Velkommen til Experians svindelrapport for 2026

De siste årene har vi sett at svindeltrusselen har vokst betydelig. Den har blitt mer organisert og industrialisert, og stadig kraftigere verktøy har bidratt til en markant økning i både omfanget og kompleksiteten av angrepene.

Hele regioner har utviklet seg til megafabrikker for svindel som retter seg mot intetanende mennesker over hele verden. Samtidig ser vi en økende trussel fra statssanksjonerte kriminelle organisasjoners involvering i disse koordinerte angrepene. Dette har fått enkelte eksperter til å hevde at vi befinner oss midt i svindelens gullalder.

Å møte denne utfordringen krever tettere samarbeid, ettersom våre individuelle tiltak blir langt mer effektive når de kombineres. Virksomheter som er del av Experians nettverk av svindelkonsortier, opplever ofte en betydelig reduksjon i svindeltap ved å dra nytte av den kollektive intelligensen som deles i nettverket.

Det har også blitt avgjørende for virksomheter å ta i bruk den mest avanserte teknologien for svindelforebygging. Kunstig intelligens har blitt en sentral muliggjører i dette forsvaret, der både maskinlæring og generativ KI åpner for nye muligheter til å identifisere svindlere mer presist, raskt tilpasse seg endringer og håndtere svindelsystemer mer effektivt. Dette bidrar til å beskytte både virksomheter og deres kunder.

I årets undersøkelse, gjennomført i samarbeid med Forrester Consulting, har vi spurt nærmere tusen beslutningstakere innen svindelhåndtering i ni land om deres syn på de viktigste trendene som påvirker svindelforebygging. Jeg er trygg på at deres samlede innsikter vil hjelpe deg med å videreutvikle og spisse svindelstrategien for året som kommer.

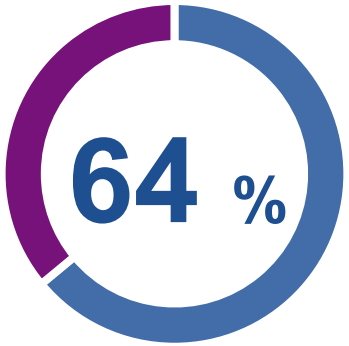
Når du er klar til å starte en samtale om vår helhetlige plattform for svindelforebygging, ser vårt globale team av ekspertkonsulenter frem til å komme i dialog med deg.

.

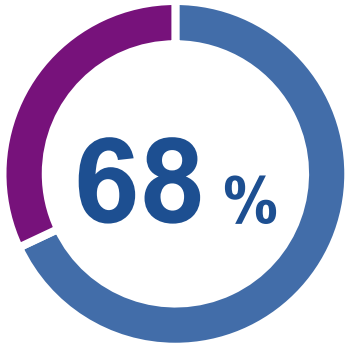
SHAIL DEEP
COO Experian EMEA og APAC

Innhold

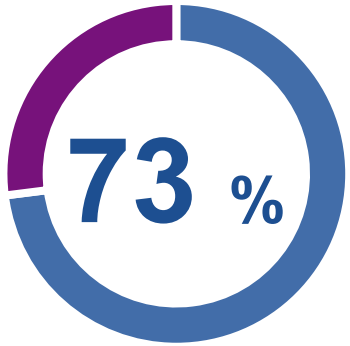
Oversikt over hovedfunn



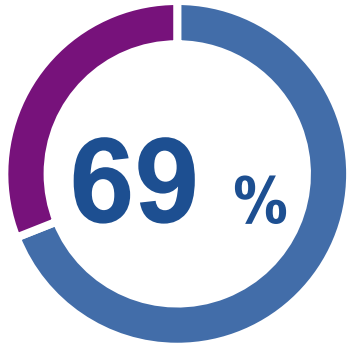
oppgir at deres svindeltap har økt fra år til år.



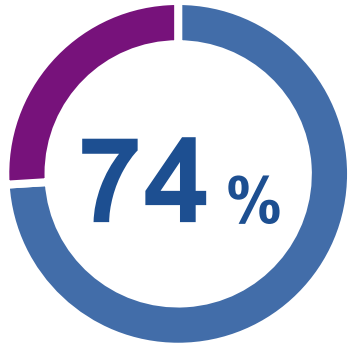
er enige i at deres nåværende teknologi stabel er utilstrekkelig for å møte en raskt utviklende svindeltrussel.



er interessert i å investere i passive svindelsjekker, som atferds- og enhetsdata, for å minimere friksjon.



planlegger å integrere svindelforebygging og kredittvurdering i en helhetlig risikostyringsstrategi.



er enige i at innen de neste tre årene vil et flertall av bedriftene være en del av en delt svindelinformasjonsgruppe.

Utvalg: 979 seniorbeslutningstakere innen svindelhåndtering fra EMEA og APAC
Kilde: Experian-undersøkelse gjennomført av Forrester Consulting, juli 2025

DEL 1: Utfordringer og prioriteringer

Rapport fra frontlinjen

Svindel

Svindel har aldri vært raskere eller billigere å gjennomføre enn i dag. Den doble trusselen fra stadig mer organiserte, transnasjonale cyberkriminelle nettverk og angrep drevet av generativ kunstig intelligens har ført til en betydelig økning i både omfanget og kompleksiteten av angrepene.

Ifølge en nylig studie har svindelsyndikater i Sørøst-Asia blitt omtalt som «det mektigste kriminelle nettverket i moderne tid». Disse nettverkene genererer årlige inntekter på mellom 50 og 70 milliarder dollar og har en arbeidsstyrke på over 350 000 personer. I tillegg tilbyr leverandører på dark web et stadig bredere spekter av Fraud-as-a-Service-løsninger, som gir svindlere tilgang til avanserte verktøy og oppdatert kriminell innsikt.

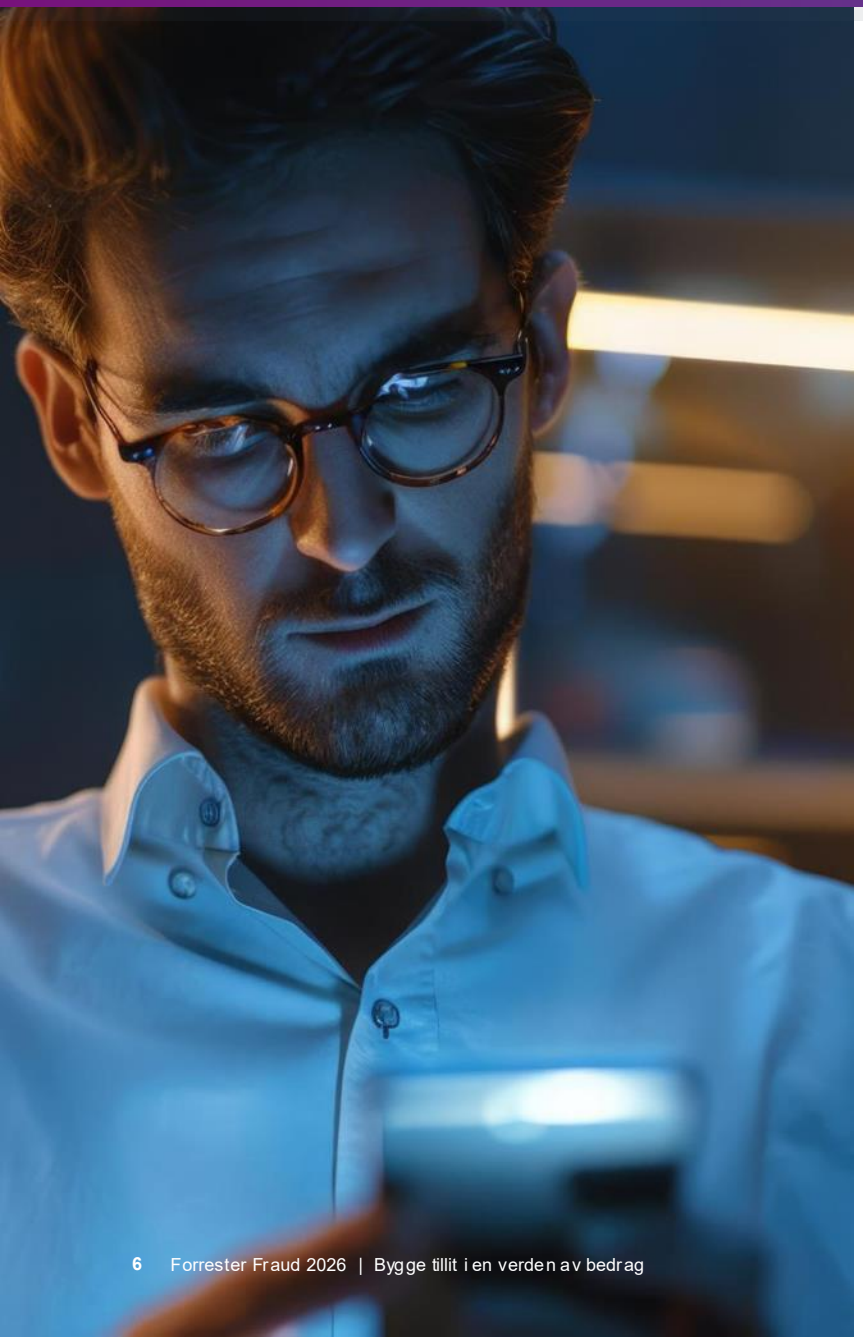
Vår forskning viser at denne trusselen rammer virksomheter over hele verden. **Mer enn to tredjedeler (67 %) av de spurte forventer flere svindelangrep i 2026 enn året før, noe som tilsvarer en årlig økning på 10 prosent.**

Som følge av denne utviklingen opplever 64 prosent av virksomhetene at svindeltapene har økt sammenlignet med året før. Den samme andelen erkjenner at organisasjonen deres sliter med å holde tritt med den raskt utviklende svindeltrusselen. Konsekvensene av denne «svindeltsunamien» strekker seg imidlertid langt utover økonomiske tap: 67 prosent er enige i at svindelsaker også påfører organisasjonen betydelig omdømmeskade.

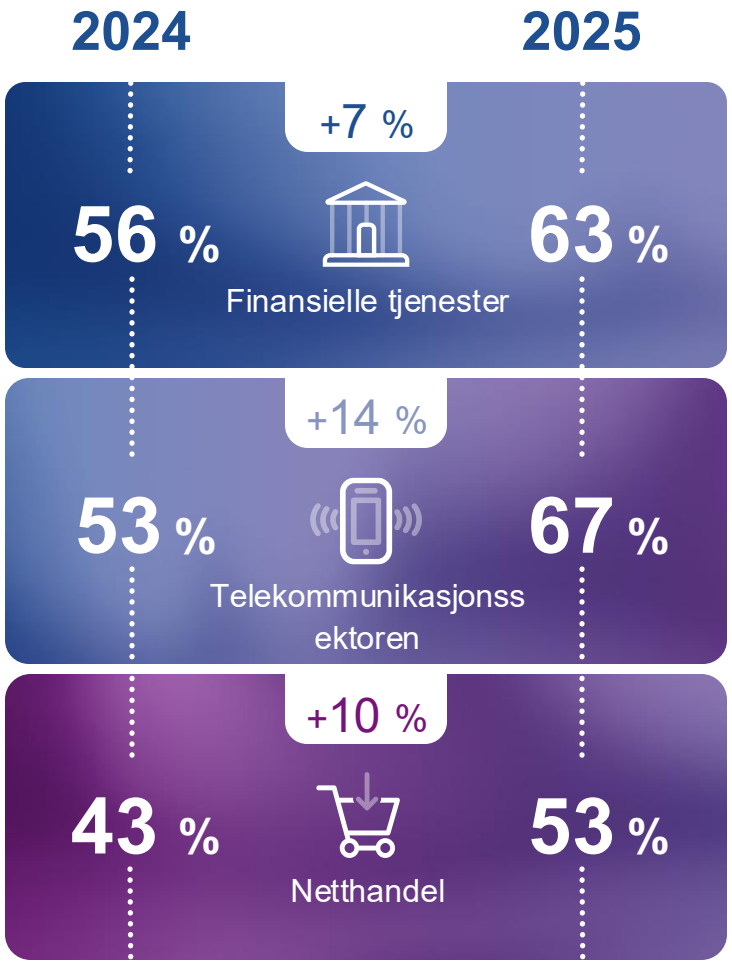
Hvilke typer svindel har økt mest?

Ser vi på de tre bransjene som inngikk i undersøkelsen, har telekommunikasjonssektoren opplevd den største økningen i det samlede antallet svindelangrep, der mer enn to tredjedeler (67 prosent) rapporterer en økning. Finanssektoren følger tett etter med 63 prosent, mens litt over halvparten (53 prosent) av aktørene innen netthandel rapporterer det samme.

67 % forventer flere svindelangrep enn i fjor



Prosentandel av organisasjoner som rapporterer økning i samlede svindelangrep 2024 vs. 2025



Utvalg: 979 seniorbeslutningstakere innen svindelhåndtering fra EMEA og APAC
Kilde: Experian-undersøkelse gjennomført av Forrester Consulting, juli 2025

Sammenlignet med året før er sosial manipulering, lojalitets- og belønningssvindel samt identitetstyveri de raskest voksende truslene innen finans- og telekommunikasjonssektoren. Økningen i sosial manipulering er ikke overraskende, gitt hvor kraftig generativ KI har blitt som fasiliterende verktøy for svindel. Forskningen indikerer også at svindlere i økende grad retter seg mot lojalitetsprogrammer og belønningsordninger, trolig fordi slike insentivsystemer ofte oppfattes som mindre sikre.

Identitetsverifisering har utviklet seg til å bli den viktigste sikkerhetsperimeteren og dermed også et hovedmål for svindlere. Etter hvert som legitime KI-agenter i stadig større grad samhandler med nettsteder side om side med bots og deepfakes, blir evnen til å autentisere og verifisere kunders identitet på en presis og pålitelig måte avgjørende.

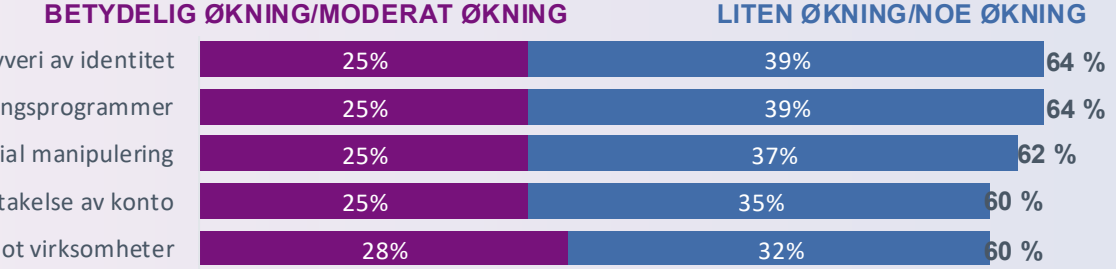
Innen netthandel har såkalt friendly fraud og misbruk av refusjonsordninger hatt den største økningen fra år til år. Angrep basert på syntetisk identitet har også økt, men i mindre omfang.

År-for-år-økning i typer svindelangrep per bransje

Finansielle tjenester

Økning i samlede svindelangrep: **63 %**

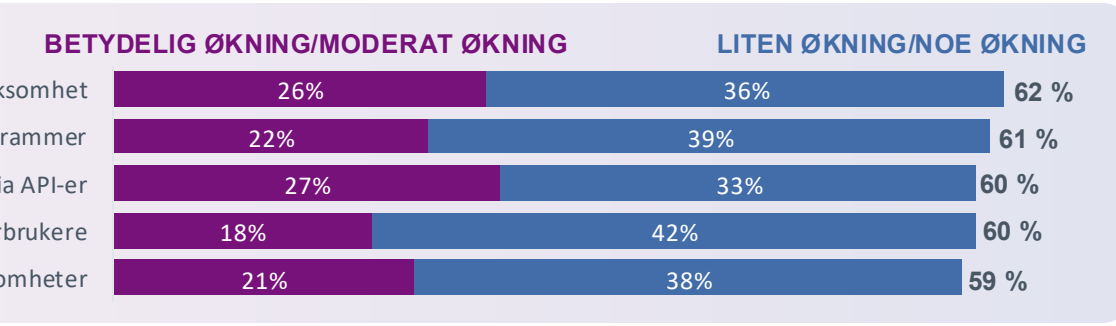
Tap som følge av svindel øker år for år: **64 %**



Telekommunikasjonssektoren

Økning i samlede svindelangrep: **67 %**

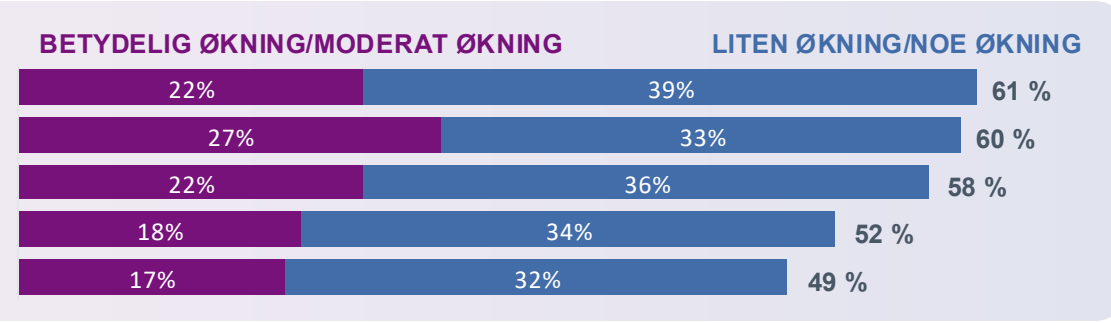
Tap som følge av svindel øker år for år: **66 %**



Netthandel

Økning i samlede svindelangrep: **53 %**

Tap som følge av svindel øker år for år: **61 %**



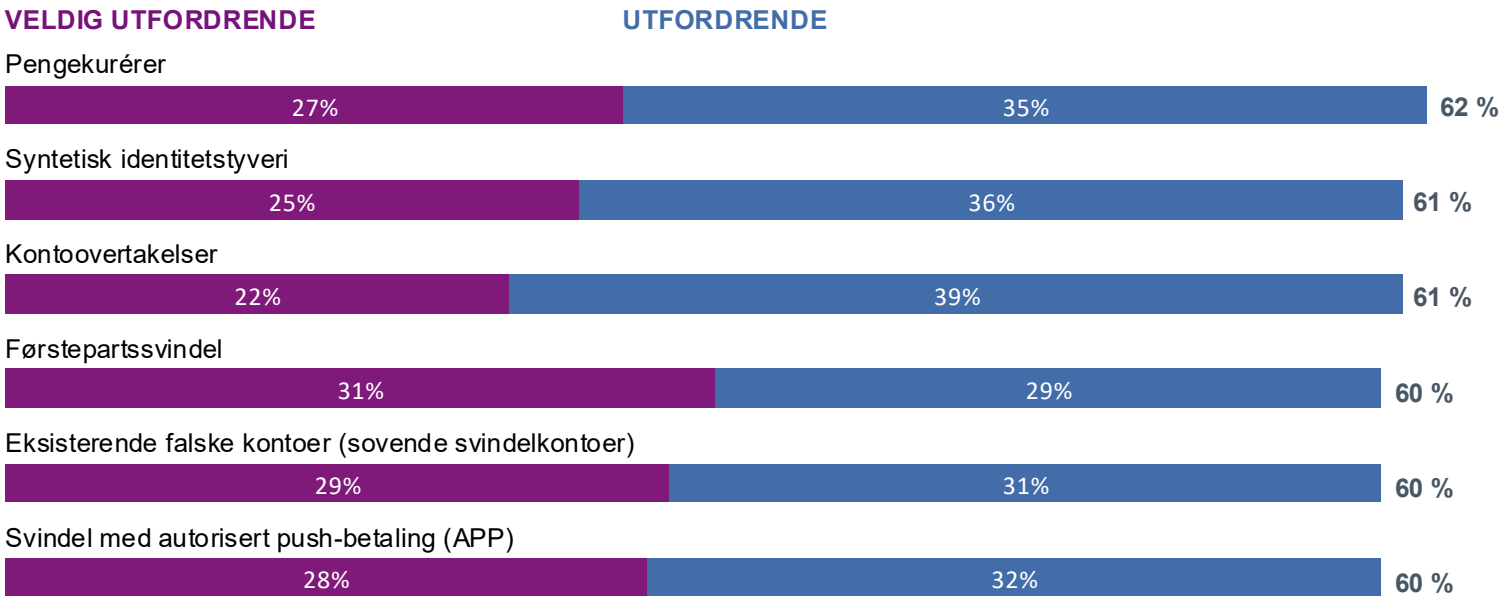
Utvalg: 979 seniorbeslutningstakere innen svindelhåndtering fra EMEA og APAC
Kilde: Experian-undersøkelse gjennomført av Forrester Consulting, juli 2025

Hvilke typer svindel er de mest utfordrende å oppdage og forhindre?

Vår forskning viser at pengekurérer er den mest utfordrende formen for svindel å motvirke, etterfulgt av svindel basert på syntetisk identitet og kontoovertakelse. Det er nettopp her utvidede svindelsignaler spiller en avgjørende rolle, ettersom de muliggjør kontinuerlig og passiv overvåking av brukerdata for å avdekke mønstre som kan indikere denne typen svindel.

Tradisjonelle autentiseringsmetoder kan i dag enkelt omgås gjennom sosial manipulering drevet av generativ KI og data hentet fra det mørke nettet. Svindeltyper som er vanskelige å avdekke, kan derfor kun forebygges ved hjelp av subtile enhets- og atferdssignaler som avslører når normal brukeratferd avviker fra det forventede.
Gitt at relativt få respondenter benytter avanserte autentiseringsverktøy, kun 42 prosent bruker i dag enhetsdata, og 39 prosent benytter atferdsbiometri, er det forståelig at denne typen svindel fortsatt er krevende å forhindre.

Hvilke typer svindel er de mest utfordrende å oppdage og forhindre?



Utvalg: 979 seniorbeslutningstakere innen svindelhåndtering fra EMEA og APAC
Kilde: Experian-undersøkelse gjennomført av Forrester Consulting, juli 2025

Uten disse verktøyene vil mange virksomheter oppleve økende svindeltap, ettersom svindlere får tilgang til systemene deres ved hjelp av kompromitterte legitimasjonsopplysninger. Overvåking av dark web har også blitt avgjørende for å ha oversikt over hvilke data som er i omløp, samt hvilke svindelmetoder og taktikker som til enhver tid benyttes.

De største utfordringene innen svindel

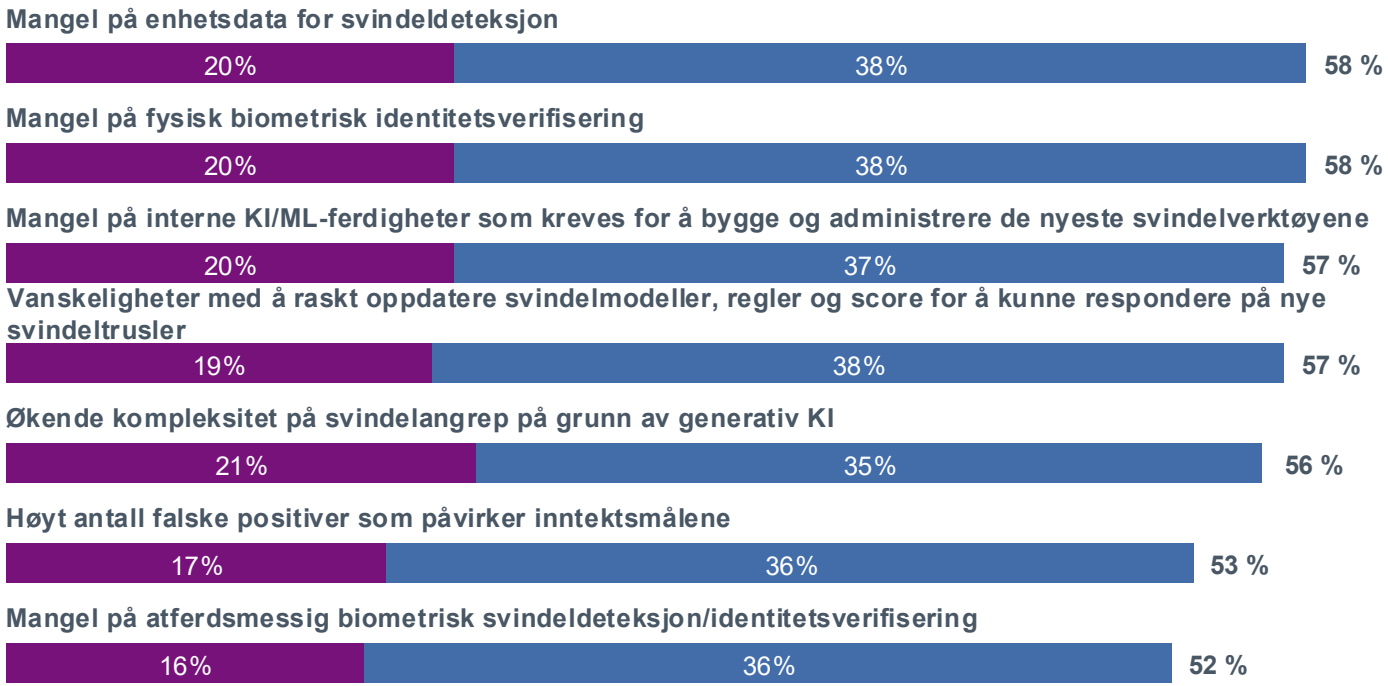
De tre største utfordringene som begrenser virksomheters evne til å oppdage og forebygge svindel, skyldes alle manglende kapasitet. Enhetsdata og fysisk biometri er identifisert som de viktigste manglende funksjonene, og tett knyttet til dette er behovet for KI- og maskinlæringsekspertise for å omsette disse signalene til presise og pålitelige svindelbeslutninger.

Vår forskning indikerer at mange virksomheter befinner seg i et kapasitetsgap: De eksisterende svindelsystemene er ikke lenger tilstrekkelige til å håndtere trusselbildet, samtidig som organisasjonene mangler kapasitet til å ta i bruk de avanserte verktøyene de trenger. Spørsmålet om «bygge versus kjøpe» er ikke nytt, men den raske økningen i både omfang og kompleksitet av svindelangrep har forsterket problemstillingen.

Virksomheter har behov for løsninger nå, ikke om ett år eller mer, slik det ofte tar å utvikle interne løsninger. Å balansere interne ferdigheter og tilgjengelig kapasitet mot en stadig voksende svindeltrussel har blitt avgjørende for fremtidig vekst. Det er også verdt å merke seg at nær tre fjerdedeler (71 prosent) av respondentene oppgir at de investerer mer i svindelteknologi enn i menneskelige svindelanalytikere.

68 % er enige i at deres nåværende teknologistabel er utilstrekkelig for å møte en raskt utviklende svindeltrussel

De største utfordringene som begrenser evnen til å oppdage og forebygge svindel



Utvalg: 979 seniorbeslutningstakere innen svindelhåndtering fra EMEA og APAC
Kilde: Experian-undersøkelse gjennomført av Forrester Consulting, juli 2025

Den generative KI-svindelmaskinen fortsetter å rulle

Ser vi på faktorene som bidrar til å øke svindeltrusselen, fremstår generativ KI som den sentrale drivkraften som kobler enorme mengder data tilgjengelig på det mørke nettet med hundretusener av kontrollerte svindlere. Mørke LLM-er, som WolfGPT og WormGPT, har gjort det mulig for nær sagt hvem som helst med internettforbindelse å utvikle avanserte ferdigheter innen en rekke svindelmetoder.

Som følge av den raske forbedringen i kvaliteten på falske dokumenter og deepfake-bilder, oppgir 64 prosent av respondentene at deres eksisterende KYC- og identitetskontroller ikke er tilstrekkelig rustet til å avdekke dokumenter generert av generativ KI.

Når ekte kundedata kombineres med syntetiske bilder og dokumenter, blir svindelen enda vanskeligere å avdekke. Etter hvert som stadig kraftigere verktøy blir tilgjengelige for et bredere publikum til lavere kostnader, vil utfordringen bare forsterkes. **Faktisk er 60 prosent enige i at vi så langt kun har sett toppen av isfjellet når det gjelder KI-drevet svindel.**

AI

66 % **av svindelekspertene er enige i at Gen KI utgjør den største utfordringen noensinne for svindelforebygging**

Et tydelig eksempel på denne raske utviklingen er at deepfakes nå kan simulere hjerteslag. Inntil nylig var dette signalet, subtile variasjoner i hudtoner som følger hjerteslag, en pålitelig metode for å avsløre deepfakes. Nyere og mer avanserte deepfakes er imidlertid i stand til å gjenskape også dette signalet, noe som gjør dem enda vanskeligere å oppdage.

Det er liten tvil om at fremveksten av generativ KI representerer et tydelig vendepunkt innen svindelforebygging. Grensen mellom det som er ekte og det som er falskt har blitt stadig mer utvisket, og konsekvensene er fortsatt usikre.

Seks av ti respondenter (60 prosent) oppgir at svindeltapene deres har økt betydelig som følge av generativ KI. Samtidig erkjenner en tilsvarende andel (58 prosent) at de har utfordringer med å avgjøre om generativ KI har vært involvert i et angrep, noe som gjør det vanskelig å kvantifisere de faktiske konsekvensene.

Bør deepfakes være ulovlige?

61 prosent av respondentene våre mener at deepfakes i alle former bør gjøres ulovlige av hensyn til samfunnets beste. Samtidig strever lovgivere verden over med å utforme regelverk for deepfakes, og dagens juridiske vakuum gjør at trusselen i stor grad forblir ukontrollert.

Danmark er blant få land som har reagert relativt raskt på denne utfordringen, blant annet ved nylig å foreslå endringer i opphavsrettslovgivningen for å sikre individers rett til egen kropp, ansiktstrekk og stemme.

Italia har også tatt viktige grep ved å fastslå at produksjon og distribusjon av skadelige deepfakes er straffbart under landets nye nasjonale KI-lov. Denne lovgivningen, som er den første av sitt slag i EU, innfører fengselsstraff for personer som ulovlig produserer eller deler KI-generert eller manipulert innhold, inkludert deepfakes. Straffenivået skjerpes ytterligere dersom teknologien benyttes til å begå alvorlige lovbrudd som svindel eller identitetstyveri.

Dette representerer et steg i riktig retning. Inntil mer omfattende rettspraksis er på plass, kan imidlertid hvem som helst lage en deepfake på få sekunder. Spørsmålet gjenstår derfor: Bør stemme- og videodeepfakes gjøres ulovlige?

Prioriteringer for det kommende året

Med den økende kompleksiteten i svindeltrusselbildet er det naturlig at den høyeste prioriteten for det kommende året er en strategisk gjennomgang av eksisterende svindelløsninger (70 prosent). Systemer som har fungert i flere tiår, blir raskt foreldet, og virksomheter ser derfor etter muligheter til å inkludere flere og mer avanserte svindelsignaler i sine vurderinger.

Denne revurderingen henger tett sammen med de neste prioriteringene: migrering av svindelløsninger til skyen (68%) og investering i nye svindelverktøy (68%).

Ser vi tre til fem år frem i tid, er det svært sannsynlig at påvirkningen fra generativ KI på svindel vil øke ytterligere. Det er derfor avgjørende å ta strategiske beslutninger om hvilke svindelkapabiliteter det bør investeres i, for å redusere risikoen for ytterligere tap.

Fremtidsrettede virksomheter vil bygge disse kapabilitetene på en samlet, skybasert plattform, fremfor å forsøke å sette sammen ulike lokale punktløsninger. I siste instans vil evnen til å kombinere arbeidsflyter for svindelforebygging og kredittrisiko gi de mest effektive resultatene. Hele 69 prosent av respondentene planlegger å integrere svindelforebygging og kredittvurdering i en helhetlig risikostyringsstrategi i nær fremtid.

Å redusere etterforskningskostnader er også en høyt prioritert målsetting. Selv om dette kan oppnås på flere måter, vil økt automatisering spille en sentral rolle. Mange svindelteam er i dag avhengige av manuelle gjennomganger for å håndtere trusler, og mer enn én av tre (35%) oppgir at det tar én uke eller mer å fullføre en slik gjennomgang. Med tilgang til riktige svindelsignaler kan en langt større andel av beslutningene automatiseres. Dette bidrar til lavere etterforskningskostnader og gir svindeleksperter bedre mulighet til å fokusere på komplekse saker og løse dem raskere.

Den siste prioriteten som fremkommer i undersøkelsen, er investering i et orkestreringslag for svindelverktøy (67%). Den samme andelen av respondentene mener at orkestrering av flere svindelløsninger på én felles plattform representerer fremtiden for svindelforebygging. Begrunnelsen er tydelig: Orkestrering forbedrer kundeopplevelsen og reduserer kostnader ved at svindelkontroller kun gjennomføres når det er nødvendig, basert på kundens risikoprofil.

Topp 5 svindelprioriteringer for det kommende året

Utvalg: 979 seniorbeslutningstakere innen svindelhåndtering fra EMEA og APAC
Kilde: Experian-undersøkelse gjennomført av Forrester Consulting, juli 2025

DEL TO: Teknologidrevne løsninger

Hvorfor maskinlære er avgjørende for å bekjempe svindel

Jo mer data som benyttes i en vurdering, for eksempel enhets- og atferdsdata, desto mer presise blir resultatene.

For å kunne hente verdi fra disse enorme datamengdene er maskinlæring (ML) avgjørende. Årsaken er enkel: Bare ML har den analytiske kapasiteten som kreves for å utlede innsikt fra store og komplekse datasett. Dette bekreftes i vår undersøkelse, der **67% av respondentene som benytter ML, rapporterer en målbar forbedring i nøyaktigheten av svindeldeteksjonen etter implementering.**

En annen sentral fordel med ML er muligheten til kontinuerlig å trene modellene på nytt med oppdaterte data, slik at de holder tritt med endrede svindeltaktikker. Regelbaserte systemer har begrenset evne til å tilpasse seg nye svindeltyper, ettersom nye regler ofte øker kompleksiteten og fører til flere falske positive og økt behov for manuelle gjennomganger. Over to tredjedeler (67%) av ML-brukerne er enige i at evnen til løpende trening og oppdatering av ML-modeller har gjort dem bedre rustet til å håndtere et raskt utviklende trusselbilde. Den samme andelen oppgir også at andelen falske positive har blitt redusert etter innføring av ML.

ML

70 %

er enige i at ML har forbedret deres evne til å oppdage svindel som et regelbasert system ville ha oversett

Hvordan påvirker ML de bedriftene som har tatt det i bruk?

67 %

Andelen falske positive har gått ned siden vi implementerte ML.

68 %

ML har gjort det mulig å redusere sikkerhetsbarrierer for gode kunder ved å bruke passive svindelsjekker.

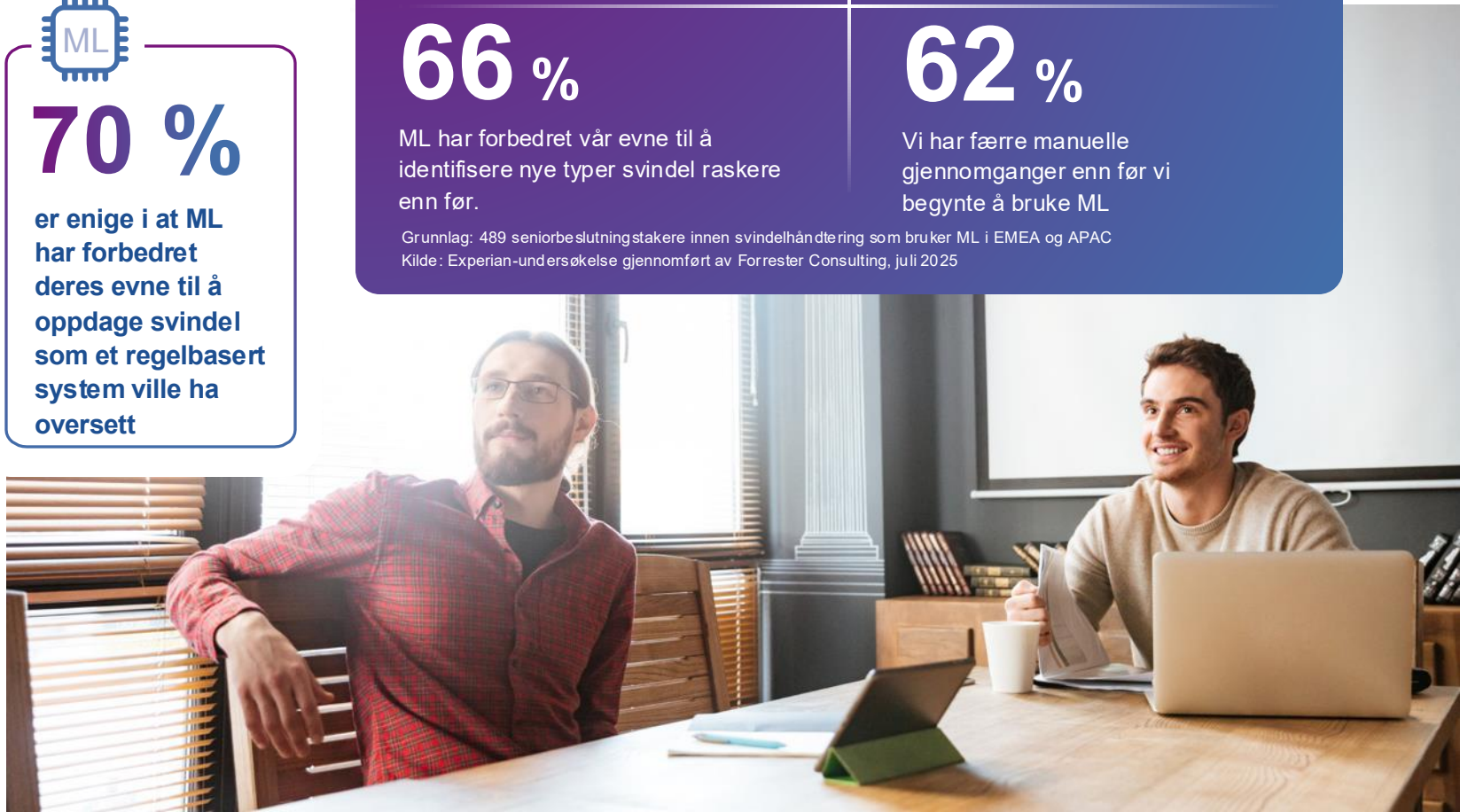
66 %

ML har forbedret vår evne til å identifisere nye typer svindel raskere enn før.

62 %

Vi har færre manuelle gjennomganger enn før vi begynte å bruke ML

Grunnlag: 489 seniorbeslutningstakere innen svindelhåndtering som bruker ML i EMEA og APAC
Kilde: Experian-undersøkelse gjennomført av Forrester Consulting, juli 2025

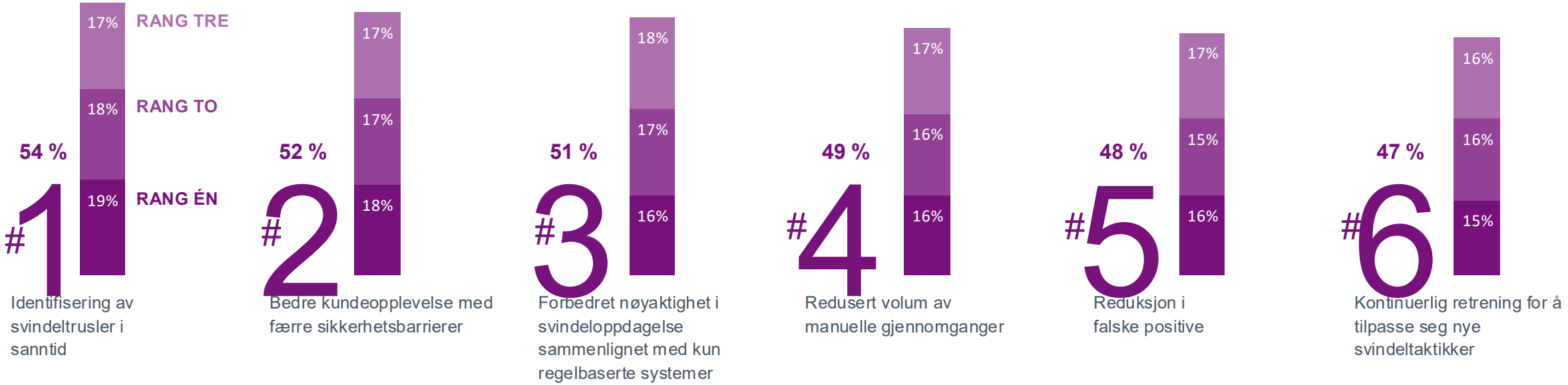


Hva er de største fordelene med ML?

Vår undersøkelse viser at den viktigste fordelen ved å ta i bruk ML er evnen til å oppdage svindeltrusler i sanntid (54%). I dag er det kun én tredjedel av virksomhetene (33%) som kan avdekke svindel i sanntid, mens et tilsvarende antall (32%) gjør det innen én dag eller mindre. Samtidig bruker 35% én uke eller mer på å identifisere svindel.

Tett knyttet til raskere identifisering er forbedret kundeopplevelse (52%), som rangeres som den nest største gevinsten. Kundeopplevelse handler imidlertid ikke bare om hurtigere beslutninger, men også om å redusere friksjon i kundereisen. Passive svindelkontroller som ikke forstyrrer kundereisen, er derfor like viktige.

Å oppdage svindel i sanntid er den viktigste fordelen med ML



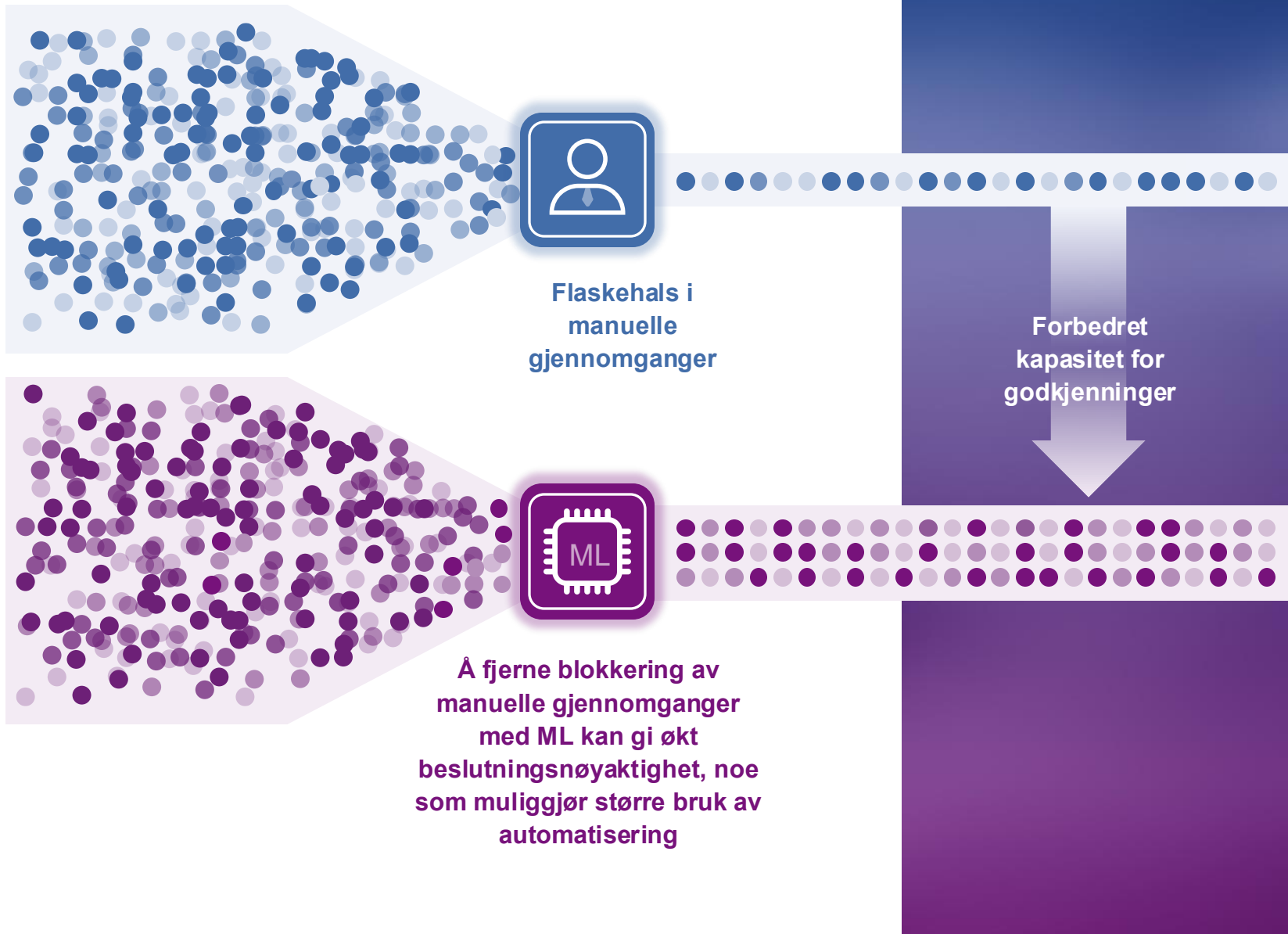
Grunnlag: 489 seniorbeslutningstakere innen svindelhåndtering som bruker ML i EMEA og APAC
Kilde: Experian-undersøkelse gjennomført av Forrester Consulting, juli 2025

ML kan redusere flaskehalser i manuelle gjennomganger betydelig

Nesten to tredjedeler av virksomhetene (64%) er avhengige av manuelle gjennomganger for å håndtere svindelvarsler. Denne andelen øker til 70% blant aktører innen netthandel. Resultatet av disse flaskehalsene er at potensielt gode kunder ofte opplever en treg og frustrerende søknads- eller kjøpsprosess, noe som øker risikoen for frafall.

Maskinlæring gir mer presise anbefalinger og muliggjør dermed økt automatisering. Nesten tre fjerdedeler (71%) av virksomhetene som benytter ML, oppgir at teknologien gjør det enklere å prioritere hvilke saker som krever manuell gjennomgang. Dette har bidratt til økt produktivitet blant svindelanalytikerne.

Månedlige søknader/kjøp med og uten ML



Hvorfor tas ikke maskinlæring i bruk i større grad?

En sammenligning av vår nyeste forskning på maskinlæring innen kredittrisiko med funnene fra denne svindelundersøkelsen er avslørende. Innen kredittrisiko er det fortsatt enkelte beslutningstakere som ikke fullt ut forstår verdien av ML, og som derfor heller ikke har investert i teknologien.

For svindelbeslutningstakere er bildet annerledes. Her er den viktigste årsaken til manglende fremdrift mangel på kvalitetsdata til å trene modellene. Hele 73% er enige i at dette er en begrensende faktor, noe som indikerer at mange allerede anerkjenner verdien ML kan tilføre.

Betydningen av tilstrekkelige treningsdata av høy kvalitet kan vanskelig overdrives. Effektiv svindelforebygging forutsetter tilgang til omfattende og mangfoldige datakilder, og med fremveksten av ML har data blitt en enda mer kritisk ressurs.

For at ML-modeller skal kunne levere presise prediksjoner, må treningsdatasettene være store og korrekt merkede. Ferdig forhåndstrente modeller kan bidra til å redusere denne barrieren, i tillegg til bruk av syntetiske data for å supplere og styrke eksisterende treningsgrunnlag.

Regulatoriske bekymringer knyttet til maskinlæring

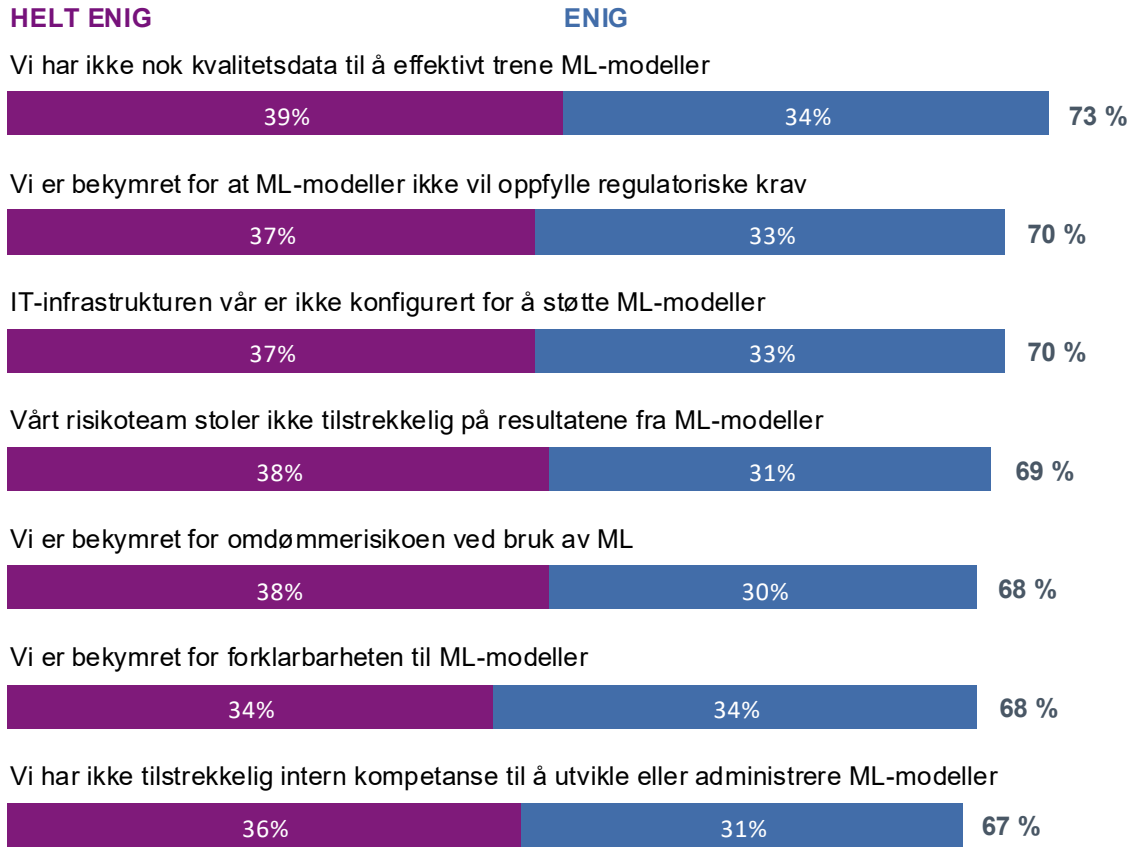
Lovgivere verden over befinner seg på ulike stadier i arbeidet med å regulere bruken av maskinlæring i svindeldeteksjon, med mål om å sikre både åpenhet og rettferdighet. Forklarbar maskinlæring gjør det mulig for kunder som får avslag å forstå og eventuelt bestride beslutninger, mens full revisjonsevne bidrar til å bygge tillit til ML-baserte beslutninger blant forretningsbrukere.

ML-modeller kan være fullt forklarbare, med tydelige begrunnelser for hver enkelt beslutning. Likevel råder det fortsatt usikkerhet rundt hva regulatorer forventer, og hvordan virksomheter best kan etterleve disse kravene. Hele 71% av respondentene oppgir at de ville hatt nytte av større regulatorisk klarhet rundt bruken av ML i svindelforebyggende systemer.

Over to tredjedeler (67%) er enige i at manglende regulatorisk tydelighet rundt hvilke ML-bruksområder som er akseptable innen svindelforebygging, i dag utgjør en barriere for implementering av teknologien.

- Intern kapasitet
- Reguleringer
- Intern kapasitet
- Sikkerhet
- Omdømme
- Reguleringer
- Intern kapasitet

De viktigste årsakene til at ML ikke har blitt tatt i bruk



Grunnlag: 490 seniorbeslutningstakere innen svindelhåndtering som bruker ML i EMEA og APAC
Kilde: Experian-undersøkelse gjennomført av Forrester Consulting, juli 2025

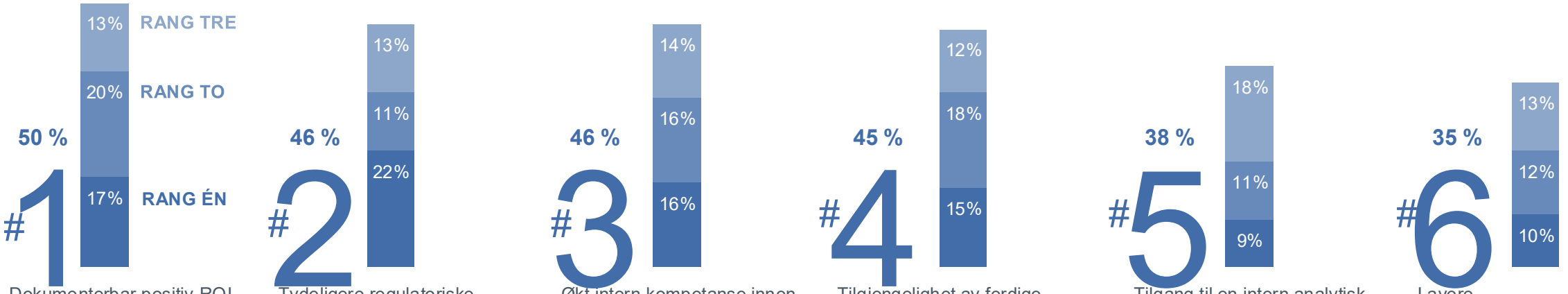
Hvilke faktorer vil motivere til implementering av maskinlæring blant ikke-brukere?

Dokumentert avkastning på investering (ROI) fra bransjekolleger er den viktigste faktoren som kan motivere virksomheter til å ta i bruk maskinlæring. Som ved innføring av ny teknologi generelt, ønsker mange virksomheter å være «først ute med å være nummer to» – slik at de kan lære av erfaringene til dem som har gått foran. Selv om dette ofte oppleves som en tryggere tilnærming til systemendringer, krever dagens alvorlige svindeltrussel en mer proaktiv holdning til å ta i bruk avansert teknologi for svindelforebygging.

Mange virksomheter har allerede implementert ML med gode resultater og dokumentert lønnsomhet. For én Experian-kunde som nylig gikk over til en ML-basert modell, ble positiv ROI oppnådd på under én måned, etter at modellen raskt avdekket et omfattende svindelsyndikatangrep kort tid etter implementering.

Virksomheter som ønsker å forstå verdien av ML nærmere, kan gjennomføre en offline Proof-of-Value (PoV)-vurdering. Dette gjør det mulig å evaluere fordelene ML kan gi basert på avtalte måleparametere, uten at eksisterende systemer må kobles direkte til modellen.

Dokumenterbar ROI og tydeligere regulatoriske retningslinjer vil stimulere til ML-implementering



Grunnlag: 490 seniorbeslutningstakere innen svindelhåndtering som bruker ML i EMEA og APAC
Kilde: Experian-undersøkelse gjennomført av Forrester Consulting, juli 2025

Generative KI-assistenter og digitale identitetslommebøker

En spennende utvikling innen svindelkontroll er bruken av generative KI-assistenter integrert i plattformer for svindelforebygging. Disse verktøyene kan samle og strukturere sentrale datapunkter, som regelsett og deres ytelse, svindelårsaker samt varighet på treff og matcher (dato og tidspunkt).

KI-assistentene kan også gi en helhetlig risikovurdering av en sak, med tilhørende begrunnelser og konkrete anbefalinger for neste steg i etterforskningen. I tillegg bidrar de til å strømlinjeforme manuelle prosesser og forbedrer både effektiviteten og presisjonen i beslutningstakingen.

Vår forskning viser at 80 prosent av respondentene mener at den største fordelen med generative KI-assistenter er at de gjør svindelforebyggingsprosesser mer tilgjengelige for ansatte med begrenset teknisk kompetanse eller uten kodeerfaring.

Hva kan en Gen KI svindelassistent gjøre for din bedrift?

77 %
Mener at den største fordelen med en Gen KI-assistent er å redusere tiden som kreves for å håndtere svindelsaker.

72 %
Er enige i at en Gen KI-assistent som er grundig trent på svindeldata, kan hjelpe dem med å gjøre mer presise svindelvurderinger.

71 %
Mener at en Gen KI-drevet assistent kan redusere tiden og innsatsen som kreves for å håndtere nye svindelsaker betydelig.

66 %
Er enige i at deres organisasjon er interessert i å integrere denne typen teknologi i sine svindelforebyggingsarbeidsflyter.

Utvalg: 979 seniorbeslutningstakere innen svindelhåndtering fra EMEA og APAC
Kilde: Experian-undersøkelse gjennomført av Forrester Consulting, juli 2025

Fremtiden for digitale identiteter

EU har nylig skissert sin plan for at digitale identitetslommebøker skal anerkjennes i hele unionen og internasjonalt, i henhold til IDAS 2.0. I løpet av de neste to årene må alle medlemsland tilby digitale identitetslommebøker, og finansielle tjenester samt teleselskaper må akseptere dem.

Digitale ID-initiativ rulles også ut i Singapore, Malaysia, Australia og mange andre land. India er i front med sitt Aadhaar-program, beskrevet som et av de mest sofistikerte digitale ID-systemene globalt, med over én milliard registrerte brukere.

Nesten tre fjerdedeler av våre respondenter (74 %) ser på digitale identitetslommebøker som en strategisk mulighet for å styrke svindelforebygging. Et lignende antall (73 %) planlegger aktivt å integrere digitale identitetslommebøker i kundereisen.

Digitale ID-er har potensialet til å redusere identitetsrelatert svindel betydelig, men statlige og forretningsmessige opplæringsprogrammer er avgjørende for å bygge tillit til dem og oppmuntre til adopsjon. Potensialet er betydelig, som vist ved at 70 % av respondentene er enige i at introduksjonen av digitale identitetslommebøker vil endre hvordan de onboarder og autentiserer kundene sine.

74 %

er enige i at utbredt bruk av digitale identitetslommebøker kan redusere avhengigheten av tradisjonell KYC (kjenn din kunde) og dokumentverifisering

Det økende behovet for delt svindelinformasjon

Kollektiv svindelintelligens vil uten tvil spille en sentral rolle i fremtidens svindelforebygging. **Hele 73% av respondentene er enige i at samarbeid er den mest effektive måten å motvirke den økende svindeltrusselen på.**

Samtidig forutsetter effektiv informasjonsdeling tilrettelegging fra en pålitelig tredjepart. Tre fjerdedeler av respondentene (75%) mener at det å bygge tillit mellom deltakerne i et svindelnettverk er avgjørende for nettverkets suksess. Velfungerende nettverk krever et sentralt koordinerings- og styringspunkt, med sikre API-tilkoblinger til hvert enkelt medlem.
Dette gjør det mulig å dele sensitiv informasjon på en trygg måte, samtidig som gjeldende regelverk for datadeling etterleves. På denne måten kan hver applikasjon kryssjekkes mot en felles pool av kollektiv intelligens, uten at medlemmene deler data direkte med hverandre.

74 %

er enige i at de neste tre årene vil de fleste bedrifter være en del av en delt svindeldata-gruppe.

For mer informasjon om hvordan nettverk fungerer og prosessen for å bli med i et, kan du lese Experians guide for nettverkskjøpere:

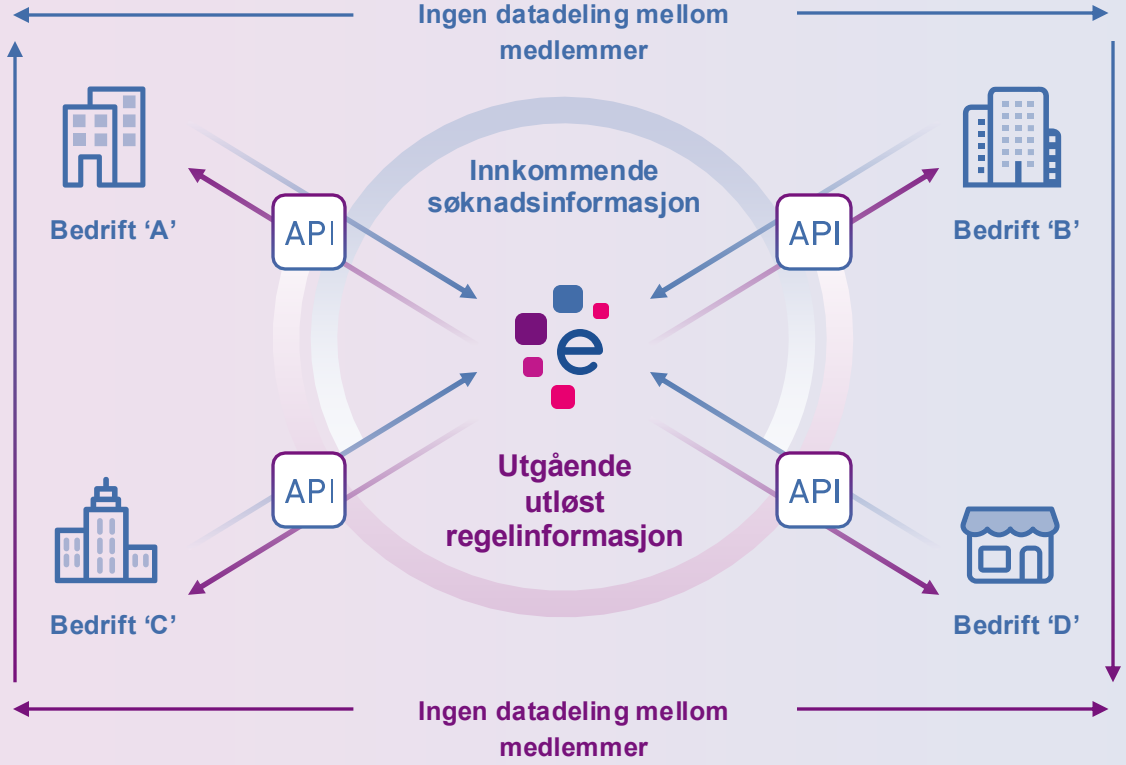
KRAFTEN I DELT INTELLIGENS

Dataoverføringsprosess i et nettverk

1 Hver bedrift sender søknads-/kjøpsdata til den sentrale databasen via et individuelt sikkert API

2 Hvis søknadsdataene utløser en varsling i det sentrale senteret, blir regelen som ble utløst returnert til bedriften

3 Ingen data deles direkte mellom bedriftsmedlemmene



Viktige lærdommer

Generativ KI og deepfakes har for alltid endret svindeltrusselbildet. Etter hvert som disse verktøyene blir stadig mer sofistikerte, har det blitt avgjørende å ta i bruk flere lag med svindelsignaler, som enhets- og atferdsdata for å forhindre en rask økning i svindeltap.

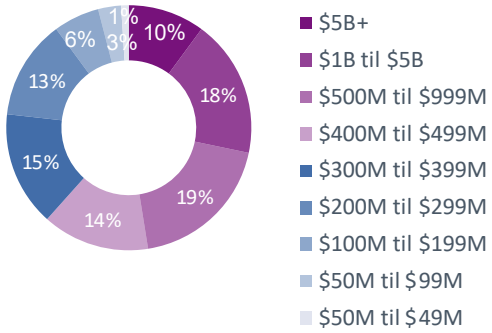
En strategisk gjennomgang av dagens svindelverktøy for å identifisere kapasitetsmangler er den høyeste prioriteten for året som kommer. Dette etterfølges av migrering av svindelløsninger til skyen og investeringer i nye, ML-drevne svindelverktøy.

Den største fordelen med maskinlæring er evnen til å oppdage svindel i sanntid. Dette etterfølges av en forbedret kundeopplevelse, der redusert friksjon i onboarding- og kjøpsreiser muliggjøres gjennom bruk av passive svindelsignaler.

Delt svindelintelligens gjennom nettverk vil spille en avgjørende rolle i fremtidens svindelforebygging. For at dette samarbeidet skal lykkes, må det imidlertid tilrettelegges av en pålitelig tredjepart som sikrer både regulatorisk etterlevelse og tillit mellom deltakerne.

Firmografikk og demografi for respondenter

BEDRIFTENS INNTEKTER



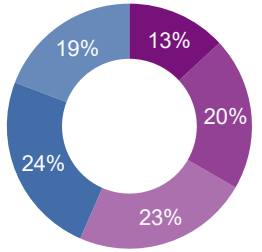
GEOGRAFI

N=~109 hvert land

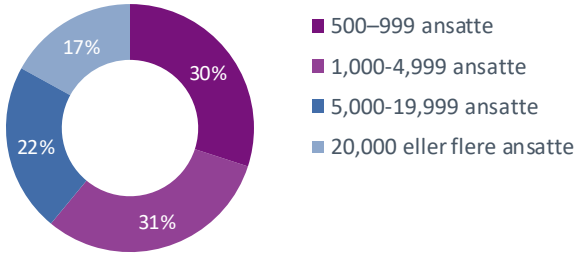
Danmark, Spania, Italia, Tyskland, Sør-Afrika, Norge

New Zealand, Australia, India

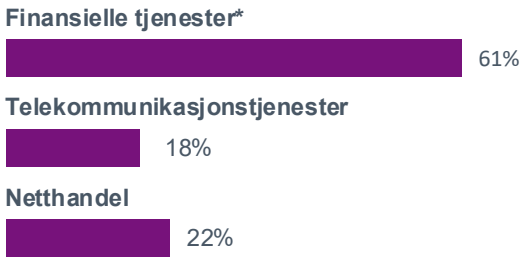
RESPONDENTNIVÅ



BEDRIFTENS STØRRELSE



BRANSJE



*Bank (38 %), kommersiell finansiering/leasing (21 %), bilfinansiering (25 %), forbrukslån (16 %)

DIREKTE ANSVAR FOR BESLUTNINGSTAKING

Ordliste

API-SVINDELANGREP
Utnyttelse av sårbarheter i API-er for å få uautorisert tilgang til data, tjenestenektangrep eller manipulering av API-en på andre ondsinnede måter.

SVINDEL MED AUTORISERT PUSH-BETALING (APP)
Svindlere manipulerer ofrene til frivillig å betale dem gjennom sosial manipulering, som å late som om de kommer fra en pålitelig finansinstitusjon.

ATFERDSBIOMETRI
Identifisering og analyse av datapunkter knyttet til den underbevisste måten en spesifikk bruker interagerer med enheten sin – uten å samle inn PII-data. Dette inkluderer musebevegelser, tastetrykk eller berøringsskjermtrykk og mange hundre andre atferdsattributter.

ATFERDSANALYSE
Identifisering av bot-angrep ved å sammenligne måten mennesker interagerer med enheter på, versus hvordan bots interagerer med enheter.

BOT-/KREDENSIALSTUFFING
Automatiserte svindelangrep hvor lister med stjålne legitimasjonsdata fra én organisasjon brukes for å prøve å få uautorisert tilgang til en konto i en annen organisasjon.

ENHETSPROFILERING/FINGERAVTRYKKING
Analyse av et sett med programvare- og maskinvareparametre knyttet til en spesifikk enhet for å gi en unik identifikator og vurdere risiko. Disse parameterne inkluderer operativsystem, nettverk, nettleser, språk, tidssone, skjermforhold og mange flere.

ENHETSINTELLIGENS
Enhetsdata kombinert med atferdsdata kalles samlet enhetsintelligens. Det gir kontinuerlige og passive svindeldeteksjonssignaler.

DEEPFAKES
Videoer, lyd eller bilder som har blitt endret og manipulert på en overbevisende måte for å feiltolke noen som å gjøre eller si noe som faktisk ikke ble gjort eller sagt. I svindelsammenheng kan de brukes til å lure Kjenn-din-kunde (KYC)-kontroller med en falsk identitet.

FRAUD-AS-A-SERVICE (FAAS)
Bedrageriverktøy og -tjenester som for det meste selges på det mørke nettet mot betaling.

PENGEKURÉR
En person som hjelper med å hvitvaske kriminelle gevinster ved å motta penger på sin konto og deretter overføre dem til en annen konto på vegne av en svindler. Disse mellomleddene blir ofte rekruttert via sosiale medier, og er kanskje uvitende om at pengeoverføring på denne måten er ulovlig.

FYSISK BIOMETRI
Unike fysiske egenskaper som kan brukes til å identifisere enkeltbrukere. For eksempel, livsdeteksjon som bruker ansiktsgjenkjenning.

SYNTETISK IDENTITET
En kombinasjon av ekte og falsk personlig identifiserbar informasjon (PII) brukes til å lage en fabrikkert identitet som er vanskelig å oppdage.

SYNTETISK BEDRIFT
Som en syntetisk forbrukeridentitet, bruker disse falske bedriftene en kombinasjon av ekte og falsk data for å lage en simulering av en legitim bedrift.

TRIANGELSVINDEL
En netthandelsvindel der en svindler oppretter en falsk nettbutikk for å samle betalinger fra intetanende kunder, for deretter å bruke stjålet kredittkortinformasjon fra en tredjepart til å kjøpe de samme varene fra en legitim forhandler og sende produktet til den opprinnelige kunden. Kunden mottar bestillingen sin, svindleren stikker av med pengene, og den legitime forhandleren blir til slutt rammet av en tilbakebetaling fra eieren av det stjålne kortet, noe som resulterer i økonomisk tap og potensiell skade på omdømme.

Om Experian

Experian er et globalt data- og teknologiselskap som skaper muligheter for mennesker og virksomheter over hele verden.

Vi hjelper med å omdefinere utlånspraksis, avdekke og forebygge svindel ved å bruke vår unike kombinasjon av data, analyser og programvare. Vi hjelper også millioner av mennesker med å realisere sine økonomiske mål og hjelper dem med å spare tid og penger.

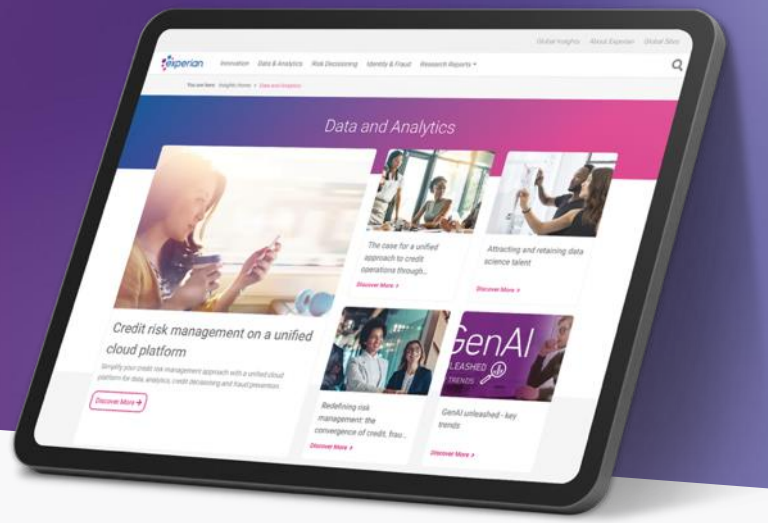
Vi opererer på tvers av flere markeder, fra finansielle tjenester til forsikring og mange andre bransjesegmenter.

Vi investerer i talentfulle mennesker og nye avanserte teknologier for å utnytte kraften i data og for å innovere. Vi er et FTSE 100-selskap notert på London Stock Exchange (EXPN) med et team på 25 100 personer fordelt på 32 land. Vårt hovedkontor ligger i Dublin, Irland.

Finn ut mer på experianplc.com

Oppdag mer →

Kontakt din lokale Experian-konsulent eller besøk experianacademy.com



Registrert kontoradresse: The Sir John Peace Building, Experian Way, NG2 Business Park, Nottingham, NG80 1ZZ Telefon: 0844 481 9920 businessuk@experian.com experian.co.uk/business