Norske bankers bekjempelse av svindel

– Status og tiltak for 2026

Finans Norge

Innhold

Forord

Svindel og annen økonomisk kriminalitet er et alvorlig samfunnsproblem. Det rammer både enkeltpersoner, virksomheter og samfunnet som helhet. Bankene har de siste årene jobbet målrettet med å hindre og stoppe svindel, og innsatsen er betydelig styrket.

Finanstilsynet svindelstatistikk for første halvår 2025 viser at de økonomiske tapene knyttet til svindel for første gang er redusert sammenlignet med foregående periode (1). Samtidig rapporterer bankene fortsatt om høy aktivitet blant svindlere og en økning i antall svindelforsøk.

Bankene stopper imidlertid flere forsøk enn tidligere, og hindret at 1,5 milliarder kroner gikk til de kriminelle.

Svindelbildet endrer seg raskt. Bankene registrerer at svindlerne tilpasser seg tiltakene som blir iverksatt, hvor de tar i bruk ny teknologi og kombinerer ulike metoder for å øke sjansen for å lykkes. For eksempel er manipulerings-svindel, der ofrene selv blir lurt eller presset til å gjennomføre handlingene, et område i sterk vekst – særlig når det gjelder kjærlighetssvindel og investeringssvindel. Her kombinerer svindlerne bruker både av sosiale medier, falske nettsider og mobil som verktøy til å svindle store beløp. Bankene er tydelige på at bruken av digitale plattformer, sosiale medier og kunstig intelligens bidrar til å gjøre svindelen mer målrettet og vanskeligere å stoppe.

Bankene har de siste årene jobbet målrettet med å hindre og stoppe svindel. Bankenes innsats omfatter både forebyggende tiltak, løpende overvåkning og håndtering av svindelforsøk når de oppstår. Et viktig tiltak har vært bedre og mer treffsikker overvåkning av transaksjoner, slik at mistenkelige bevegelser kan oppdages og stoppes raskere. Et annet viktig tiltak har vært å styrke mobil- og nettbankløsninger, som gjør det vanskeligere å begå svindel.

Bankene har i tillegg styrket det felles informasjonsarbeidet gjennom kampanjen «No way – du lurer ikke meg», som gir forbrukere oppdatert informasjon om svindelmetoder og hvordan de kan beskytte seg (3).

Godt samarbeid gir ekstra effekt. Det er flere aktører som har bidratt til å stoppe svindel for svært store beløp. I november 2024 lanserte teleselskapene et felles «digitalt skjold» som blokkerer svindeltelefoner før de når norske forbrukere. Jo færre som kontaktes av svindlere, jo færre blir lurt. At flere nordmenn har tatt i bruk BankID-appen, kan også ha påvirket tallene. BankID-appen gir tydeligere informasjon om hva kunden er i ferd med å gjøre, og dermed gjør det lettere å avbryte dersom noe virker mistenkelig.

Effektiv bekjempelse av svindel forutsetter et godt samarbeid mellom banker, myndigheter og andre relevante aktører. Arbeidet med ses i sammenheng med et bredt *totalforsvar mot svindel* (2), der flere aktører bidrar med tiltak innenfor sine ansvarsområder.

> Denne rapporten gir en samlet fremstilling av bankenes vurdering av svindelbildet 2026. Vi har listet opp hvilke svindelmetoder som anses som mest aktuelle, og hvilke tiltak bankene mener det er nødvendig å prioritere fremover
>
> Gry Nergård, fagdirektør antisvindel i Finans Norge, og ansvarlig for fagutvalg antisvindel bank (FAB)

Status på svindelmetoder fra norske banker

Bankene vurderte de mest aktuelle svindelmetodene i desember 2025. Denne vurderingen gir grunnlag for hvilke tiltak som bør settes i verk for å forebygge, oppdage og følge opp svindel.

Svindelmetodene kan ramme ulike grupper, og alle aldersgrupper kan rammes av en eller flere metoder. Tapene kan variere fra små beløp til store summer, avhengig av hvilken metode svindlerne bruker. Noen svindelmetoder er svært inngripende i enkeltmenneskers privatsfære, og kan medføre store menneskelige belastninger, i tillegg til økonomiske tap.

Bankene peker spesielt på ulike former for manipuleringssvindel som den største utfordringen i 2026. Her blir ofrene lurt til å utføre svindelen selv. Eksempler er «trygg konto»-svindel, investeringssvindel og kjærlighetssvindel. En annen utvikling er at når bankene har blitt bedre til å stoppe svindel gjennom kontooverføringer, har svindel med betalingskort økt.

Bankene snakker også mer om «hybridsvindel». Det betyr at svindlerne kombinerer flere metoder mot samme offer. For eksempel kan noen som har blitt lurt én gang, være i større risiko for å bli kontaktet igjen av svindlere som later som om de vil «hjelpe» offeret.

Basert på felles erfaringer har norske banker kartlagt et bredt spekter av svindelmetoder, og samlet vurdert hvilke som vil være mest aktuelle i 2026. I denne listen finner du 17 aktuelle svindelmetoder.

Svindelmetoder

1. Phishing i alle varianter

En ofte brukt svindelmetode er phishing. Her «fisker» svindlerne etter personlige opplysninger, eller med andre ord, prøver å lure deg til å gi fra deg BankID-informasjon, passord eller kortnummer. Det skjer ofte gjennom telefon, SMS, e post, lenker på nettet eller QR koder. Opplysningene fra offeret brukes deretter av de kriminelle til å utføre svindel.

2. Svindel med hjemmebesøk

Svindlerne ringer ofte eldre og enslige, og påstår at ofret har blitt utsatt for svindel – noe som i mange tilfeller stemmer. De utgir seg for å være politi, bankansatt eller teknikere og sier at noen vil komme hjem til dem for å «hjelpe». Kort tid etter dukker en falsk politibetjent eller bankansatt opp, ofte med falsk uniform og legitimasjon. De kan:

- Tømme bankkontoer
- Ta med seg verdisaker
- Holde offeret tilbake hjemme eller et annet sted
- Bruke trusler og fysisk makt

I noen tilfeller blir offeret bedt om å legge bankkort og verdisaker i postkassa, som svindlerne deretter henter.

Bankene ser at denne typen svindel blir mer organisert, med tydelig rolle-fordeling og systematisk kontakt med sårbare ofre. Svindelen kan ligne ran og vurderes som svært alvorlig både strafferettslig og i bankenes risiko-klassifisering.

3. Gavekortsvindel

Gavekortsvindel brukes ofte som del av en annen svindel. Det starter som regel med at offeret blir kontaktet via telefon, e-post, SMS eller på sosiale medier.

Svindleren utgir seg gjerne for å være kjæreste eller en venn fra nettet (kjærlighetssvindel), en offentlig etat (politi eller Skatteetaten), teknisk support (bank eller Microsoft), en sjef i bedriften eller et familiemedlem som er i trøbbel.

Ofrene blir bedt om å kjøpe gavekort, skrape fram koden og sende bilde eller lese opp kodene. Svindleren bruker eller selger kodene videre.

4. «Trygg konto»-svindel

Stadig hyppigere blir svindelofferet oppringt av «banken» eller «politiet» og får beskjed om at de er i ferd med å bli svindlet. De blir deretter manipulert til å overføre penger til en «sikker konto», som egentlig tilhører svindleren eller en muldyrskonto.

Ofte overføres pengene først til en ny konto i offerets eget navn for å unngå at banken fanger det opp, før pengene sendes videre.

5. Investeringssvindel og kjærlighetssvindel

Dette er de mest alvorlige formene for manipuleringssvindel. I en investeringssvindel og kjærlighetssvindel tar ofrene selv kontakt med svindler, enten gjennom annonser på sosiale medier om falske investeringer med høy avkastning (ofte med falske kjendisanbefalinger) eller falske profiler på nett.

Svindelen kan vare lenge, og ofrene mister store pengebeløp. Mange tar opp lån for å «investere mer» eller for å hjelpe en «ny venn».

Ofte bruker svindlerne fjernstyringsprogrammer for å hjelpe offeret gjennom «tekniske problemer».

Bankene ser også mer bruk av kryptovaluta:

- Penger veksles raskt til krypto og flyttes mellom mange digitale lommebøker
- Falske trading-apper viser «fiktiv» avkastning
- Ofre kontaktes på nytt med tilbud om hjelp til å få tilbake tapte midler (recovery-svindel)

Dette gjør svindelen svært vanskelig å avdekke og etterforske.

6. Lånebedragerier

Svindelen er knyttet til samtykkebasert lånesøknad (SBL) gjelder boliglån, billån (pantesikret kreditt) og forbrukslån (usikret kreditt). Svindelen utnytter offentlige digitale systemer som Altinn og Skatteetatens innsynsløsninger. Svindelen kan ofte ses i sammenheng med en større svindel hos Skatteetaten, NAV eller forsikringsselskapene.

Typisk tegn i en SBL-svindel:

1. Falske lønnsmeldinger (A-meldinger) sendes inn rett før en lånesøknad
2. Meldingene slettes kort tid etter at lånet er innvilget
3. A-meldinger måneder før virksomheten er registrert i Enhetsregisteret
4. Virksomheter endrer informasjon i Brønnøysundregisteret tilbake i tid
5. Flere ansatte fra samme virksomhet søker lån samtidig
6. Lønnsopplysningene stemmer ikke med det som rapporteres til NAV eller Skatteetaten

7. BNPL-svindel («Kjøp nå, betal senere»)

Denne svindelen refererer til enhver form for svindel utført ved bruk av «Kjøp nå, betal senere»-løsninger. Svindelen kan enten angripe betalingssystemene, eller så utnytter de onboarding-prosessen hos leverandører og forhandlere.

- **Kontoovertakelse** Svindlere stjeler brukernavn og passord via phishing og bestiller varer som legitime kunder
- **Syntetisk identitetssvindel** Falske identiteter opprettes ved å kombinere ekte og falske personopplysninger
- **Ny konto-svindel** Svindlere oppretter nye kontoer med stjålne data
- **Manglende tilbakebetaling** Bestillinger gjøres uten intensjon om å betale hele beløpet
- **Refusjonsmisbruk og «venne-svindel»** Kunden ber om refusjon uten å returnere varen, eller hevder at transaksjonen er ukjent

8. Konto- og identitetssvindel via nye betalingsaktører

Flere svindlere bruker nye betalingsapper og digitale lommebøker for å få tilgang til offerets konto og betale eller overføre penger uten at offeret merker det.

Noen stjeler også telefoner, kjøper telefoner i offerets navn eller oppretter eSIM for å få full kontroll over enhet og kontoer – og gjør dem i stand til å gjennomføre flere typer svindler.

9. Kortsvindel

Dette er en svindelform som de fleste kjenner til, men svindlerne finner stadig nye måter å utføre kortsvindel på. Kortsvindel kan blant annet skje på ulike måter:

- Bruk av stjålne kort
- Misbruk av korthemmeligheter
- Relay-svindel, der svindleren fanger opp NFC-signalet fra et kort eller telefon og videresender det i sanntid til en annen svindler som gjennomfører kjøpet

10. Svindel på nett og sosiale medier

Det er en økning av falske annonser, falske profiler og falske søkeresultat på internett. Det øker risikoen for mer nettbutikksvindel, investeringssvindel, kjærlighetssvindel og phishing. I tillegg svekkes tilliten til digitale løsninger.

11. Rekruttering av muldyr

Bankene ser en økende og mer systematisk rekruttering av såkalte muldyr – personer som stiller konto, identitet eller betalingsløsninger til disposisjon for å flytte og skjule utbytte fra svindel. Ofte rammes unge voksne. Nettverkene blir mer profesjonelle og brukes til å flytte penger fra mange typer svindel.

Rekrutteringen skjer ofte via sosiale medier, meldingsplattformer og falske jobbannonser som «enkelt hjemmearbeid», «pakkehåndtering hjemmefra» eller økonomiske oppdrag mot provisjon.

12. Hybrid svindel

Bankene ser en tydelig økning i såkalt hybrid svindel. Her kombinerer svindlere flere metoder mot samme offer, over tid. Svindelen starter ofte med phishing eller annen sosial manipulering, etterfulgt av «trygg konto»-overføringer, låneopptak og videre flytting av midler via muldyrnettverk.

Tidligere svindelofre blir også kontaktet på nytt, for å tilby hjelp eller tilbakeføring av tapte penger. Svindelen kjennetegnes av sterkt psykisk press, høy grad av troverdighet og tidskritiske situasjoner på tvers av kanaler, noe som gjør den vanskeligere å avdekke og stoppe.

13. Innsidesvindel

Svindlere retter seg i økende grad mot ansatte i ulike virksomheter, som for eksempel bankansatte eller andre som har tilgang til betalingssystemer eller verdifulle ressurser. Det kan inkludere penger, varer, tjenester eller data. Ansatte kan bli involvert i svindel enten frivillig (de går med på det av egen vilje) eller ufrivillig (de blir lurt eller presset til å gjøre det).

14. CEO-svindel (direktørsvindel)

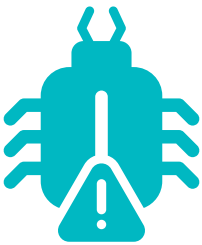
Bankene rapporterer at CEO-svindel og annen fakturarelatert svindel fortsatt gir store tap i bedriftsmarkedet. Svindelen skjer ofte gjennom falske eller manipulerte e-poster som utgir seg for å komme fra en leder, leverandør, advokat eller annen betrodd part, med mål om å endre kontonummer eller presse fram en hastebetaling. Angrepene gjennomføres ofte uten teknisk innbrudd og bygger på spoofing, sosial manipulering og utnyttelse av interne rutiner.

15. Vennesvindel

Her samarbeider venner eller bekjente for å utnytte bankenes regler om tilbakeføring ved svindel. Det kan innebære falske transaksjoner som rapporteres som uautoriserte for å få penger tilbake. På grunn av sterke forbrukerrettigheter og lav risiko for svindlerne, ser bankene en økning av denne type svindel. Det ligner også på mønstrene vi ser i forsikringssvindel.

16. Malware

Malware (forkortelse for "malicious software") er en skadelig programvare som utnytter svakheter i datasystemer for å oppnå økonomisk vinning, og kan brukes på flere måter for å svindle enkeltpersoner og virksomheter. Bankene ser at dette øker i Sverige, og forventer derfor at det blir mer vanlig i Norge også.



17. Kunstig intelligens i svindel

Svindlere bruker kunstig intelligens i stadig større grad for å gjøre svindelen mer troverdig og vanskeligere å avsløre. Med KI kan de lage falske bilder, videoer og lydopptak som virker ekte, og dermed utgi seg for personer offeret stoler på.

Dette ser vi blant annet i falske nettannonser med manipulerte kjendisklipp og i falske nettmøter, for eksempel i Teams, der svindlere bruker KI generert stemme eller deepfake video for å fremstå som ledere eller beslutningstakere. Målet er ofte å presse fram betalinger eller få tilgang til sensitiv informasjon.

Bankene vurderer denne utviklingen som en økende trussel, fordi KI gjør sosial manipulering mer overbevisende og langt vanskeligere å oppdage i tide.

Tiltak for å bekjempe svindel

Det finnes dessverre ingen enkeltløsning for å håndtere de utfordringene som er beskrevet. Svindel må bekjempes med en kombinasjon av tiltak fra flere aktører. Økokrim har lansert ideen om et totalforsvar mot svindel (2), der både næringslivet, offentlige myndigheter, lovgiver og enkeltmennesker må bidra. Bankene i Norge er klare til å gjøre sin del i dette arbeidet.

Nedenfor er det angitt flere tiltak som bankene mener bør prioriteres i 2026. Noen av tiltakene skal gjøres i bankene, mens andre tiltak innebærer samarbeid med andre aktører, eller å påvirke andre til å bidra i totalforsvaret. Noen av tiltakene er svært konkrete, mens andre er mer overordnet. Dette reflekterer at noen av dem har vært under arbeid i lengre tid, mens andre er nye og i utvikling. Tiltakene, og prioriteringene mellom dem, vil trolig også endres etter hvert som svindelmetodene utvikler seg.

Tiltakene retter seg mot ulike faser av svindelprosessen. Noen har som hovedformål å forebygge svindel, ettersom effektiv forebygging reduserer antall ofre og begrenser økonomiske tap for banker, samfunnet og enkelt-personer. Andre tiltak er utviklet for å avdekke svindel i det den pågår, slik at hendelser kan stanses raskt og skadeomfanget begrenses. I tilfeller der svindel likevel skjer, finnes det også egne tiltak for oppfølging.

Her følger en oversikt over de 16 tiltakene bankene mener det er nødvendig å jobbe med i 2026. Tiltakene er ikke rangert etter prioritet. Hvilke tiltak som til enhver tid vil få høyest prioritet, vil blant annet avhenge av utviklingen i svindelbildet. Utviklingen følges nøye av fagutvalg antisvindel bank (FAB) (5).

Bankenes tiltak mot svindel

1. Antisvindelhåndbok

I 2024 utviklet bankene i samarbeid «Bankenes antisvindelhåndbok». Dette er en verktøykasse som skal styrke hver enkelt bank i sitt arbeid mot svindel. Håndboken inneholder tiltak og metoder som bankene kan bruke basert på egne risikovurderinger. Verktøyene er delt inn i seks hovedkategorier:

1. **Varsel:** Banken gir kunden varsel om mistenkelig aktivitet i mobil- og nettbank, slik at kunden kan reagere i tide
2. **Kontekst:** Kundene får mer informasjon om hva de er i ferd med å gjøre, bekrefte eller signere, slik at de kan avsløre svindel
3. **Tidsbegrensninger:** Banken og kunden får ekstra tid til å oppdage, undersøke og stoppe forsøk på svindel
4. **Forsterket bekreftelse (step-up):** Ved høyrisikoaktivitet blir kunden bedt om ekstra bekreftelse på identitet eller hensikt
5. **Antisvindelsystem:** Banken overvåker transaksjoner for å oppdage mistenkelig aktivitet og kan innføre sperrer ved behov
6. **Periodisk kontroll:** Banken oppfordrer kontoeier til jevnlig å gjennomgå innstillinger som kan påvirke svindelrisiko

Disse verktøyene kan brukes på flere områder i banken og kombineres på forskjellige måter for å tilpasses hver situasjon.

Våren 2026 gjennomføres en undersøkelse for å vurdere hvordan bankene har tatt i bruk tiltakene i håndboken og om det bør gjøres oppdateringer i denne.

2. Transaksjonsovervåkning

Alle bankene i Norge har enten egne eller eksternt leverte systemer for transaksjonsovervåkning. Formålet med transaksjonsovervåkning er å avdekke mistenkelige/unormale transaksjoner for å kunne stoppe svindel. Et slikt system krever aktivt vedlikehold slik at det så godt som mulig fanger opp de til enhver tid aktuelle svindelmetodene.

Ny betalingsregulering fra EU stiller krav til transaksjonsovervåkning. Disse reglene kan legge nye føringer for bankenes transaksjonsovervåkning.

Finans Norge vil legge til rette for nærmere diskusjoner i næringen om EUs fremtidige krav til transaksjonsovervåkning og hvordan disse best kan implementeres.

3. Personellsikkerhet

I 2024 utarbeidet Finans Norge en veileder om personellsikkerhet for å forebygge innsideproblematikk (6). Det er et prioritert tiltak å følge opp denne veilederen for å unngå svindel og annen økonomisk kriminalitet.

Veilederen gir en innføring i hvordan virksomheter kan arbeide helhetlig med personellsikkerhet med særlig fokus på de ulike fasene i et arbeidsforhold.

Du finner veilederen på Finans Norges **nettside**

4. Felles retningslinjer, veiledninger og maler

Både på bakgrunn av gjeldende rett og med tanke på kommende implementering av EU-regler, kan det være behov for å utvikle felles retningslinjer, veiledninger og maler for hvordan bankene kan utføre konkrete oppgaver.

Finans Norge vil legge til rette for å utvikle det bankene til enhver tid har behov for, i nært samarbeid med representanter fra bankene.

Datadeling

5. Informasjons- og datadeling

For å bygge et godt totalforsvar mot svindel er deling av informasjon og data mellom ulike aktører avgjørende. Informasjons- og dataflyten må forbedres på flere nivåer:

- Mellom bankene
- Mellom banker og politiet
- Mellom banker og offentlige myndigheter
- Mellom banker og ekomtilbydere

Flere banker har deltatt i Finanstilsynets og Datatilsynets felles regulatoriske sandkasse for å avdekke behovet for datadeling mellom banker og mellom banker og andre aktører (7). Blant annet på bakgrunn av arbeidet i disse prosjektene har Finansdepartementet foreslått endringer i finansforetaksloven som skal gjøre det mulig å dele mer data med formål å forebygge og avdekke svindel (8). Datadeling er også et aktuelt tema i den nye betalingsforordningen fra EU.

Det har også vært, og pågår fortsatt, utredninger med tanke på datadeling i og mellom de andre sektorene som er nevnt ovenfor.

Finans Norge vil fortsatt legge til rette for, og delta videre i diskusjoner om datadeling.

6. Trygg digital deling av informasjon og data

Forutsatt at det blir anledning til å dele mer data, er det også nødvendig å finne hensiktsmessige og trygge måter å dele data på. Bankene i Norge har pekt på NFCERT som sin foretrukne aktør. NFCERT har i sitt mandat fra sitt nordiske styre fått utvidet sitt ansvarsområde til å omfatte forebygging av økonomisk kriminalitet og datadeling.

DSOP har utviklet tekniske løsninger for digital deling av data mellom finansforetak og offentlige etater gjennom ulike prosjekter som strekker seg tilbake i tid. Det utredes nå om disse løsningene også kan brukes til å dele data mellom banker og det offentlige i antisvindelsammenheng.

Problemstillingene rundt datadeling diskuteres også i oppfølgingen av Stortingsmelding nr. 15 (2023–2024) Styrket innsats for forebygging og bekjempelse av økonomisk kriminalitet (9), hvor Finans Norge også deltar.

Mer generell informasjon, som ikke karakteriseres som persondata eller er sensitive data, bør også deles fortløpende for å sikre relevante tiltak mot svindel. Inn under DSOP-paraplyen har man etablert OPS ØK, som er et offentlig-privat samarbeid mellom finansnæringen og offentlige aktører for å styrke kampen mot hvitvasking, terrorfinansiering og bedrageri (10). Finans Norge bistår her med administrasjon og felles samhandlingsplattform, møteplasser og aktiviteter. Bankene utveksler informasjon i flere ulike fora. Det mest sentrale for arbeidet mot svindel er Fagutvalg antisvindel bank (FAB) i regi av Finans Norge (5).

Finans Norge vil fortsatt støtte opp om, og delta aktivt, i arbeidet for god informasjonsutveksling og trygg datadeling.

Samarbeid med og påvirkning av andre

7. Samarbeid med politiet

Et tett og godt samarbeid med politiet vil fortsatt være høyt prioritert. Dette er viktig både for å forebygge svindel og for å sikre rask og effektiv oppfølging av svindelsaker gjennom god etterforskning.

Særlig vil følgende saker bli prioritert:

- Samarbeidet med Bedragerienheten på Gjøvik om forebygging av svindel
- Å være en pådriver for at tjenesten «Digitale politianmeldelser av bedrageri» benyttes aktivt
- Følge med og etterspørre god intern håndtering fra politiet når det kommer til etterforskning og påtaleavgjørelser i svindelsaker
- Å være en pådriver for at de mest alvorlige formene for svindel prioriteres høyt av politiet. Særlig gjelder dette svindel med innslag av vold, fysisk tvang eller trusler, og svindel hvor kriminelle nettverk står bak
- Utvikling av klare og effektive rutiner for samarbeid mellom banker og politiet

8. Samarbeid med e-komsektoren

Et godt samarbeid med e-komsektoren, slik det er lagt til rette for gjennom Nasjonal ekspertgruppe mot digital svindel, vil fortsatt være høyt prioritert. En stor del av dagens svindel starter med e-post, telefonsamtaler eller SMS. Jo mer e-komaktørene kan stoppe, desto vanskeligere blir det å utføre svindel i Norge.

Særlig vil følgende saker bli prioritert:

- Innføring av flere tiltak mot spoofing fra utlandet
- Bedre kundekontroll ved opprettelse eller bytte av telefonabonnement, herunder ved opprettelse av e-sim
- Bedre tiltak mot svindel via e-post

9. Samarbeid med andre aktører i betalingsmarkedet

Bankene vil etablere kontakt med andre aktører i betalingsmarkedet og arbeide for å ansvarliggjøre dem i kampen mot svindel. Fagutvalg Antisvindel Bank (5) er bekymret for at enkelte betalingsformidlere og aktører bak digitale

betalingsløsninger og digitale lommebøker, ikke har tilstrekkelig fokus på antisvindelmekanismer. Dette gjør dem sårbare for å bli utnyttet i svindelsammenheng.

Det er usikkert i hvilken grad nytt EU-regelverk vil bidra til å løse disse utfordringene eller om de vil bidra til nye svindelutfordringer. Derfor vil bankene samarbeide om å adressere disse problemene både direkte overfor aktørene det gjelder, og gjennom dialog med forvaltningen og lovgiver.

10. Samarbeid med andre deler av næringslivet

Finans Norge er en landsforening i NHO, og i 2025 ble svindel løftet høyere på agendaen i NHOs digitaliseringsnettverk. Finans Norge understreker at også andre næringer enn finans er utsatt for svindel, og at virksomheter i ulike bransjer kan bli utnyttet som ledd i svindel som rammer både bedrifter og forbrukere.

Også Virke organiserer bransjer som det kan være aktuelt å samarbeide nærmere med. Blant annet er det ønskelig at dagligvaresektoren etablerer bedre rutiner mot gavekortsvindel.

Brukthandelsbransjen er også utsatt for svindlere som utnytter deres plattform til å svindle andre. I 2025 har Finans Norge hatt nær kontakt med Vend som forvalter Finn.no, og Vend har iverksatt flere antisvindeltiltak.

I 2026 vil Finans Norge fortsette å ha dialog med ulike deler av næringslivet for å bistå med og påvirke til bedre forebygging av svindel, også i andre bransjer.

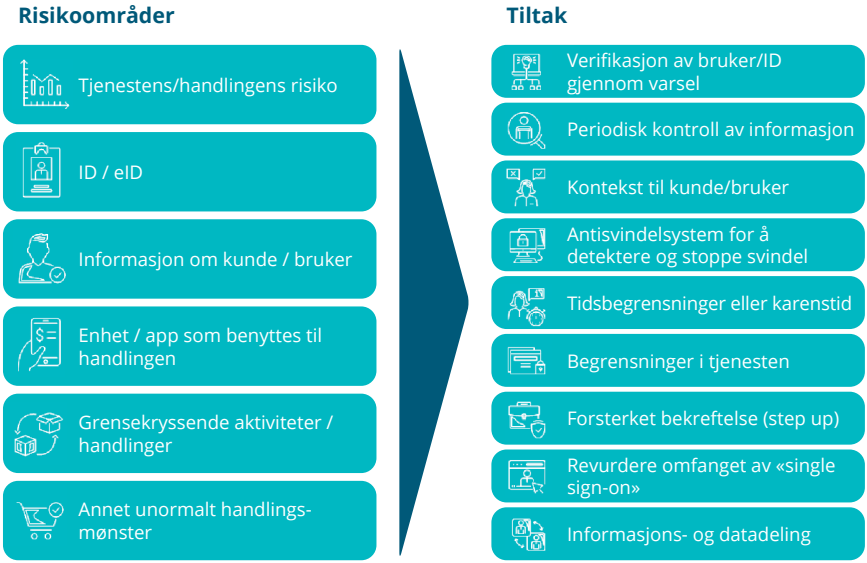
11. Samarbeid med offentlige etater

Bankene spiller en sentral rolle i å støtte andre aktører, inkludert offentlige etater, i arbeidet med å forebygge og avdekke svindel. Samtidig er bankene avhengige av at offentlige etater har effektive tiltak mot svindel, blant annet for å begrense lånebedragerier som følge av registermanipulasjon.

OPS ØK, offentlig-privat samarbeid mot økonomisk kriminalitet, samler finansnæringen og offentlige etater for å bekjempe økonomisk kriminalitet, herunder bedragerier (10). Det er en prioritert oppgave å sikre at dette samarbeidsforumet fungerer som en sterk og effektiv aktør i kampen mot svindel.

12. Antisvindelhåndbok for offentlig og privat sektor

I 2025 utarbeidet Finans Norge sammen med representanter fra bank, forsikring, NAV, Skatteetaten, Brønnøysundregistrene, Økokrim og NTAES «Antisvindelhåndbok for offentlig og privat sektor», etter mønster av bankenes antisvindelhåndbok. Finans Norge skal i 2026 ha møter med både offentlig sektor og andre deler av norsk næringsliv for å presentere håndboken, for å påvirke til bedre forebygging av svindel i ulike deler av verdikjeden.



13. Nordisk samarbeid

Svindelsituasjonen er i stor grad lik på tvers av de nordiske landene, og mange banker opererer på tvers av regionen. I 2025 ble det etablert et tettere og mer regelmessig samarbeid mellom de nordiske bankorganisasjonene. Dette styrker informasjonsutvekslingen og legger til rette for et mer effektivt samarbeid over landegrensene.

Finans Norge vil videreføre den nære kontakten med sine nordiske søster-organisasjoner.

Juridiske problemstillinger

14. EU-regelverk og implementering i norsk lov

Flere vedtatte og kommende EU-reguleringer er svært aktuelle for utviklingen av bankenes handlingsrom i antisvindelarbeidet. Det gjelder blant annet Instant Payment Regulation (IPR) fra 2024, Payment Services Regulation (PSR), hvor endelige tekst forventes før sommeren 2026, samt eIDAS 2.0, EUs reviderte regulering for elektronisk identifikasjon og elektroniske tillits-tjenester.

Det er usikkert i hvilken grad disse regelverkene vil bidra til å redusere svindel, og om det vil gjøre bankenes antisvindelarbeid lettere eller ikke. Finans Norge vil bidra til å klargjøre dette.

Generelt er det et etterslep på norsk implementering av regelverk fra EU. Dette kan være en ulempe for norske banker. Finans Norge vil være en pådriver for implementering og vil bistå i implementeringen på vegne av bankene der det er naturlig.

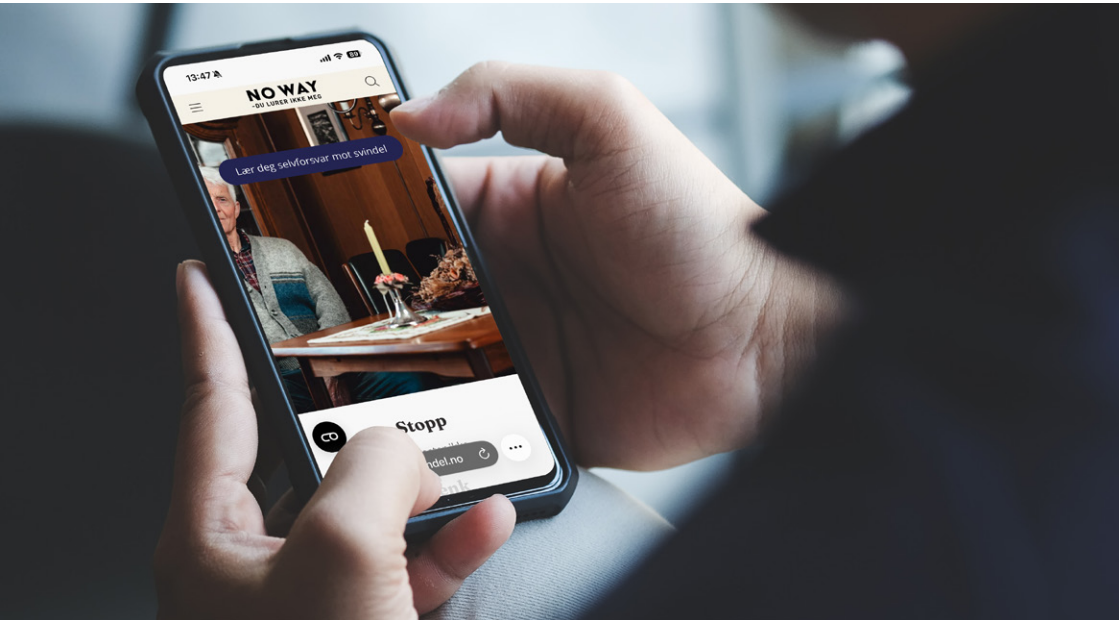
Forbrukerinformasjon

15. Felles informasjonstiltak mot svindel

I 2024 lanserte bankene en felles kampanje, «No Way – du lurer ikke meg!», for å lære forbrukere hvordan de kan beskytte seg mot svindel (3). Kampanjen inneholdt materiale som ble vist på TV, radio, sosiale medier, nettaviser og boards i bybildet. Bankene brukte også materialet i sin egen kunde-kommunikasjon.

Som en del av kampanjen ble nettsiden svindel.no lansert. Den gir nyttig og oppdatert informasjon til forbrukere om hvordan de kan unngå svindel. Innholdet i kampanjen er fremdeles relevant og bør brukes aktivt av bankene i 2026.

Flere ulike informasjonstiltak vurderes fortløpende, herunder muligheten for å kjøre en ny felles runde av «No way – du lurer ikke meg!» i regi av Finans Norge i 2026. Finans Norge drifter svindel.no og sørger for at innholdet holdes oppdatert, slik at både bankene og andre aktører kan bruke den som en del av sin informasjonsformidling.



eID

16. Nytt regime for eID og forventninger til dette

I dag fungerer BankID som den nasjonale eIDen i Norge, med 4,6 millioner brukere. Nå arbeider Digdir med å avgjøre hvilken løsning Norge skal bruke for å oppfyllet ansvaret i det nye regelverket fra EU, eIDAS 2.0. Regelverket pålegger alle EØS-land å tilby innbyggerne tilgang til en eID på høyt sikkerhetsnivå. I dag oppfyller ikke BankID dette kravet.

eIDAS-forordningen fra 2014 skal gjøre det enklere for næringsliv, borgere og myndigheter å samhandle digitalt på tvers av EU/EØS. I 2024 ble forordningen revidert. eIDAS 2.0 forplikter staten til å tilby alle en gratis digital lommebok med eID på høyt sikkerhetsnivå. Lommeboken blir en mobilapp med attesterte attributter – som digitale førerkort, vitnemål, bostedsattester, fullmakter og resepter – utstedt av offentlige og private aktører. Den skal kunne brukes på tvers av landegrenser.

Uansett hva som velges for eID i Norge, vil resultatet ha stor betydning for bankene som eiere og utstedere av BankID, og som sentrale brukere av eID og e-signering. Det er derfor viktig å følge utviklingen tett og gi innspill til beslutningstakere.

Svindel har ikke vært en sentral del av eIDAS-diskusjonen. Det er imidlertid ønskelig ved implementeringen i Norge at endringene som kommer i alle fall ikke fører til økt svindel.

BankID har de senere årene tatt flere grep for å bidra til bedre antisvindelarbeid i Norge, som blant annet utvikling av et nytt antisvindelsystem som gjør det lettere å alarmere når en BankID blir misbrukt. Det er også lagt til rette for kontekstinformasjon til kunden ved bruk av BankID.

Det nye antisvindelsystem gir bankene varsel når en BankID ser ut til å være misbrukt. Siden en stor del av digitale tjenester forholder seg til BankID i dag, ville det styrke det samlede antisvindelarbeidet dersom også disse aktørene ble varslet via antisvindelsystemet. Dette gjelder særlig offentlige tjenesteleverandører som NAV og Skatteetaten, men også andre både offentlige og private virksomheter.

Gjennom det felles antisvindelarbeidet har bankene de senere årene fremmet en rekke krav til BankID om tiltak som anses nødvendige for å redusere svindel. Flere av disse tiltakene er nå innført, mens andre fortsatt gjenstår. Som et minimum bør disse kravene oppfylles i de fremtidige eID-løsningene som norske forbrukere og virksomheter skal benytte.

Finans Norge vil fortsette å gi innspill til utredningen av nytt eID-regime, og vil bidra til implementeringen av regelverket i norsk rett.

Referanseliste

(1) **Finanstilsynet. (2025). Svindelstatistikk første halvår 2025.**
https://www.finanstilsynet.no/publikasjoner-og-analyser/svindel-og-svindelstatistikk/2025/h1/svindelstatistikk-forste-halvar-2025/

(2) **Økokrim. (2024). Økokrim-modellen; En forebyggende prosess og vektingsmodell. Frigitt 09.09.2024.**
https://www.okokrim.no/veiledninger.6419850-565567.html

(3) **Finans Norge. (2024) Svindel.no: Norske banker hjelper deg å gjenkjenne og stoppe svindel.**
https://www.finansnorge.no/tema/personlig-okonomi/forbrukerinformasjon-slik-unngar-du-a-bli-svindlet/

(4) **Regjeringen. (2026). Over 80 millioner svindelforsøk stanset i 2025 – nå rettes innsatsen mot svindel på nett.**
https://www.regjeringen.no/no/aktuelt/over-80-millioner-svindelforsok-stanset-i-2025-na-rettes-innsatsen-mot-svindel-pa-nett/id3152314/

(5) **Finans Norge. (u.å.). Fagutvalg antisvindel bank.**
https://www.finansnorge.no/om-finans-norge/styrer-og-utvalg/fagutvalg-antisvindel-bank-fab/

(6) **Finans Norge. (2024). Veileder for personellsikkerhet for finansnæringen. Frigitt 2024.**
https://www.finansnorge.no/bransjer/arbeidsliv/arbeidsrett/veileder-i-personellsikkerhet/

(7) **Finanstilsynet. (2026). Sluttrapporter fra prosjekter om deling av data for å bekjempe økonomisk kriminalitet.**
https://www.finanstilsynet.no/nyhetsarkiv/nyheter/2026/sluttrapporter-fra-prosjekter-om-deling-av-data-for-a-bekjempe-okonomisk-kriminalitet/

(8) **Regjeringen. (2025). Høring - finansforetaks informasjonsdeling for å bekjempe økonomisk kriminalitet.**
https://www.regjeringen.no/no/dokumenter/horing-finansforetaks-informasjonsdeling-for-a-bekjempe-okonomisk-kriminalitet/id3118997/

(9) **Stortinget. (2024). Felles verdier – felles ansvar – styrket innsats for forebygging og bekjempelse av økonomisk kriminalitet. (St.meld. nr. 15 (2023–2024)).**
https://www.stortinget.no/no/Saker-og-publikasjoner/Saker/Sak/?p=98244

(10) **Finans Norge. (u.å). Samarbeid mot økonomisk kriminalitet.**
https://www.finansnorge.no/tema/okonomisk-kriminalitet/samarbeid-mot-okonomisk-kriminalitet/

Finans Norge

Besøksadresse: Finansnæringens Hus, Hansteens gate 2, 0253 Oslo
Telefon: 23 28 42 00 | firmapost@finansnorge.no | finansnorge.no