Building Trust in a World of Deception

Experian research conducted by Forrester Consulting

Velkommen til Experians svindelrapport for 2026

I løpet av de siste årene har vi sett svindeltrusselen øke betraktelig. Den har blitt mer organisert og industrialisert, med stadig kraftigere verktøy som øker omfanget av angrepene.

Hele soner har blitt svindelmegafabrikker som retter seg mot uskyldige mennesker over hele verden. Det er også en økende trussel fra statssanksjonerte kriminelle organisasjoners involvering i disse koordinerte angrepene, noe som får enkelte eksperter til å hevde at vi befinner oss midt i svindelens gyldnealder.

For å møte denne utfordringen kreves større samarbeid, ettersom våre individuelle innsatsområder er langt mer effektive når de kombineres. Organisasjoner som er en del av Experians nettverk for svindelsamarbeid, opplever ofte en betydelig reduksjon i svindeltap ved å støtte seg på den kollektive intelligensen som deles i gruppen.

Det har også blitt avgjørende at bedrifter utnytter den mest avanserte teknologien for svindelforebygging. Kunstig intelligens har blitt en avgjørende faktor i dette forsvaret, hvor både maskinlæring og generativ KI gir nye muligheter til bedre å identifisere svindlere, raskt tilpasse seg endringer og mer effektivt håndtere svindelsystemer, og dermed bidra til å beskytte både bedrifter og deres kunder.

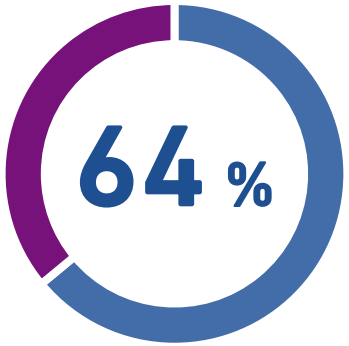
I årets undersøkelse, gjennomført i samarbeid med Forrester Consulting, spurte vi nærmere tusen beslutningstakere innen svindelhåndtering fra ni land om deres syn på de store trendene som påvirker svindelforebygging. Jeg er sikker på at deres kollektive innsikter vil hjelpe deg med å finjustere svindelstrategien din for det kommende året.

Og når du er klar til å starte en samtale om vår helhetlige plattform for svindelforebygging, ser vårt globale team av ekspertkonsulenter frem til å snakke med deg.

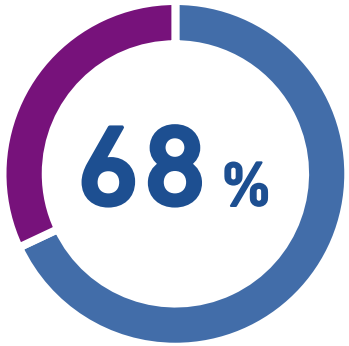
SHAIL DEEP
COO Experian EMEA & APAC

Innhold

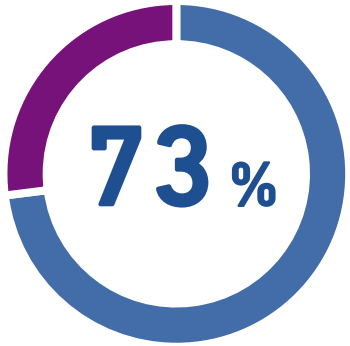
Oversikt over hovedfunn



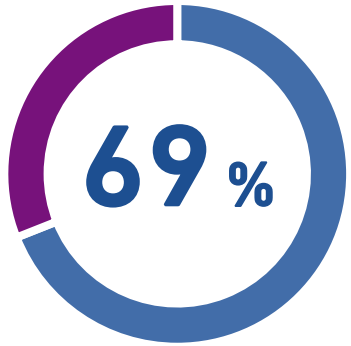
oppgir at deres svindeltap har økt fra år til år.



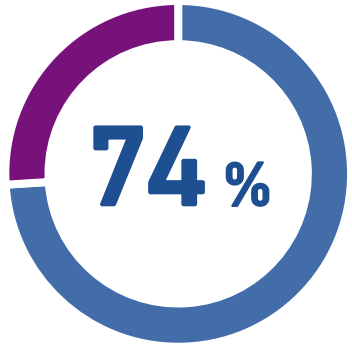
er enige i at deres nåværende teknologistabel er utilstrekkelig for å møte en raskt utviklende svindeltrussel.



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 har blitt raskere og billigere å gjennomføre enn noen gang før. Den doble trusselen fra stadig mer organiserte transnasjonale cybertrusler og Gen KI-drevne angrep har betydelig økt både volumet og kompleksiteten av angrepene.

Ifølge en nylig studie har svindelsyndikater i Sørøst-Asia blitt «det mest mektige kriminelle nettverket i moderne tid», og genererer 50–70 milliarder dollar per år med en arbeidsstyrke på over 350 000. I tillegg tilbyr darkweb-leverandører av Fraud-as-a-Service et stadig bredere spekter av produkter som gir svindlere tilgang til de nyeste verktøyene og den nyeste kriminelle innsikten.

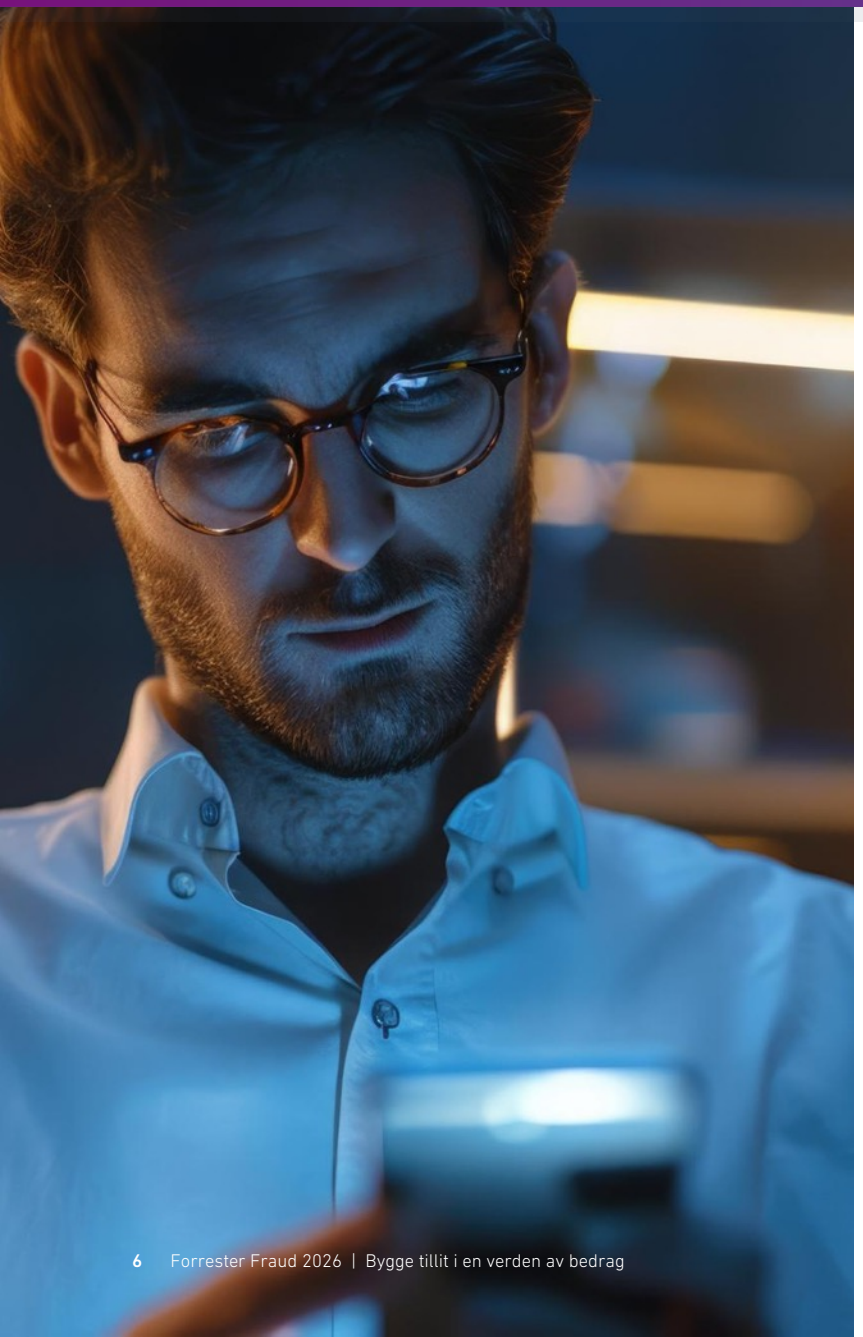
Vår forskning viser at denne trusselen påvirker bedrifter over hele verden, og at **mer enn to tredjedeler (67 %) av de spurte forventer flere svindelangrep i 2026 enn året før, en økning på 10 % fra år til år.**

Som et resultat av denne pågangen ser 64 % av bedriftene at svindeltapene deres øker sammenlignet med året før. Den samme prosentandelen innrømmer at organisasjonen deres sliter med å holde tritt med den raskt utviklende svindeltrusselen. Og virkningen av denne svindeltsunamien går utover tapene, noe som vises av de 67 % som er enige i at svindelsaker skader organisasjonens omdømme.

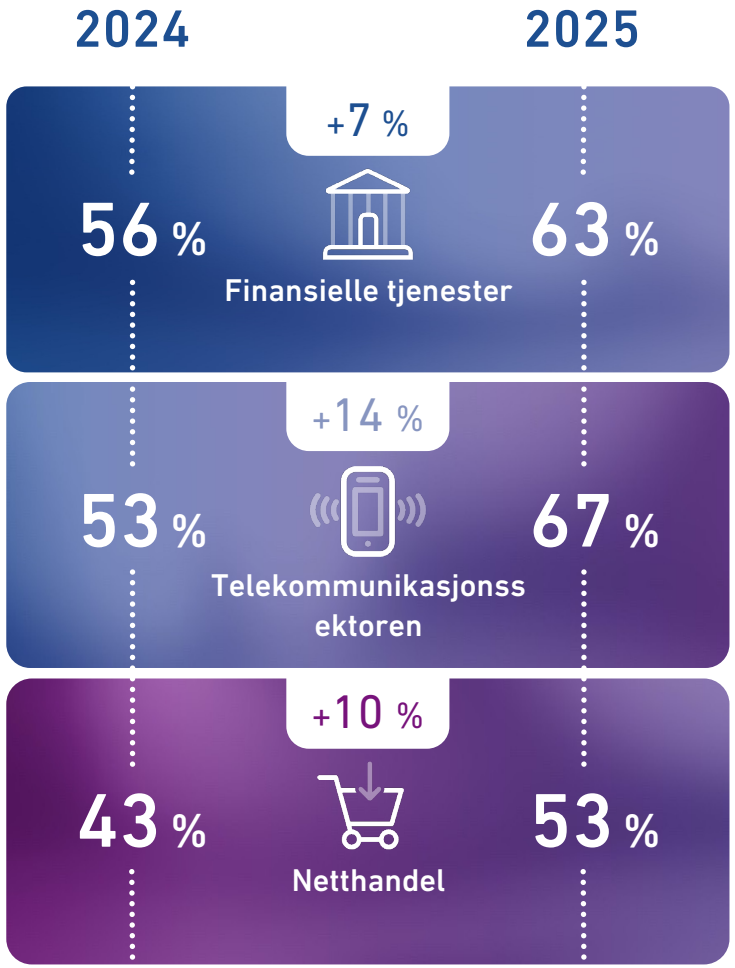
Hvilke typer svindel har økt mest?

Når vi ser på de tre bransjene vi undersøkte, har telekommunikasjonssektoren opplevd den største økningen i samlede svindelangrep, hvor mer enn to tredjedeler (67 %) rapporterer en økning. Deretter følger finanssektoren tett på (63 %), og litt over halvparten (53 %) av netthandelsaktørene.

67 % **forventer flere svindelangrep enn i fjor**



Prosentandel 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-/belønningssvindel og identitetstyveri de raskest voksende truslene for finanssektoren og telekommunikasjonssektoren. Det er ikke overraskende at sosial manipulering øker, gitt hvor kraftig et fasiliteringsverktøy Gen KI har blitt. Forskningen antyder også at svindlere i økende grad retter seg mot lojalitetsprogrammer og belønninger, kanskje på grunn av oppfatningen om at insentivordninger generelt er mindre sikre.

Identitetsverifisering har blitt den viktigste sikkerhetsperimeteren og hovedmålet for svindlere.
Etter hvert som legitime KI-agenter i økende grad samhandler med nettsteder sammen med bots og deepfakes, blir evnen til å nøyaktig autentisere og verifisere kundens identitet avgjørende.

For netthandel har 'friendly fraud' og misbruk av refusjoner vist den største år-for-år-økningen. Svindelangrep med syntetisk identitet har også økt, men ikke i samme grad.

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 %**

	BETYDELIG ØKNING/MODERAT ØKNING	LITEN ØKNING/NOE ØKNING	
Svindel mot tyveri av identitet	25%	39%	64%
Svindel mot lojalitets- og belønningsprogrammer	25%	39%	64%
Sosial manipulering	25%	37%	62%
Svindel mot overtakelse av konto	25%	35%	60%
Syntetiske bedrageriangrep mot virksomheter	28%	32%	60%

Telekommunikasjonssektoren

Økning i samlede svindelangrep: **67 %**

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

	BETYDELIG ØKNING/MODERAT ØKNING	LITEN ØKNING/NOE ØKNING	
Pengekurervirksomhet	26%	36%	62%
Svindel mot lojalitets- og belønningsprogrammer	22%	39%	61%
Svindelangrep via API-er	27%	33%	60%
Syntetiske identitetssvindelangrep mot forbrukere	18%	42%	60%
Syntetiske bedrageriangrep mot virksomheter	21%	38%	59%

Netthandel

Økning i samlede svindelangrep: **53 %**

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

	BETYDELIG ØKNING/MODERAT ØKNING	LITEN ØKNING/NOE ØKNING	
Misbruk av refusjonsordninger	22%	39%	61%
Såkalt «vennlig svindel»	27%	33%	60%
Syntetisk identitetssvindel	22%	36%	58%
Kontoovertakelsesangrep	18%	34%	52%
Trianguleringssvindel	17%	32%	49%

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?

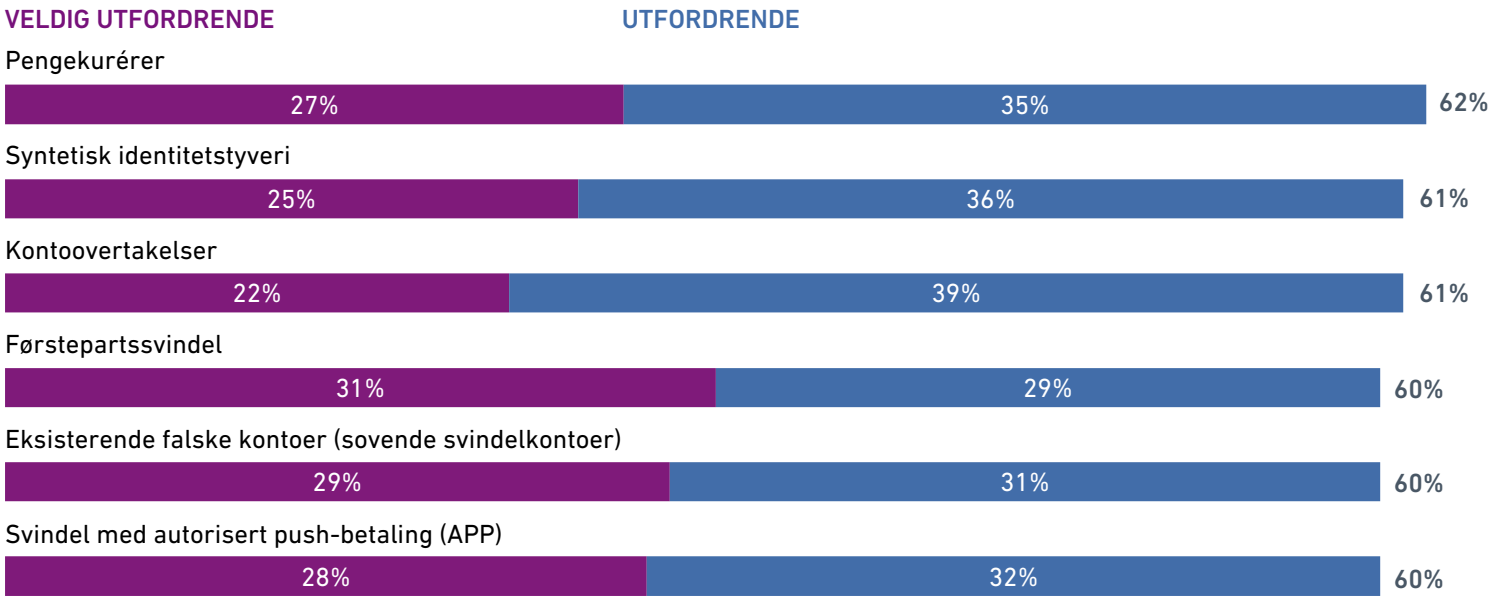
Vår forskning viser at pengekurérer er den vanskeligste typen svindel å motvirke, etterfulgt av syntetisk identitetstyveri og kontoovertakelse. Det er her ytterligere svindelsignaler har en avgjørende rolle å spille, da de tillater kontinuerlig og passiv overvåking av brukerdata for å identifisere mønstre som kan indikere disse typene svindler.

Tradisjonelle autentiseringsmetoder kan nå enkelt omgås gjennom sosial manipulering drevet av Gen KI og data fra det mørke nettet. Svindeltyper som er vanskelige å identifisere, kan bare forhindres gjennom subtile enhets- og atferdssignaler som viser når normal brukeratferd har avviket.

Med tanke på hvor få respondenter som bruker avanserte autentiseringsverktøy, med bare 42 % som for øyeblikket bruker enhetsdata og 39 % som bruker atferdsbiometri, er det forståelig hvorfor disse typene svindel fortsatt er utfordrende å forhindre.

Uten disse verktøyene vil mange virksomheter oppleve at svindeltapene øker etter hvert som svindlere får tilgang til systemene deres med kompromittert legitimasjon. Dark web-overvåking har også blitt avgjørende for å holde oversikt over hvilke data som er tilgjengelige og gjeldende svindeltaktikk.

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

De største utfordringene innen svindel

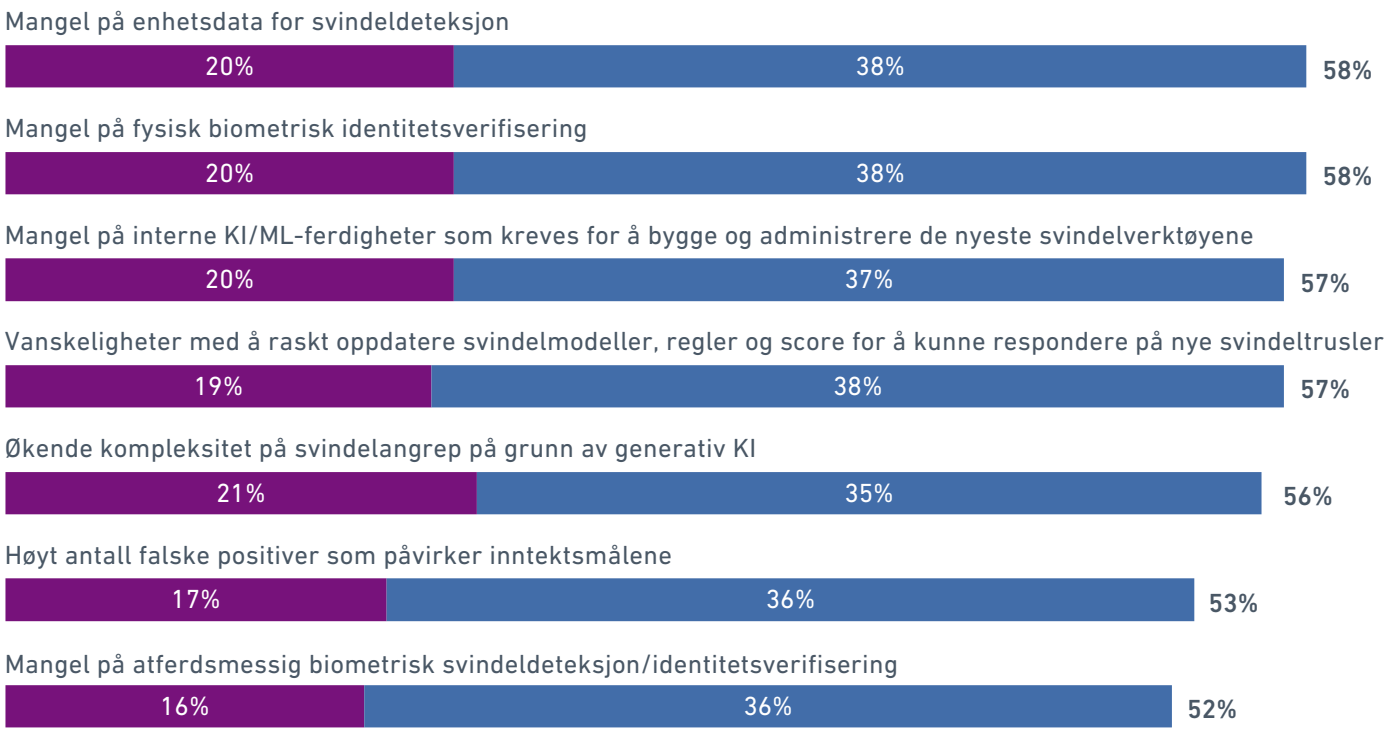
De tre største problemene som begrenser organisasjonenes evne til å oppdage og forhindre svindel, er alle basert på manglende evne. Enhetsdata og fysisk biometri er identifisert som de viktigste manglende funksjonene, og tett knyttet til disse er behovet for KI/ML-ekspertise for å forvandle disse signalene til nøyaktige, pålitelige svindelbeslutninger.

Vår forskning tyder på at mange virksomheter er fanget i et kapasitetsgap, ettersom deres nåværende svindelsystemer har blitt utilstrekkelige til å kontrollere svindel, men de har ikke kapasitet til å introdusere de avanserte verktøyene de trenger. Dette spørsmålet om «bygge versus kjøpe» er selvsagt ikke nytt, men den raske utviklingen i kompleksiteten av svindelangrep har økt presset.

Virksomheter trenger løsninger nå – ikke om et år eller mer, slik det tar å utvikle en løsning internt. Å balansere interne ferdigheter og kapasitet mot en økende svindeltrussel har blitt avgjørende for fremtidig vekst. Det er interessant å merke seg at nær tre fjerdedeler (71 %) 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

Gen KI-svindelmaskinen ruller videre

Hvis vi ser på faktorene som øker svindeltrusselen, er Gen KI drivkraften som knytter de enorme mengdene data tilgjengelig på det mørke nettet til hundretusener av kontrollerte svindlere. Mørke LLM-er, som WolfGPT og WormGPT, har gjort det mulig for hvem som helst med internettforbindelse å bli dyktig i en rekke svindelangrep.

Som følge av denne raske utviklingen i kvaliteten på falske dokumenter og deepfake-bilder, oppgir 64 % av respondentene at deres eksisterende KYC- og identitetskontroller ikke er rustet til å oppdage dokumenter generert av Gen KI.

Når ekte kundedata kombineres med syntetiske bilder og dokumenter, blir det enda vanskeligere å identifisere. Ettersom stadig kraftigere verktøy blir tilgjengelige for publikum til lavere kostnader, vil problemet bare forverres. **Faktisk er 60 % enige i at vi kun har sett toppen av isfjellet når det gjelder AI-drevet svindel.**

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

Et eksempel på denne raske utviklingen er at deepfakes nå har hjerteslag. Frem til nylig var dette signalet – hudtoner som varierer med hjerteslag – en pålitelig metode for å oppdage en deepfake. Imidlertid kan nye avanserte deepfakes gjenskape dette signalet, noe som gjør dem enda vanskeligere å oppdage.

Det råder ingen tvil om at fremveksten av Gen KI representerer et vendepunkt innen svindelforebygging. Grensen mellom hva som er ekte og hva som er falskt har blitt utvisket, og konsekvensene er usikre. 60 % var enige i at deres tap som følge av svindel har økt betydelig siden Gen KI. En lignende andel (58 %) innrømmer imidlertid at de har problemer med å identifisere om Gen KI har vært involvert i et angrep, og at de derfor har vanskeligheter med å kvantifisere konsekvensene.

Bør deepfakes være ulovlig?

61 % av respondentene våre er enige i at deepfakes av alle slag bør gjøres ulovlige til samfunnets beste. Lovgivere over hele verden kjemper for å utarbeide regler for deepfakes, men det nåværende vakuumet i lovverket gjør at trusselen nesten er helt ukontrollert.

Danmark er ett av de få landene som har respondert på dette problemet med en viss hast, ved nylig å foreslå endringer i opphavsrettsloven for å sikre at alle har rett til egen kropp, ansiktstrekk og stemme.

Italia har også tatt avgjørende grep ved å offisielt erklære at produksjon og distribusjon av skadelige deepfakes er en straffbar handling under deres nye nasjonale lov om KI. Denne lovgivningen, den første av sitt slag i EU, innfører fengselsstraff for personer som ulovlig produserer eller deler KI-generert eller manipulert innhold, inkludert deepfakes. Straffene blir enda strengere dersom teknologien brukes til å begå forbrytelser som svindel eller identitetstyveri.

Dette er et steg i riktig retning, men inntil ytterligere rettspraksis foreligger, kan hvem som helst lage en deepfake på få sekunder. Så – bør stemme- og videodeepfakes være ulovlige?

Prioriteringer for det kommende året

Med tanke på den økende kompleksiteten i svindeltrusler, er det fornuftig at den høyeste prioriteten for det kommende året er å strategisk gjennomgå eksisterende svindelløsninger (70 %). Systemer som har fungert i flere tiår, blir raskt foreldet, og bedriftene ser etter muligheter til å inkludere flere svindelsignaler i sine vurderinger.

Denne revurderingen av svindelløsninger henger tett sammen med den andre og tredje prioriteten – **å migrere svindelløsninger til skyen (68 %) og å investere i nye svindelverktøy (68 %).**

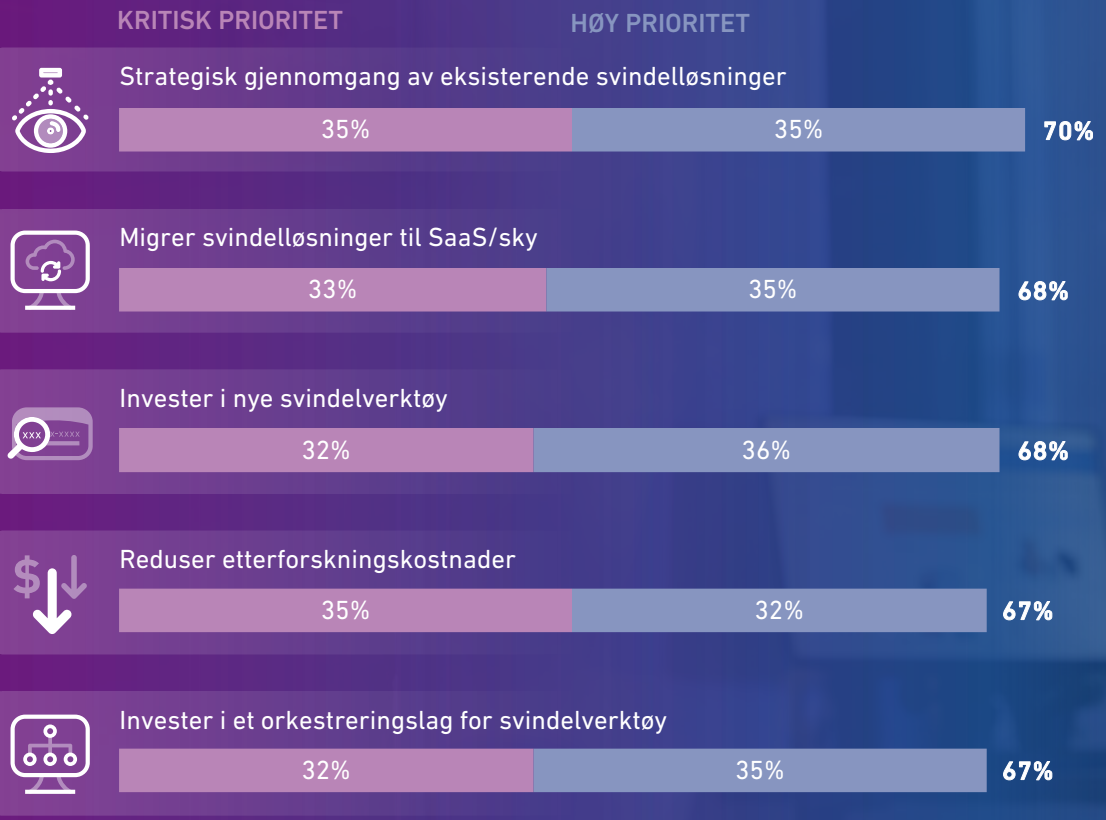
Ser vi fremover de neste 3–5 årene, er det svært sannsynlig at påvirkningen fra Gen KI på svindel vil tilta. Derfor er det avgjørende å foreta strategiske valg av hvilke svindelkapabiliteter det skal investeres i, for å unngå ytterligere tap.

Fremtidsrettede virksomheter vil bygge disse kapabilitetene på en samlet, skybasert plattform, fremfor å forsøke å sette sammen ulike lokale punktløsninger. Til syvende og sist vil evnen til å kombinere arbeidsflyter for svindelforebygging og kredittrisiko gi de mest kraftfulle resultatene. 69 % av respondentene våre planlegger å integrere svindelforebygging og kredittvurdering i en helhetlig risikostyringsstrategi i nær fremtid.

Å redusere etterforskningskostnader er også en høy prioritet. Selv om det finnes flere måter å oppnå dette på, kan økt automatisering spille en betydelig rolle. Mange svindelteam er i dag avhengige av manuelle gjennomganger for å håndtere svindeltrusler, og mer enn en tredel (35 %) oppgir at det tar dem én uke eller mer å gjennomføre en manuell gjennomgang. Med de riktige svindelsignalene kan en langt større andel av beslutningene automatiseres, noe som reduserer etterforskningskostnadene og gjør det mulig for svindelekspertene å løse komplekse saker raskere.

Den siste prioriteten som er identifisert i undersøkelsen, er å investere I et orkestreringslag for svindelverktøy (67 %). Den samme andelen av respondentene er enige i at orkestrering av flere svindelløsninger på én plattform er fremtiden for svindelforebygging. Årsakene til dette er klare, ettersom orkestrering forbedrer kundeopplevelsen og reduserer kostnader ved kun å gjennomføre svindelsjekker etter behov, basert på kundens risikoscore.

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 brukes for å gjøre en vurdering, for eksempel enhets- og atferdsdata, desto mer presise blir resultatene.

For å få mening ut av dette enorme datavolumet kreves ML. Hvorfor – fordi bare ML har den analytiske muskelen som trengs for å trekke ut innsikt fra slike store datasett. Vår undersøkelse tydeliggjør dette, **med 67 % av brukerne av (ML som har sett en målbar forbedring i nøyaktigheten av svindeldeteksjonen etter implementering av ML.**

Den andre viktige fordelen med ML er muligheten til jevnlig å trene modellene på nytt med nye data for å holde seg oppdatert på endrede svindeltaktikker. Systemer som kun baserer seg på regler, sliter med å tilpasse seg nye typer svindel, ettersom nye regler øker kompleksiteten og fører til flere falske positive og manuelle gjennomganger. Mer enn to tredeler (67 %) av ML-brukerne er enige i at denne evnen til kontinuerlig å trene og oppdatere ML-modellene har hjulpet dem med å holde tritt med en raskt utviklende svindeltrussel. Den samme andelen har sett at andelen falske positive har gått ned etter implementering 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.

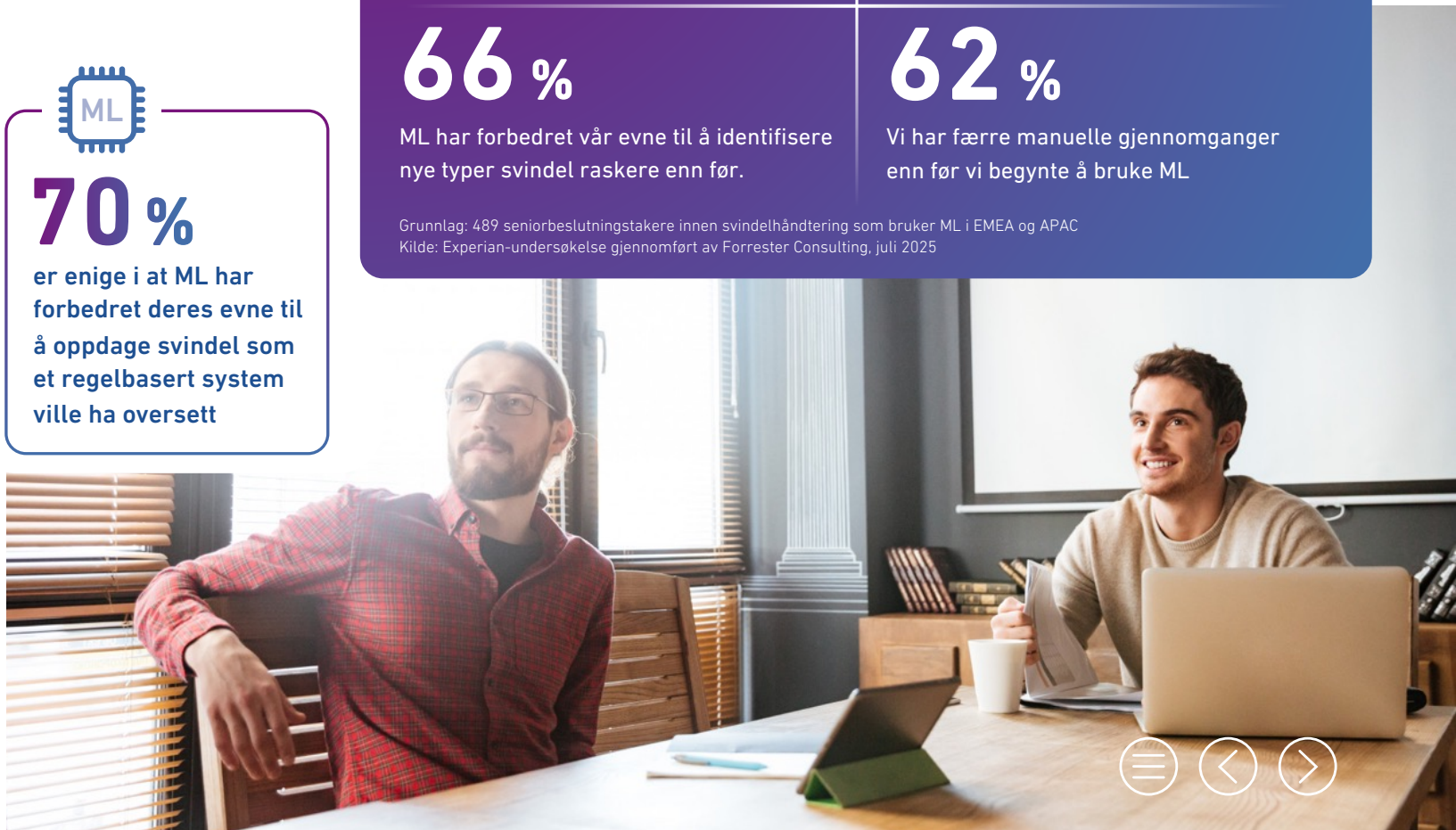
66 %

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

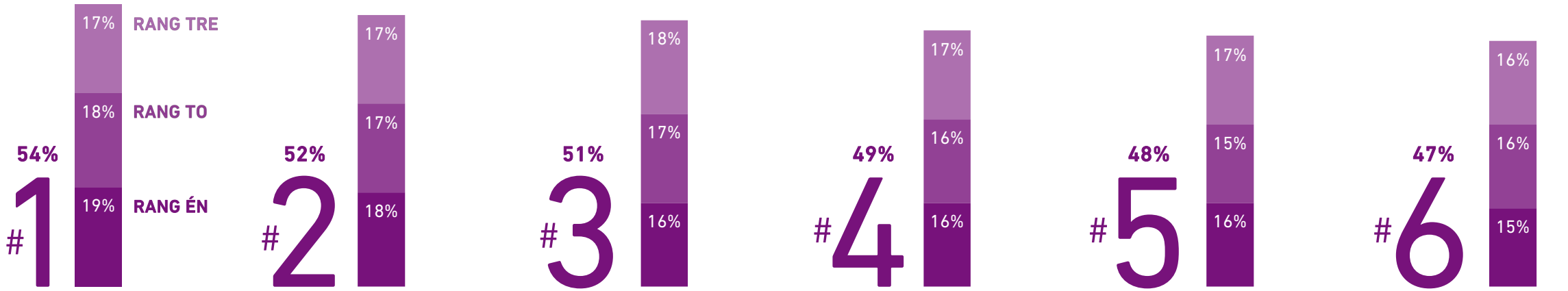


Hva er de største fordelene som ML gir?

Vår undersøkelse viser at den største fordelen ved å implementere ML er evnen til å oppdage svindeltrusler i sanntid (54 %). Kun en tredjedel (33 %) av organisasjonene kan i dag oppdage svindel i sanntid, mens et tilsvarende antall (32 %) gjør det på en dag eller mindre, og 35 % bruker én uke eller mer.

Tett knyttet til raskere identifisering er bedre kundeopplevelse (52 %), som rangeres som den nest største fordelen. Kundeopplevelse handler ikke bare om raskere beslutninger; det er også kritisk å redusere friksjon. Passive svindelsjekker som ikke forstyrrer kundereisen, er like viktige.

Å oppdage svindel i sanntid er den viktigste fordelen med ML



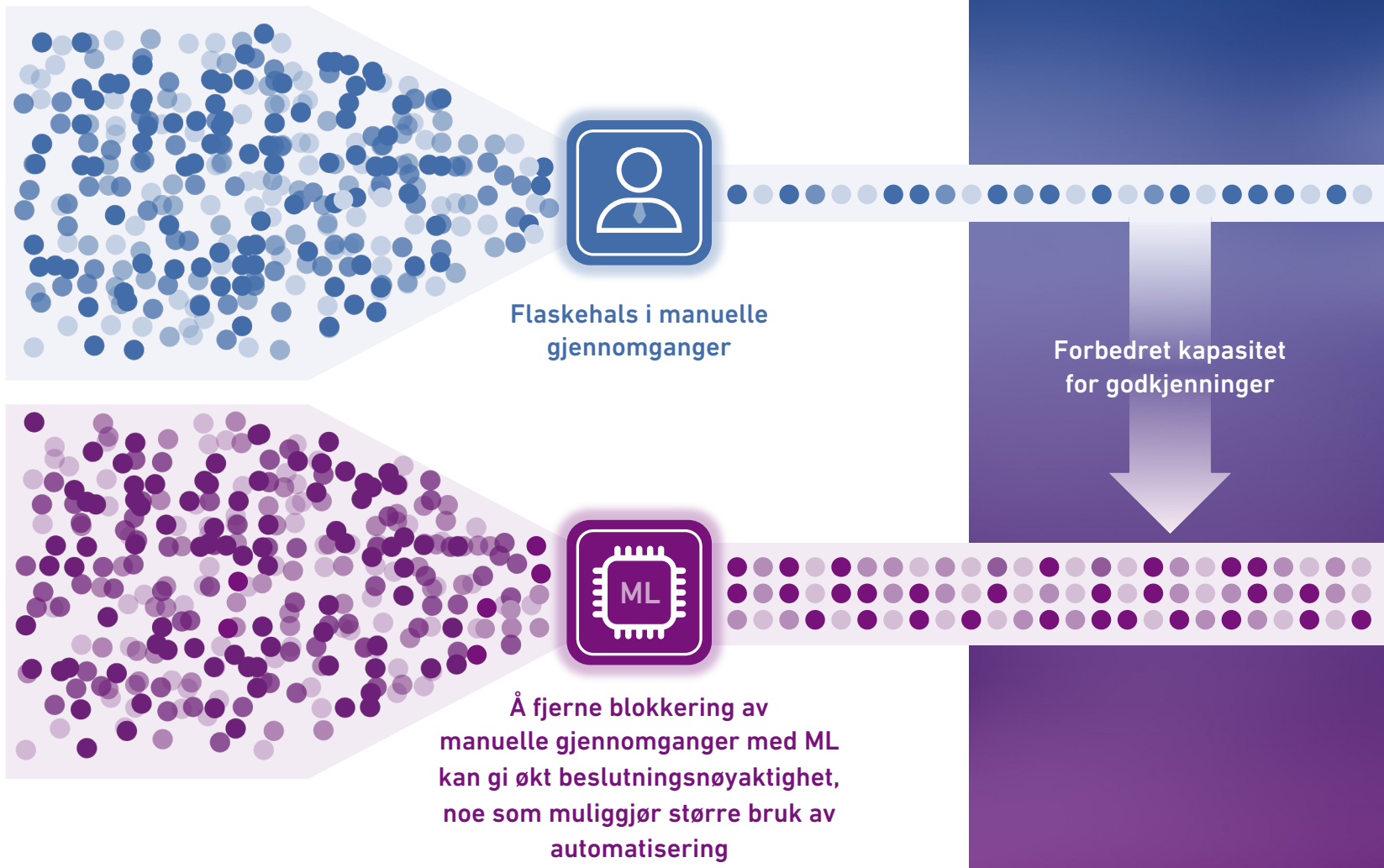
Grunnlag: 489 seniorbeslutningstakere innen svindelhåndtering som bruker ML i EMEA og APAC
Kilde: Experian-undersøkelse gjennomført av Forrester Consulting, juli 2025

ML kan redusere flaskehalser i manuelle gjennomganger betydelig

Nesten to tredjedeler (64 %) av organisasjonene er avhengige av manuelle gjennomganger for å håndtere svindelvarsler, og dette tallet stiger til 70 % for eCommerce-respondenter. Konsekvensen av denne flaskehalsen er at potensielt gode kunder opplever en langsom og frustrerende søknads- eller kjøpsreise, med høy sannsynlighet for at mange vil forlate den.

ML gir mer nøyaktige anbefalinger, noe som muliggjør mer automatisering. Nesten tre fjerdedeler (71 %) av de som bruker ML, er enige om at det lar dem prioritere manuelle gjennomgangssaker bedre, noe som har forbedret produktiviteten til svindelanalytikerne deres.

Monatliche Anträge/Einkäufe mit und ohne ML



Hvorfor blir ikke ML tatt i bruk?

En sammenligning av vår nyeste ML-forskning på kredittrisiko med denne svindelforskningen er avslørende; noen beslutningstakere innen kredittrisiko forstår ikke verdien av ML, og har derfor ikke investert i det.

I sammenligning er den største grunnen til at svindelbeslutningstakere står stille, mangel på kvalitetsdata for å trene modeller (73 % er enige) – dette antyder at mange allerede anerkjenner verdien det kan gi.

Viktigheten av å ha tilstrekkelig, høy kvalitet på treningsdata kan ikke overdrives. Nøyaktig svindelforebygging er avhengig av å ha tilstrekkelig data fra ulike kilder, og med fremveksten av ML har verdien av data blitt enda viktigere.

Treningsdatasett må være store og korrekt merkede for at ML skal kunne gi nøyaktige prediksjoner. Forhåndstrente modeller som kan kjøpes ferdig kan bidra til å overvinne denne utfordringen, det samme kan bruken av syntetiske data for å supplere treningsdatasett.

Forskriftsmessige bekymringer om ML

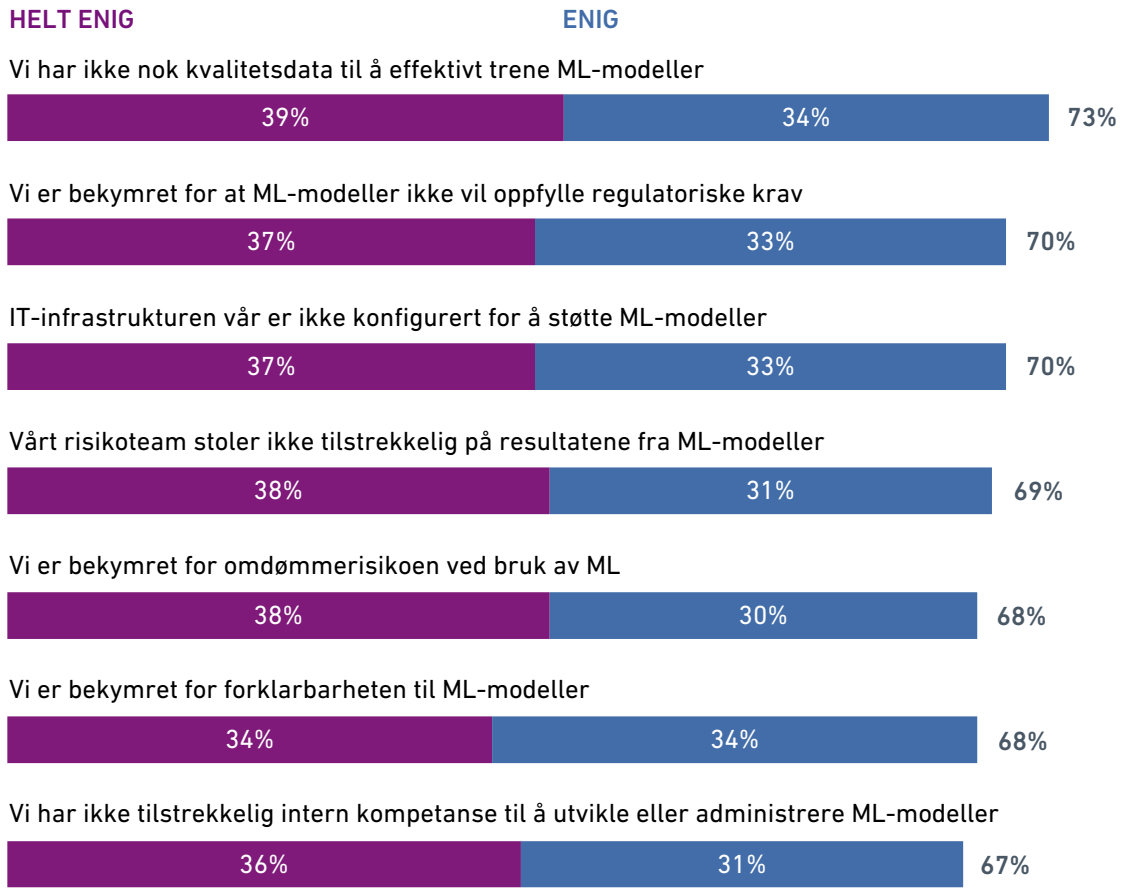
Lovgivere over hele verden er på ulike stadier i arbeidet med å lovregulere bruken av ML for svindeldeteksjon, for å sikre åpenhet og rettferdighet. Forklarbar ML gjør det mulig for avviste kunder å bestride beslutninger, og full revisjonsevne bidrar til å bygge tillit til ML-beslutninger for forretningsbrukere.

ML-modeller kan være fullt forklarbare, med grunner oppgitt for hver beslutning, men usikkerhet om hva regulatorer ser etter og hvordan man kan oppnå dette, er fremdeles til stede. 71 % av våre respondenter ville satt pris på større regulatorisk klarhet rundt bruken av ML i svindelforebyggende systemer.

Mer enn to tredjedeler (67 %) er enige i at mangel på regulatorisk klarhet om akseptable ML svindelbruksområder hindrer implementeringen av denne 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

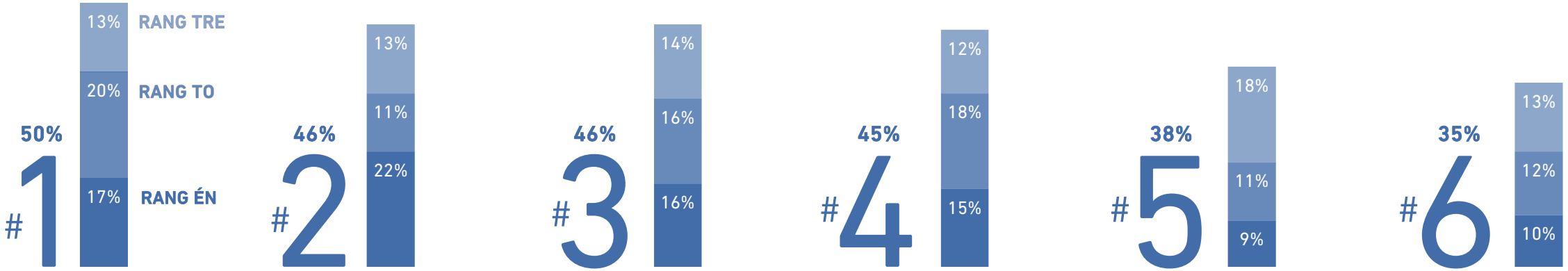
Hvilke faktorer vil oppmuntre til ML-implementering for ikke-brukere?

Dokumentert avkastning på investering (ROI) fra bransjekolleger er den største faktoren som vil oppmuntre til ML-implementering. Som med enhver ny teknologiimplementering, ønsker de fleste bedrifter å være 'først til å være nummer to', slik at de kan lære av de som har gått foran. Selv om dette er en tryggere måte å tilnærme seg systemendringer på, krever den nåværende alvorlige svindeltrusselen en mer proaktiv tilnærming til å ta i bruk den mest avanserte svindelforebyggingsteknologien.

Mange virksomheter har allerede implementert ML med gode resultater og ROI. For en Experian-klient som nylig byttet til en ML-modell, var tidsrammen for positiv ROI mindre enn en måned, ettersom modellen identifiserte et stort syndikatangrep kort tid etter at den ble tatt i bruk.

Bedrifter som er interessert i å forstå verdien av ML, kan arrangere en offline Proof-of-Value (POV)-vurdering. Dette gjør det mulig for dem å se fordelene ML kan tilby basert på avtalt måleparametere, uten å koble systemet sitt 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

Gen KI-assistenter og digitale identitetslommebøker

En spennende utvikling innen svindelkontroll er Gen KI-assistenter som er integrert i svindelforebyggende plattformer. Disse verktøyene kan samle viktige datapunkter, som regler og deres ytelse, svindelårsaker og matchens tidslengde (dato/tidspunkt).

De kan også gi et risikonivå for saken, med passende begrunnelse og 'neste steg'-instruksjoner for å fullføre en etterforskning. I tillegg kan de strømlinjeforme manuelle prosesser, og forbedre både effektivitet og nøyaktigheten i beslutningstakingen.

Vår forskning viser at 80 % av respondentene mener at den største fordelen med en Gen KI-assistent er at den gjør svindelforebyggingsprosessene mer tilgjengelige for mindre teknisk kompetente/ikke-kodende ansatte.

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 adopsjon av digitale identitetslommebøker kan redusere avhengigheten av tradisjonell KYC (kjenn din kunde) og dokumentverifisering

Den økende overgangen til delt svindelinformasjon

Kollektiv svindelintelligens vil uten tvil spille en betydelig rolle i fremtidens svindelforebygging. **73 % av respondentene er enige i at den beste måten å motvirke svindeltrusselen på, er å samarbeide og bekjempe svindel sammen.**

Imidlertid må denne informasjonsutvekslingen tilrettelegges av en pålitelig tredjepart – tre fjerdedeler (75 %) mener at å bygge tillit mellom ulike medlemmer av et svindelnettverk er nøkkelen til deres suksess.

Effektive nettverk krever et sentralt ledelsesenter, med sikre API-tilkoblinger til hvert medlem. Dette gjør det mulig å dele sensitiv data over nettverket samtidig som man overholder forskriftene om datadeling. Slik at hver applikasjon kan kryssjekkes mot den kollektive intelligens-poolen 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

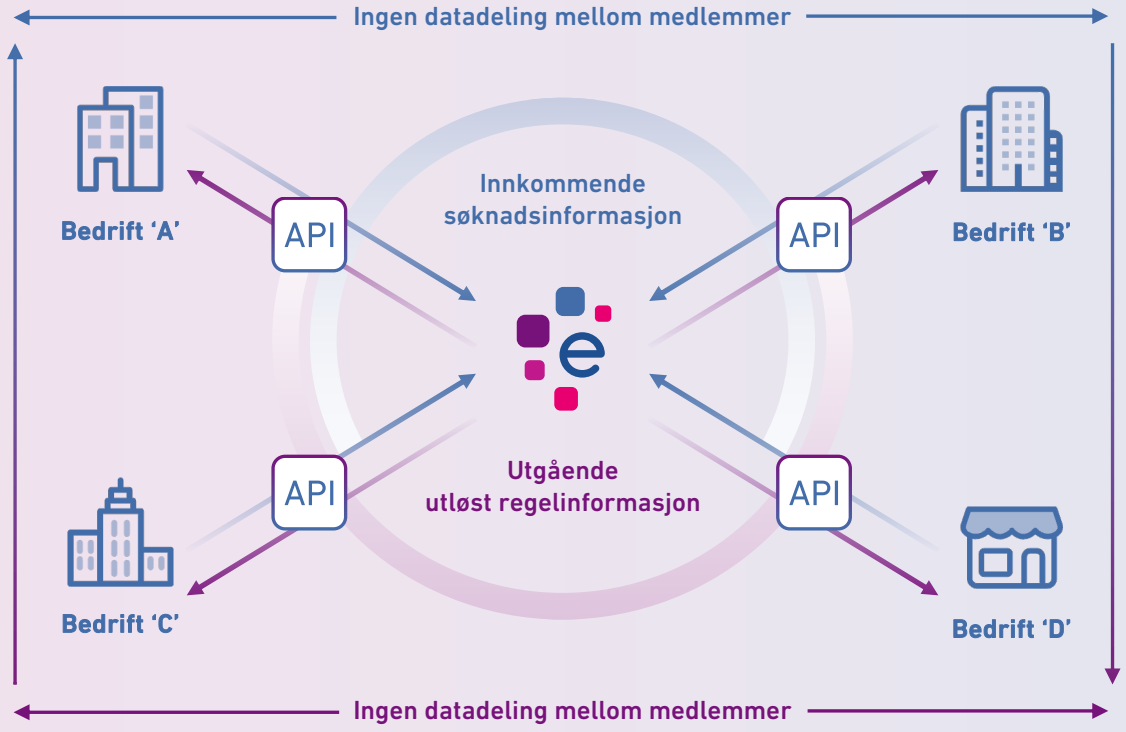
Hver bedrift sender søknads-/kjøpsdata til den sentrale databasen via et individuelt sikkert API

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

Gen KI og deepfakes har endret svindeltrusselen for alltid. Etter hvert som disse verktøyene blir mer sofistikerte, har ytterligere lag med svindelsignaler, som enhets- og atferdsdata, blitt essensielle for å hindre en rask økning i svindeltap.

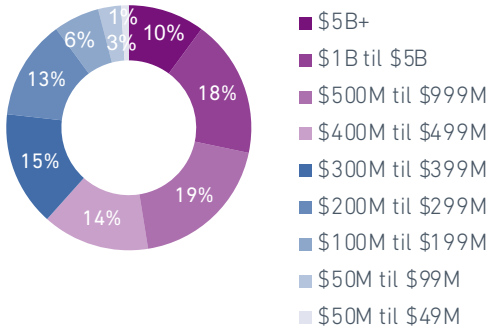
En strategisk gjennomgang av dagens svindelverktøy for å identifisere kapasitetsmangler er den høyeste prioriteten for året som kommer, etterfulgt av å migrere svindelløsninger til skyen og investere i nye ML-drevne svindelverktøy.

Den største fordelen med ML er evnen til å oppdage svindel i sanntid, etterfulgt av forbedret kundeopplevelse gjennom redusert friksjon i onboarding- og kjøpsreiser, muliggjort av passive svindelsignaler.

Delt svindelintelligens gjennom nettverk vil spille en avgjørende rolle i fremtidens svindelforebygging, men dette samarbeidet må tilrettelegges av en pålitelig tredjepart for å sikre regulatorisk samsvar og tillit mellom medlemmene.

Firmografikk og demografi for respondenter

BEDRIFTENS INNTEKTER



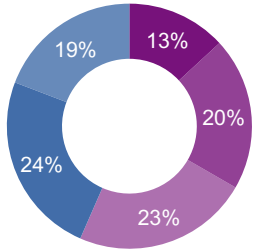
GEOGRAFI

N=~109 hvert land

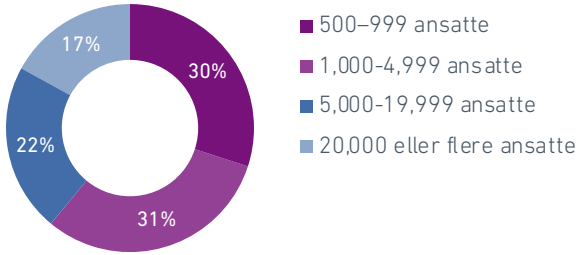
Danmark, Spania, Italia, Tyskland, Sør-Afrika, Norge

New Zealand, Australia, India

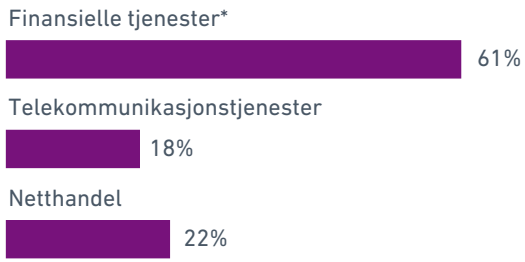
RESPONDENTNIVÅ



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, forenkle helsetjenester, levere digitale markedsføringsløsninger og skaffe dypere innsikt i bilmarkedet – alt 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.

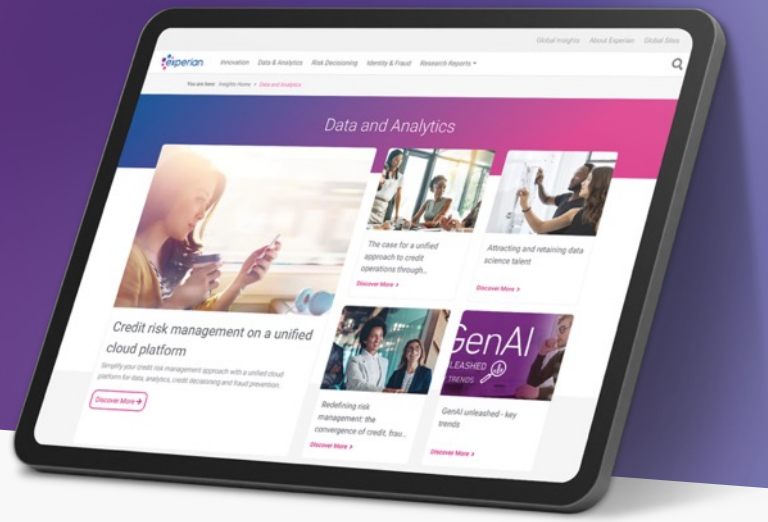
Vi opererer på tvers av flere markeder, fra finansielle tjenester til helsevesen, bilindustri, landbruksfinansiering, forsikring og mange andre bransjesegmenter.

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