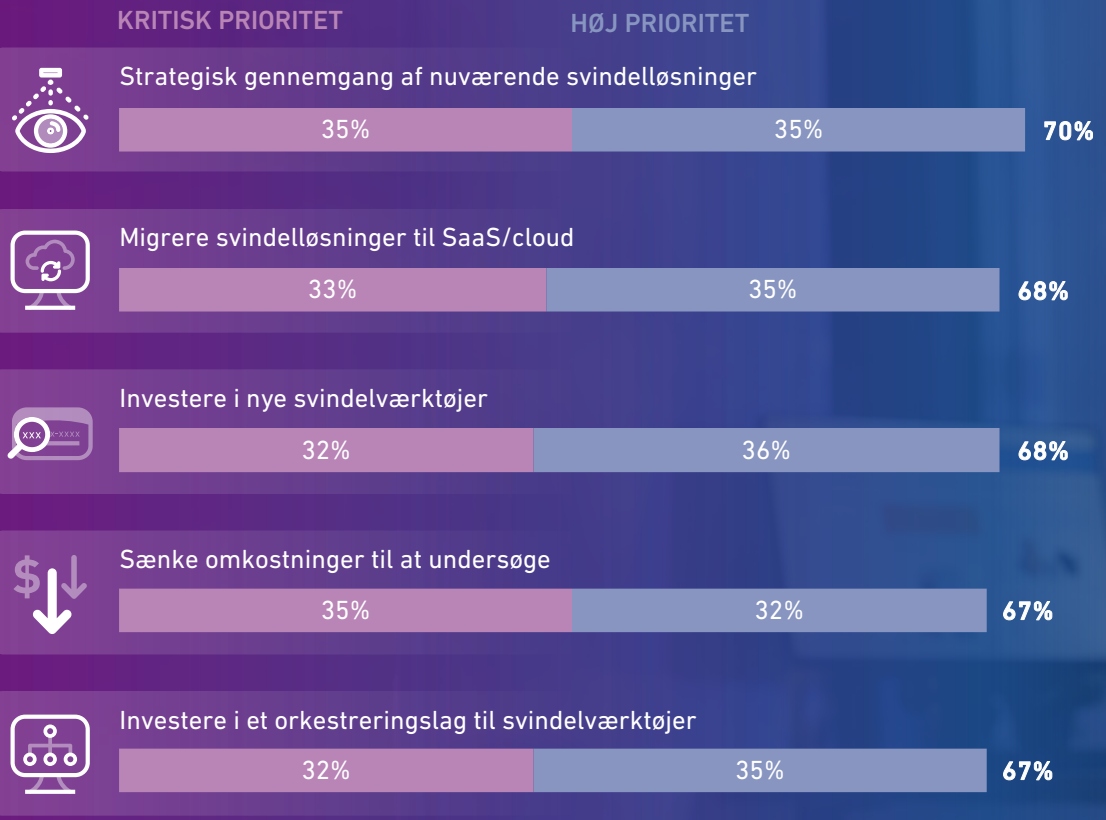
Ser vi frem mod de næste tre til fem år, er det sandsynligt, at GenAI's indvirkning på svindel vil intensiveres yderligere. Derfor bliver det afgørende at foretage velovervejede, strategiske investeringer i de rette svindelsystemer for at begrænse fremtidige tab.

Fremsynede virksomheder vil udvikle disse kapabiliteter på en samlet cloud-platform frem for at forsøge at sammensætte en række lokale punktløsninger. I sidste ende vil muligheden for at kombinere arbejdsgange til forebyggelse af svindel og vurdering af kreditrisiko skabe de mest effektive resultater. 69% af vores respondenter planlægger da også at integrere svindelforebyggelse og kreditrisikovurdering i en samlet risikostyringsstrategi i den nærmeste fremtid.

En anden central prioritet er at reducere omkostningerne ved undersøgelser. Dette kan opnås på flere måder, men øget automatisering spiller en afgørende rolle. Mange svindelteams er i dag afhængige af manuelle gennemgange for at håndtere svindeltrusler, og mere end en tredjedel (35%) angiver, at en manuel gennemgang tager en uge eller længere. Med adgang til de rette svindelsignaler kan en langt større del af beslutningsprocessen automatiseres, hvilket både reducerer undersøgelsesomkostningerne og giver svindeleksperter mulighed for hurtigere at fokusere på de mest komplekse sager.

Den sidste prioritet, der fremhæves i undersøgelsen, er investering i et orkestreringslag for svindelværktøjer (67%). En tilsvarende andel af respondenterne er enige i, at orkestrering af flere svindelløsninger på én samlet platform repræsenterer fremtiden for effektiv svindelforebyggelse. Fordelene er tydelige: Orkestrering forbedrer kundeoplevelsen og reducerer omkostninger ved kun at gennemføre svindeltjek, når kundens risikoscore gør det nødvendigt.

## De fem vigtigste prioriteter inden for svindel i det kommende år




Basis: 979 ledende beslutningstagere inden for svindel i EMEA og APAC
Kilde: Experian-undersøgelse udført af Forrester Consulting, juli 2025

ANDEN DEL: Teknologidrevne løsninger

# Hvorfor machine learning er afgørende for at bekæmpe svindel

## Jo flere datakilder der inddrages i en vurdering - eksempelvis enheds- og adfærdsdata - desto mere præcise bliver beslutningerne.

At omsætte disse store datamængder til reel indsigt kræver imidlertid machine learning (ML). Kun ML har den nødvendige analytiske kapacitet til at identificere komplekse mønstre i så omfattende datasæt. Dette afspejles tydeligt i vores undersøgelser: **67% af organisationer, der anvender ML, har oplevet en målbar forbedring i nøjagtigheden af deres svindeldetektion siden implementeringen.**

En anden central fordel ved ML er muligheden for løbende at genoptræne modeller på nye data og dermed holde trit med hurtigt skiftende svindeltaktikker. Regelbaserede systemer har vanskeligt ved at tilpasse sig nye svindelformer, da tilføjelsen af nye regler øger kompleksiteten og typisk medfører flere falske positiver og et større behov for manuel sagsbehandling.

Mere end to tredjedele (67%) af ML-brugerne angiver, at kontinuerlig genoplæring og opdatering af modeller har gjort dem bedre i stand til at håndtere en svindeltrussel i hastig udvikling. Samtidig har den samme andel konstateret en procentvis reduktion i antallet af falske positiver efter implementeringen af ML.

ML

**70 %**

**er enige i, at ML har forbedret deres evne til at detektere svindel, som et system, der kun er baseret på regler, ville have overset.**

### Hvordan påvirker ML de virksomheder, der har taget det i brug?

**67 %**

Der er procentvis færre falske positive siden implementeringen af ML.

**68 %**

ML har givet os mulighed for at reducere sikkerhedsfriktionen for gode kunder ved at bruge passive svindelkontroller.

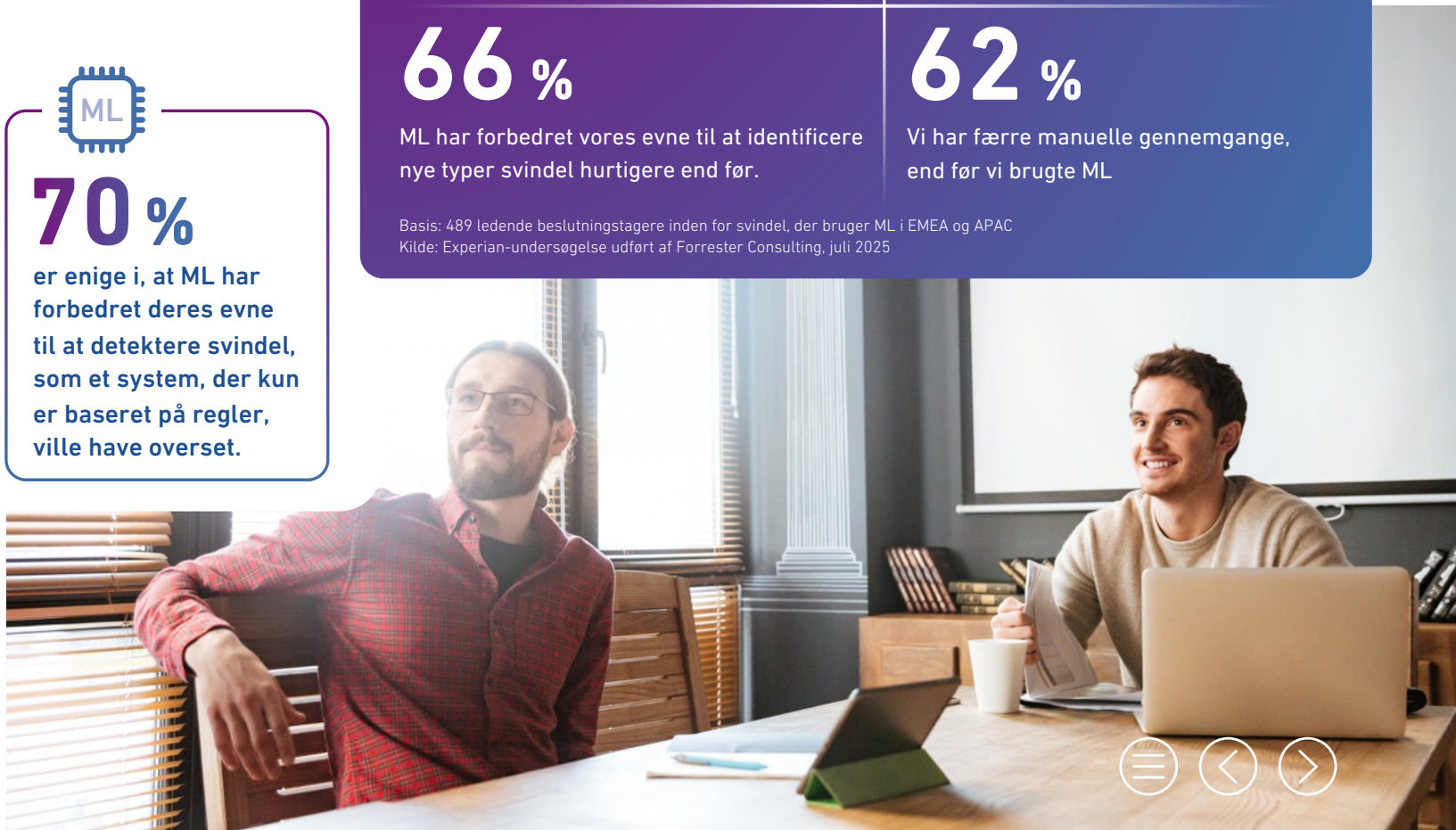
**66 %**

ML har forbedret vores evne til at identificere nye typer svindel hurtigere end før.

**62 %**

Vi har færre manuelle gennemgange, end før vi brugte ML

Basis: 489 ledende beslutningstagere inden for svindel, der bruger ML i EMEA og APAC
Kilde: Experian-undersøgelse udført af Forrester Consulting, juli 2025



## Hvad er de største fordele ved machine learning?

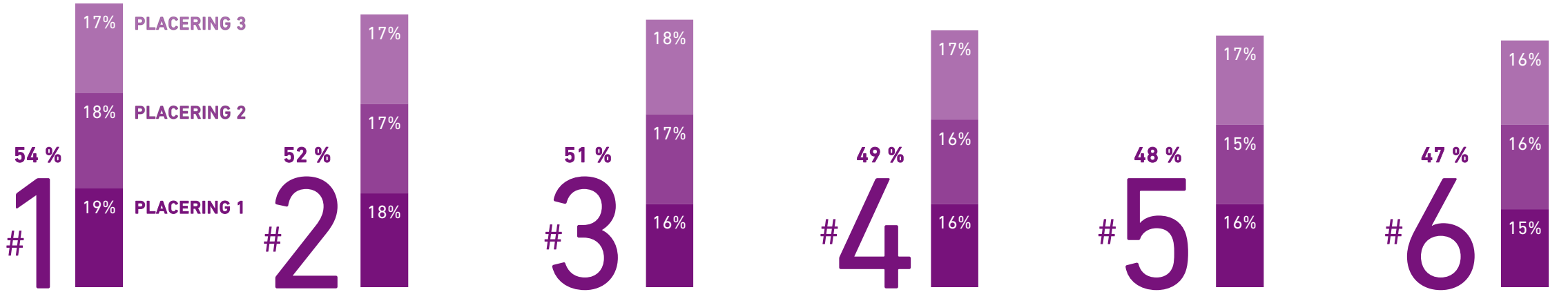
Vores undersøgelse viser, at den væsentligste fordel ved at implementere machine learning (ML) er muligheden for at opdage svindel i realtid (54 %). I dag er det kun en tredjedel (33 %) af organisationerne, der kan detektere svindel i realtid, mens et tilsvarende antal (32 %) reagerer inden for en dag eller mindre. Samtidig angiver 35 %, at det tager en uge eller længere at identificere svindel.

Tæt knyttet til hurtigere identifikation er en forbedret kundeoplevelse (52 %), som vurderes som den næstvigtigste fordel. Kundeoplevelse handler dog ikke udelukkende om hurtigere beslutninger. Lige så afgørende er det at minimere friktion i kunderejsen. Passive svindelkontroller, som kan gennemføres uden at afbryde eller belaste kunden, spiller derfor en central rolle i moderne svindelforebyggelse.

Experian tilbyder en række aktive og passive identitets- og svindelkontroller samt vores prisbelønnede orkestreringsplatform, der hjælper dig med at finde den perfekte balance.

Se denne korte video, for at se hvordan din kunde-onboarding-rejse kunne se ud.


### Identificering af svindel i realtid er den største fordel ved machine learning



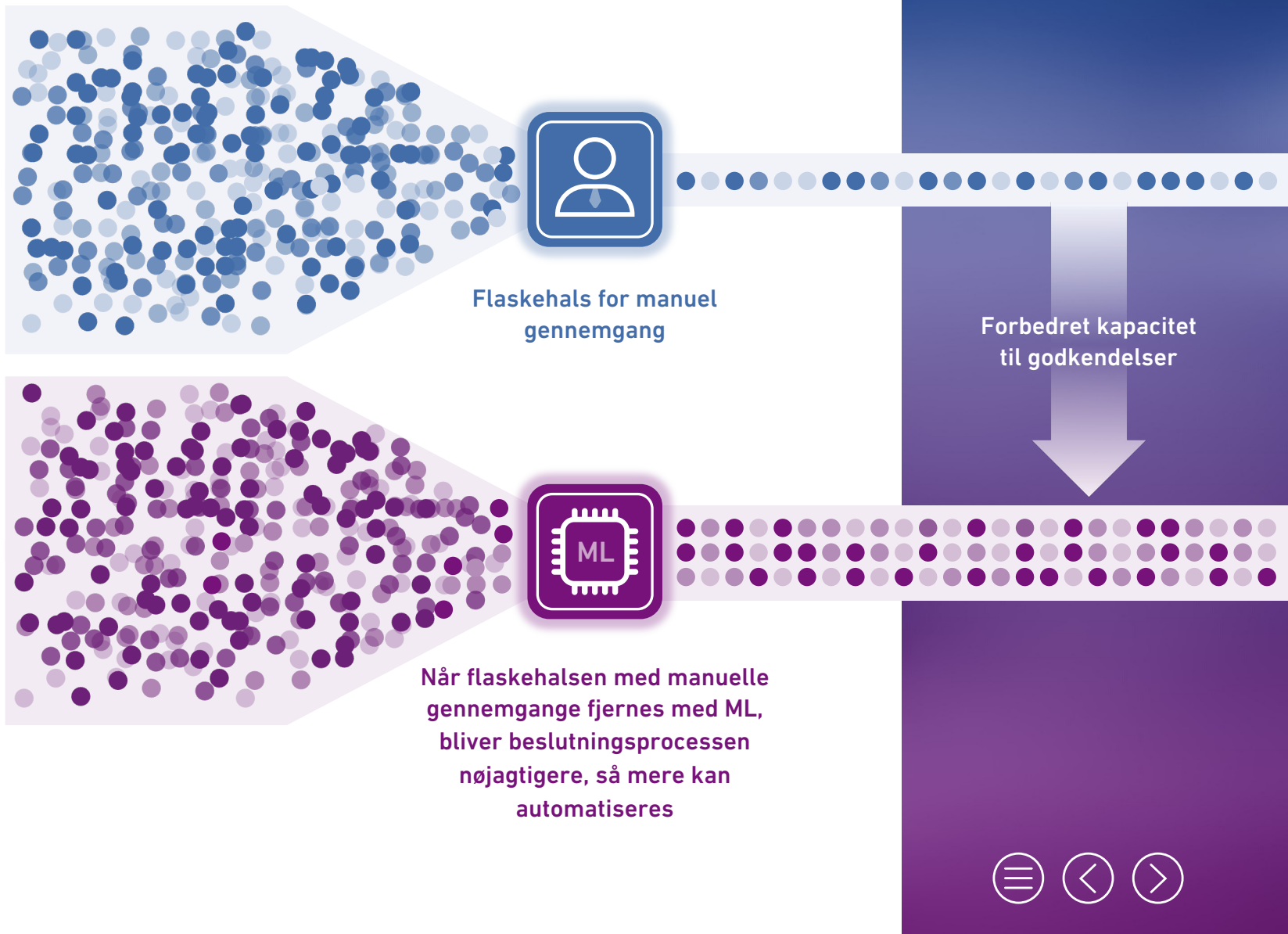

Basis: 489 ledende beslutningstagere inden for svindel, der bruger ML i EMEA og APAC
Kilde: Experian-undersøgelse udført af Forrester Consulting, juli 2025

## Machine learning kan markant reducere flaskehalse i manuel gennemgang

Næsten to tredjedele (64 %) af organisationerne anvender i dag manuel gennemgang til at håndtere svindeladvarsler, og andelen stiger til 70 % blandt respondenter inden for e-handel. Denne afhængighed af manuelle processer skaber betydelige flaskehalse, som ofte resulterer i langsomme og frustrerende ansøgnings- eller købsrejser for ellers legitime kunder – med stor risiko for, at mange vælger at afbryde processen.

Machine learning muliggør mere præcise anbefalinger og dermed en højere grad af automatisering. Næsten tre fjerdedele (71 %) af organisationer, der anvender ML, angiver, at teknologien gør dem bedre i stand til at prioritere manuelle gennemgangssager. Dette har samtidig ført til en markant forbedring af svindelanalytikernes produktivitet.

### Månedlige applikationer/køb med og uden ML



## Hvorfor bliver Machine Learning ikke taget i brug?

Sammenlignes vores seneste undersøgelser inden for machine learning i kreditrisiko med denne svindelundersøgelse, fremgår det, at nogle beslutningstagere på kreditrisikoområdet fortsat ikke fuldt ud forstår værdien af ML og derfor endnu ikke har investeret i teknologien.

Billedet ser anderledes ud inden for svindelforebyggelse. Her angiver et flertal af beslutningstagerne, at den største barriere for at tage ML i brug er manglen på tilstrækkelige kvalitetsdata til træning af modeller – 73% er enige i dette. Det indikerer, at mange allerede anerkender den værdi, ML kan skabe, men oplever praktiske udfordringer i forhold til implementeringen.

**Betydningen af adgang til tilstrækkelige datakilder af høj kvalitet kan ikke overvurderes.** Effektiv svindelforebyggelse forudsætter store mængder data fra forskellige kilder, og med udbredelsen af ML er data blevet en endnu mere central strategisk ressource.

For at ML-modeller kan levere præcise forudsigelser, skal træningsdatasæt være både omfattende og korrekt mærkede. Forhåndstrænede modeller, der er klar til brug, kan bidrage til at reducere denne barriere. Det samme gælder anvendelsen af syntetiske data, som kan bruges til at udvide og styrke eksisterende træningsdatasæt.

## Lovgivningsmæssige bekymringer ved brug af machine learning

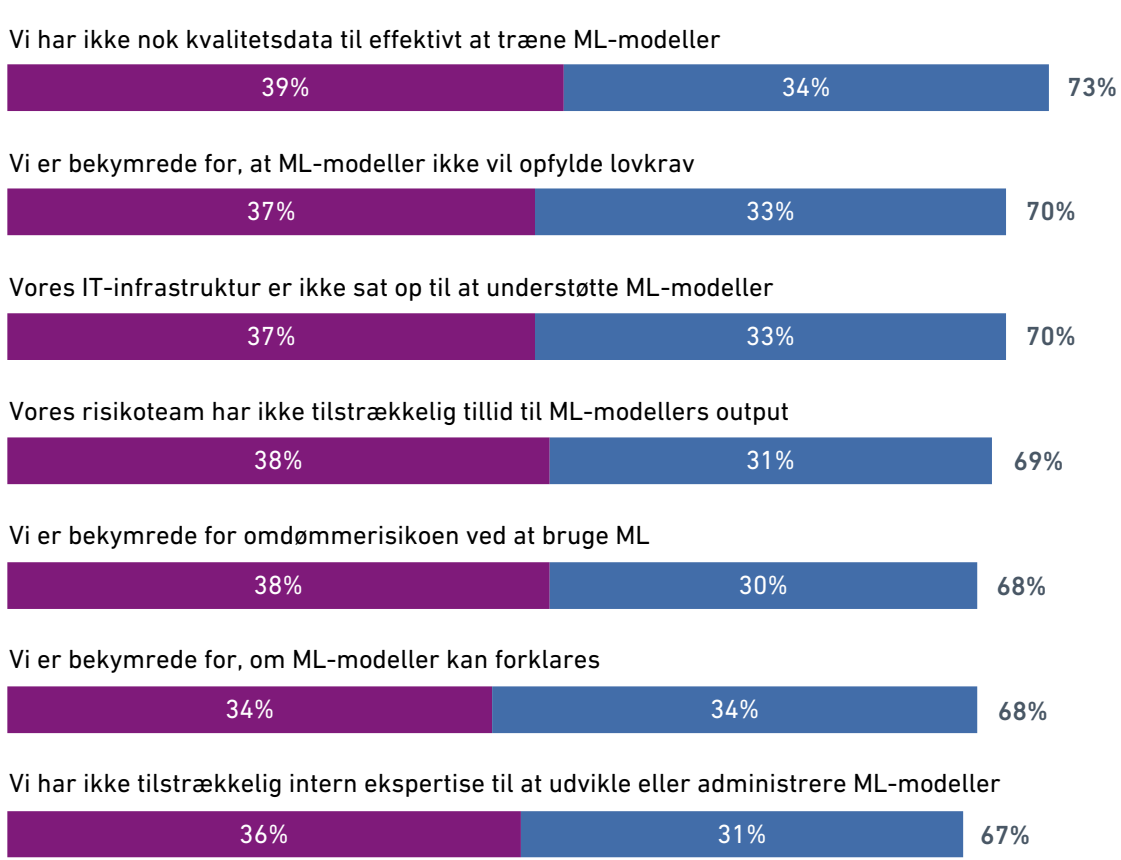
Lovgivere verden over befinder sig på forskellige stadier i reguleringen af brugen af machine learning til svindeldetektion med det formål at sikre gennemsigtighed og retfærdighed. Forklarlig machine learning (explainable AI) gør det muligt for afviste kunder at anfægte beslutninger, mens fuld reviderbarhed bidrager til at opbygge tillid til ML-baserede beslutninger blandt virksomhedens brugere.

ML-modeller kan designes til at være fuldt forklarlige med tydelige begrundelser for hver enkelt beslutning. Der hersker dog fortsat usikkerhed om, hvilke krav lovgivere konkret vil stille, og hvordan disse bedst imødekommes i praksis. 71% af vores respondenter angiver, at de ville sætte pris på større lovgivningsmæssig klarhed om anvendelsen af ML i systemer til forebyggelse af svindel.

**Mere end to tredjedele (67%) er enige i, at manglende regulatorisk klarhed om acceptable anvendelsesscenarier for ML inden for svindelforebyggelse holder dem tilbage fra at tage teknologien i brug.**

- Interne funktioner
- Lovregler
- Interne funktioner
- Tillid
- Omdømme
- Lovregler
- Interne funktioner

### De vigtigste grunde til, at machine learning ikke er blevet taget i brug




Basis: 490 ledende beslutningstagere inden for svindel, der ikke bruger ML i EMEA og APAC
Kilde: Experian-undersøgelse udført af Forrester Consulting, juli 2025

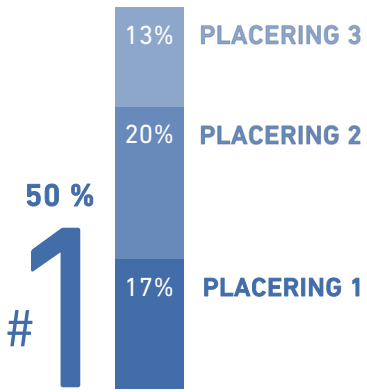
## Hvilke faktorer ville tilskynde ikke-brugere til at tage ML i brug?

Dokumenteret ROI fra kolleger er den største faktor, der ville tilskynde til at indføre ML. Som med al anden ny teknologi ønsker de fleste virksomheder at være "de første, der bliver de næste", så de kan lære af dem, der er gået foran. Selvom dette er en sikrere måde at gribe systemændringer an på, kræver den nuværende alvorlige svindeltrussel en mere proaktiv tilgang til at indføre den mest avancerede teknologi til forebyggelse af svindel.

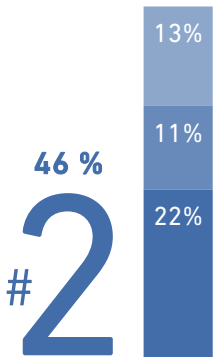
Mange virksomheder har allerede implementeret ML med gode resultater og positiv ROI. For en Experian-kunde, der for nylig skiftede til en ML-model, var tidsrummet til positiv ROI mindre end en måned, da den identificerede et stort syndikatangreb kort efter at være taget i brug.

Virksomheder, der er interesserede i at forstå værdien af ML, kan arrangere en offline Proof-of-Value (POV)-vurdering. Dette giver dem mulighed for at se fordelene ved ML baseret på aftalte målepunkter uden at forbinde deres system til modellen.

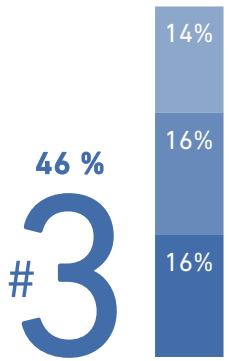
### Påviselig ROI og klarere lovgivningsmæssige retningslinjer ville stimulere indførelsen af ML



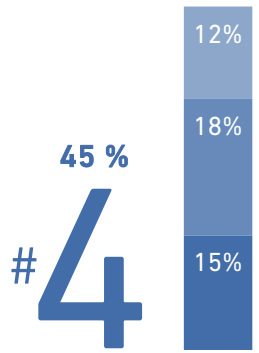

Påviselig positiv ROI fra sammenlignelige organisationer



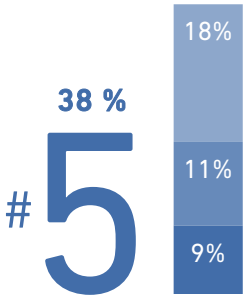

Klarere regulatoriske retningslinjer på de markeder, hvor vi opererer



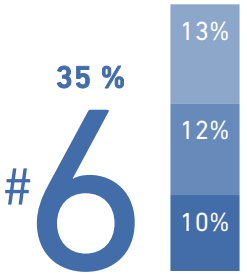

Øget intern ekspertise i data science for at lette indførelsen af ML




Tilgængelighed ML-modeller, der er klar til brug og kan forklares helt




Adgang til en intern analytisk sandbox, hvor vi kunne eksperimentere med ML-modeller




Lavere omkostninger ved implementering

Basis: 490 ledende beslutningstagere inden for svindelhåndtering, som bruger ML i EMEA og APAC
Kilde: Experian undersøgelse gennemført af Forrester Consulting, Juli 2025

# GenAI-assistenter og digitale identitetsløsninger

## En spændende udvikling inden for svindelhåndtering er GenAI-assistenter, der er indlejret i platforme til forebyggelse af svindel. Disse værktøjer kan konsolidere vigtige datapunkter som regler og deres resultater, årsager til svindel og matchvarigheder (dato/tidspunkter).

De kan også give en sag et risikoniveau med passende begrundelse og instruktioner om "næste skridt" for at gennemføre en undersøgelse. Derudover kan de strømline manuelle processer og derved forbedre både effektivitet og nøjagtighed af beslutningstagning.

Vores undersøgelse viser, at 80 % af respondenterne mener, at den største fordel ved en GenAI-assistent er at gøre deres svindelforebyggelsesprocesser mere tilgængelige for mindre tekniske medarbejdere.

### Hvad kunne en GenAI-svindelassistent gøre for din virksomhed?

**77 %**

tror, at den største fordel ved en GenAI-assistent er at reducere den tid, der skal bruges til at håndtere svindelsager.

**72 %**

er enige i, at en GenAI-assistent, der er grundigt trænet i svindeldata, kunne hjælpe dem med at foretage mere præcise svindelvurderinger.

**71 %**

tror, at en GenAI-drevet assistent kunne reducere den tid og indsats, der skal bruges til at håndtere nye svindelsager, betydeligt.

**66 %**

er enige i, at deres organisation er interesseret i at integrere denne slags teknologi i deres arbejdsgange til forebyggelse af svindel.

Basis: 979 ledende beslutningstagere inden for svindel i EMEA og APAC
Kilde: Experian-undersøgelse udført af Forrester Consulting, juli 2025

## Fremtiden for digitale identiteter

EU har for nylig skitseret sin plan for anerkendelse af digitale identitetsløsninger på tværs af EU og internationalt som led i eIDAS 2.0. Inden for de næste to år skal alle medlemsstater tilbyde digitale identitetsløsninger, og udbydere af finansielle tjenester og telekommunikation vil være forpligtet til at acceptere dem.

Digitale ID-initiativer er samtidig under udrulning i lande som Singapore, Malaysia og Australien, mens Indien går forrest med sit Aadhaar-program. Programmet beskrives ofte som et af verdens mest avancerede digitale ID-systemer og har i dag mere end én milliard registrerede brugere.

Næsten tre fjerdedele (74%) af vores respondenter betragter digitale identitetsløsninger som en strategisk mulighed for at styrke forebyggelsen af svindel. Et tilsvarende antal (73%) planlægger aktivt at integrere digitale identitetsløsninger i deres kunderejser.

Digitale identiteter har et betydeligt potentiale til at reducere identitetsrelateret svindel. Offentlige og private oplysnings- og uddannelsesinitiativer vil dog være afgørende for at opbygge tillid til løsningerne og fremme udbredelsen. Potentialet understreges af, at 70% af respondenterne er enige i, at indførelsen af digitale identitetsløsninger grundlæggende vil ændre den måde, de onboarder og verificerer deres kunder på.

**74%**

er enige i, at udbredt anvendelse af digitale identitetsløsninger kunne reducere afhængigheden af traditionel "kend din kunde" og dokumentbekræftelse.

# Det voksende skift mod delt svindelintelligens

Kollektiv svindelintelligens vil uden tvivl spille en central rolle i fremtidens forebyggelse af svindel. **73% af de adspurgte er enige i, at den mest effektive måde at imødegå svindeltruslen på er gennem samarbejde og fælles indsats.**

Denne informationsudveksling forudsætter imidlertid en pålidelig tredjepart. Tre fjerdedele (75%) vurderer, at opbygning af tillid mellem medlemmerne i et konsortium til bekæmpelse af svindel er afgørende for succes.

Effektive konsortier kræver en central administrationshub med sikre API-forbindelser til hvert enkelt medlem. En sådan struktur gør det muligt at dele følsomme data på tværs af netværket, samtidig med at gældende regler for databeskyttelse og datadeling overholdes. På den måde kan hver applikation krydstjekkes mod den samlede intelligenspulje, uden at medlemmerne behøver at dele data direkte med hinanden.

**74%**

**er enige i, at de fleste virksomheder i løbet af de næste tre år vil være en del af en delt svindeldatagruppe.**

Hvis du vil vide mere om, hvordan konsortier fungerer, og hvordan man bliver en del af et, kan du læse Experians Køberguide til konsortier:

STYRKEN VED DELT INTELLIGENS


## Dataoverførselsproces i et konsortium

**1**

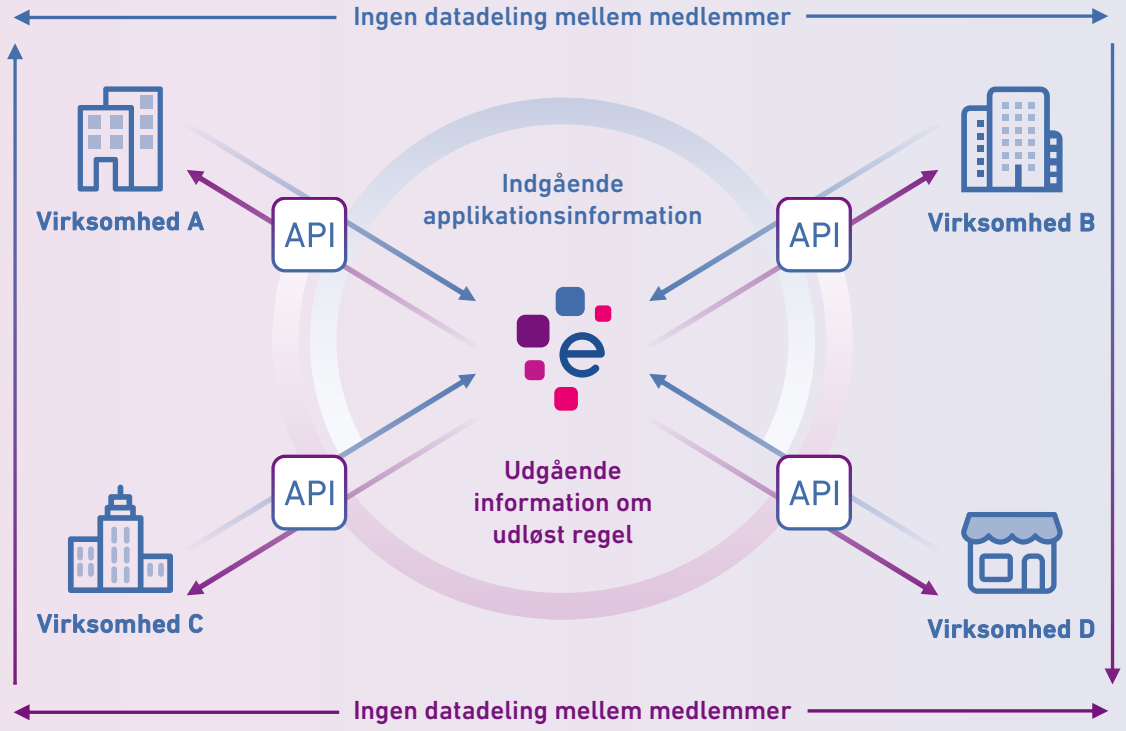
Hver virksomhed sender applikations-/købsdata til den centrale database via en individuel sikker API

**2**

Hvis applikationsdataene udløser en advarsel i den centrale hub, returneres den regel, der er blevet udløst, til virksomheden

**3**

Ingen data deles direkte mellem virksomheds-medlemmer



# De vigtigste take aways

GenAI og deepfakes har permanent ændret svindellandskabet. I takt med at disse værktøjer bliver stadig mere sofistikerede, er supplerende lag af svindelsignaler – såsom enheds- og adfærdsdata – blevet afgørende for at forhindre en accelererende stigning i svindeltab.

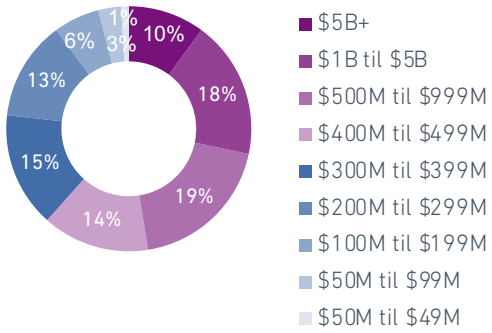
En strategisk gennemgang af eksisterende svindelværktøjer med henblik på at identificere manglende kapabiliteter er den højest prioriterede indsats for det kommende år. Herefter følger migration af svindelløsninger til cloud-baserede platforme samt investering i nye, ML-drevne svindelværktøjer.

Den væsentligste fordel ved machine learning er evnen til at opdage svindel i realtid. Dernæst følger en forbedret kundeoplevelse gennem reduceret friktion i onboarding- og købsrejser, hvilket i høj grad muliggøres af passive svindelsignaler.

Kollektiv deling af svindelintelligens via konsortier vil spille en afgørende rolle i fremtidens svindelforebyggelse. For at sikre regulatorisk overholdelse og opbygge tillid mellem deltagerne er det imidlertid afgørende, at dette samarbejde faciliteres af en betroet tredjepart.

# Firmografi og respondentdemografi

## VIRKSOMHEDENS OMSÆTNING



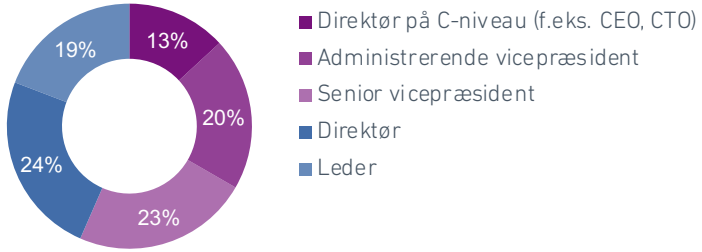

## GEOGRAFI

N=~109 i hvert land

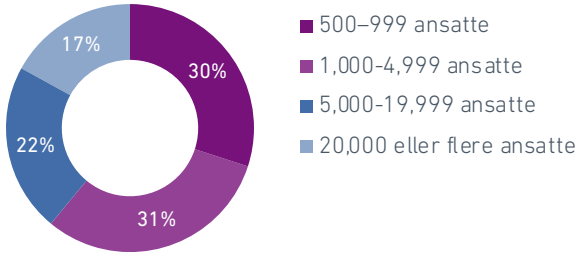
Danmark, Spanien, Italien, Tyskland, Sydafrika, Norge

New Zealand, Australia, India

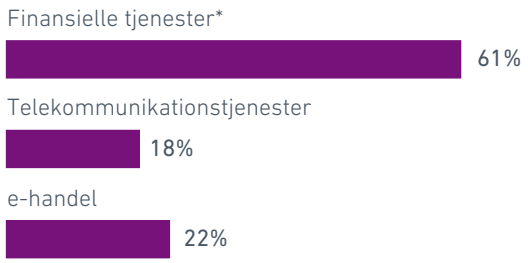
## RESPONDENTNIVEAU




## VIRKSOMHEDENS STØRRELSE




## BRANCHE




* Bankvirksomhed (38%), kommerciel finansiering/leasing (21%), bilfinansiering (25%), forbrugslån (16%)

## DIREKTE ANSVAR FOR BESLUTNINGSTAGNING

# Ordliste

### API-SVINDELANGREB

Udnyttelse af sårbarheder i API'er for at få uautoriseret adgang til data, denial of service-angreb eller manipulation af API'et på en anden skadelig måde.

### SVINDEL MED AUTORISERET PUSH-BETALING (APP)

Svindlere manipulerer ofre til frivilligt at foretage betalinger til dem gennem social engineering, f.eks. ved at udgive sig for at være fra en betroet finansiel institution.

### ADFÆRDSBASERET BIOMETRI

Identifikation og analyse af datapunkter forbundet med den ubevidste måde, en bestemt bruger interagerer med sin enhed på – uden at indsamle personoplysninger. Disse omfatter musebevægelser, tastetryk eller tryk på berøringsskærmen og mange hundrede andre adfærdsattributter.

### ADFÆRDSANALYSE

Identifikation af bot-angreb ved at sammenligne den måde, mennesker interagerer med enheder på, med den måde, bots interagerer med enheder på.

### BOT-/CREDENTIAL STUFFING

Automatiserede svindelangreb, hvor lister med stjålne legitimationsoplysninger fra en organisation bruges til at forsøge at få uautoriseret adgang til en konto hos en anden organisation.

### ENHEDSPROFILERING/FINGERAFTRYK

Analyse af et sæt software- og hardwareparametre forbundet med en bestemt enhed for at give en unik identifikator og vurdere risikoen. Disse parametre omfatter operativsystem, netværk, browser, sprog, tidszone, skærmforhold og mange flere.

### ENHEDSINTELLIGENS

Enhedsdata kombineret med adfærdsdata kaldes samlet set for enhedsintelligens. Den giver kontinuerlige
og passive tegn til at detektere svindel.

### DEEPFAKES

Video, lyd eller billeder, der på overbevisende vis er blevet ændret og manipuleret for at give et forkert billede af en person, der gør eller siger noget, som faktisk ikke blev gjort eller sagt. I svindelsammenhæng kan de bruges til at narre "kend din kunde"-tjek med en falsk person.

### FRAUD-AS-A-SERVICE (FAAS)

Svindelværktøjer og -tjenester, der for det meste sælges på det mørke net på betal-som-du-bruger-basis.

### PENGEKURÉR

En person, der hjælper med at hvidvaske kriminelle gevinster ved at modtage penge på sin egen konto og derefter overføre dem til en anden konto på vegne af en svindler. Disse mellemmænd rekrutteres ofte på sociale medier og er måske ikke klar over, at det er ulovligt at være pengekurér.

### FYSISK BIOMETRI

Unikke fysiske egenskaber, der kan bruges til at identificere individuelle brugere. For eksempel liveness detection, der bruger ansigtsgenkendelse.

### SYNTETISK IDENTITET

En kombination af ægte og falske personoplysninger bruges til at skabe en opdigtet identitet, der er svær at detektere.

### SYNTETISK VIRKSOMHED

Ligesom en syntetisk forbrugeridentitet bruger disse falske virksomheder en kombination af ægte og falske data til at skabe en simulation af en legitim virksomhed.

### TREKANTSSVINDEL

Et fupnummer inden for e-handel, hvor en svindler opretter en falsk onlinebutik for at indsamle betalinger fra intetanende kunder for derefter at bruge stjålne kreditkortoplysninger fra en tredjepart til at købe de samme varer fra en legitim forhandler og sende produktet til den oprindelige kunde. Kunden modtager sin ordre, svindleren stikker pengene i lommen, og den legitime forhandler bliver til sidst ramt af en tilbageførsel fra det stjålne korts ejer, hvilket resulterer i økonomisk tab og potentiel skade på dennes omdømme.

# Om Experian

## Experian er en global data- og teknologivirksomhed, der skaber muligheder for mennesker og virksomheder i hele verden.

Vi hjælper med at omdefinere udlånspraksis, afdække og forhindre svindel, forenkle sundhedsydelser, levere digitale marketingløsninger og få dybere indsigt i bilmarkedet, alt sammen ved hjælp af vores unikke kombination af data, analyser og software. Vi hjælper også millioner af mennesker med at realisere deres økonomiske mål og hjælper dem med at spare tid og penge.

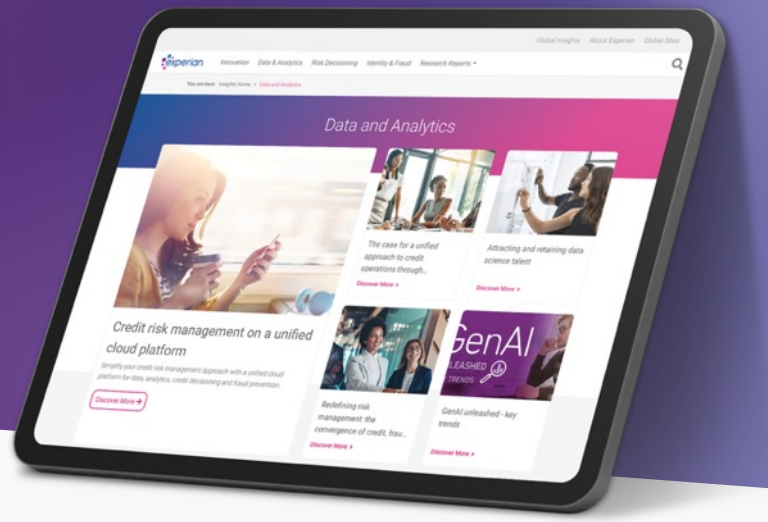
Vi opererer i hele spektret af markeder, fra finansielle tjenester til sundhedspleje, bilindustrien, landbrugsfinansiering, forsikring og mange flere branchesegmenter.

Vi investerer i talentfulde mennesker og nye avancerede teknologier for at udnytte datakraft og skabe innovation. Vi er en FTSE 100-indeksvirksomhed, der er noteret på London Stock Exchange (EXPN), og vi har et team på 25.100 mennesker i 32 lande. Vores hovedkvarter ligger i Dublin, Irland.

**Få mere at vide på experianplc.com**

Læs mere →

Kontakt din lokale Experian-konsulent, eller besøg experianacademy.com




Hjemstedsadresse: The Sir John Peace Building, Experian Way, NG2 Business Park, Nottingham, NG80 1ZZ, Storbritannien Telefon: +44-(0)844 481 9920 businessuk@experian.com experian.co.uk/business

© Experian 2025. Alle rettigheder forbeholdes. Experian Ltd er autoriseret og reguleret af Financial Conduct Authority. Experian Ltd er registreret i England og Wales under virksomhedsregistreringsnummer 653331. Ordet "EXPERIAN" og det grafiske element er varemærker tilhørende Experian og/eller virksomhedens tilknyttede virksomheder og kan være registreret i EU, USA og andre lande. Det grafiske element er et registreret EU-design. Experian Public.