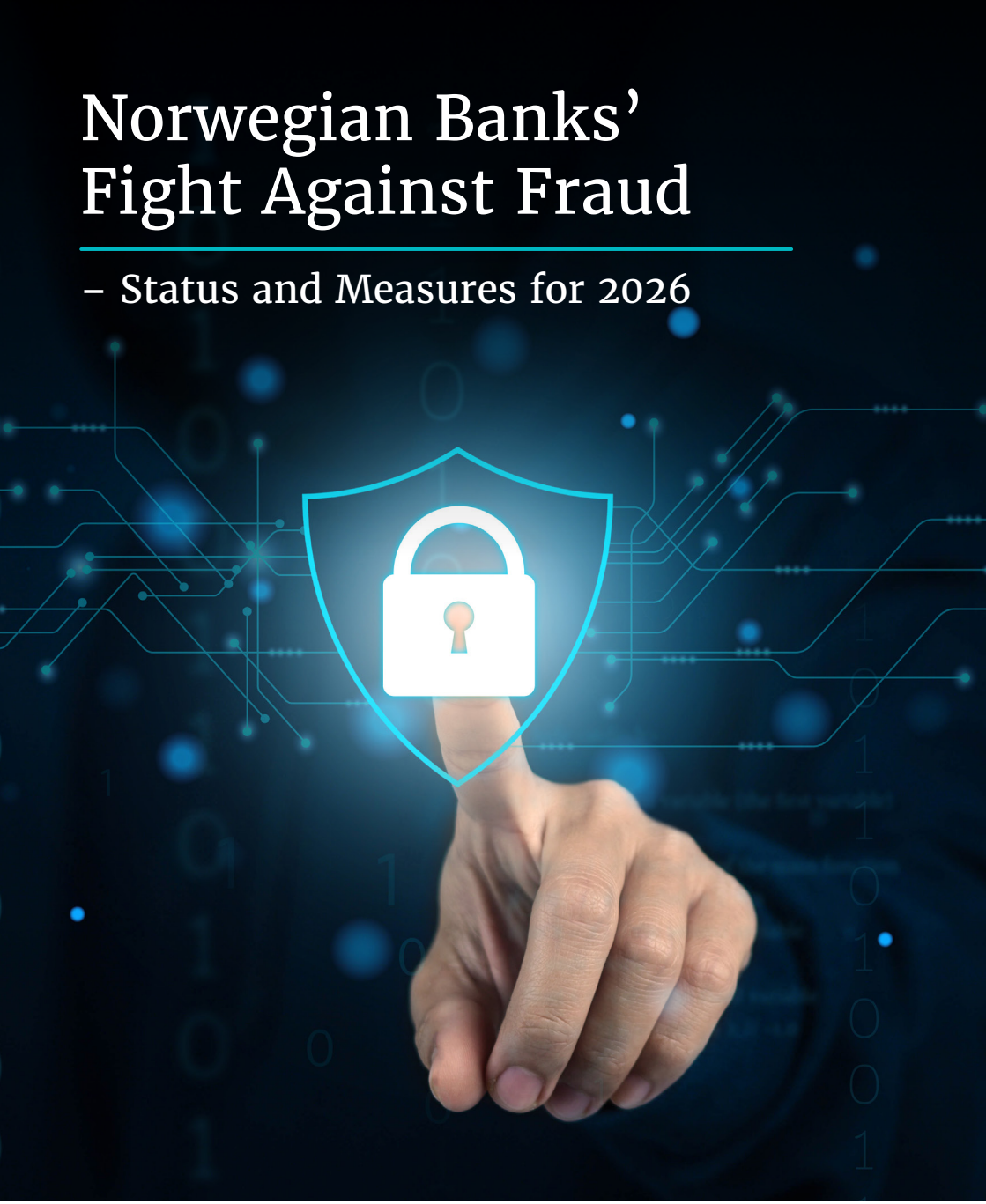
# Norwegian Banks' Fight Against Fraud

## – Status and Measures for 2026



Finance Norway

# Innhold

# Foreword

**Fraud and other forms of financial crime represent a serious societal challenge to individuals, businesses and society as a whole.** In recent years, Norwegian banks have significantly strengthened their effort to prevent and stop fraud. These efforts are delivering results.

According to fraud statistics from the Financial Supervisory Authority of Norway, total financial losses related to fraud declined in the first half of 2025 compared to the previous period, despite a continued increase in attempted fraud.

## *Banks are stopping more fraudulent transactions than before and prevented NOK 1,5 billion from reaching criminal networks.*

**At the same time, the fraud landscape is changing rapidly.** The banks observe that fraudsters are adapting their methods, using new technology and combining multiple methods to increase their chances of success. A growing share of fraud is based on manipulation, where victims themselves are deceived or pressured into carrying out the fraudulent actions. This is particularly evident in investment fraud and romance scams. The widespread use of digital platforms, social media and artificial intelligence has made fraud more targeted, more convincing and more difficult to detect.

**Norwegian banks address these challenges through a broad set of measures.** These include preventive actions, continuous transaction monitoring and rapid response when fraud attempts occur. Improved monitoring systems, more friction in mobile and online banking solutions and better customer information have all contributed to reducing losses and limiting harm.

**Cooperation has proven to be a key success factor.** Close collaboration between banks, authorities, telecom providers and other stakeholders has led to effective measures, such as blocking scam calls before they reach customers and providing clearer information to customers during critical transactions. Increased use of the BankID app, which gives users better context and warnings, has also strengthened fraud prevention,

**Effective fraud prevention requires a coordinated and long-term approach.** Banks are part of a broader total defence against fraud, where public authorities, private enterprises and individuals each have a role to play.

This report presents Norwegian banks' joint assessment of the fraud landscape in 2026. It outlines the fraud methods considered most relevant and describes the measures banks believe must be prioritised to strengthen prevention, detection and cooperation in the year ahead.

Gry Nergård, Director of Anti-Fraud at Finance Norway and Chair of the Expert Committee on Bank Fraud (FAB).

# Status of Fraud Methods Reported by the Norwegian Banks

In December 2025, Norwegian banks conducted a joint assessment of the fraud methods considered most relevant for the year ahead. This assessment forms the basis for identifying which measures should be prioritised to prevent, detect and respond to fraud.

Fraud affects a wide range of population groups, and individuals of all ages may be targeted. Losses vary from minor amounts to significant financial impact, depending on the fraud method used. Some forms of fraud are highly intrusive and can cause severe personal distress in addition to financial loss.

Banks identify manipulation-based fraud as the most serious challenge in 2026. In these cases, victims are deceived or pressured into carrying out the fraudulent actions themselves. Examples include so-called "safe account" scams, investment fraud and romance scams. At the same time, banks observe that as they have become more effective at stopping account-to-account fraud, card-related fraud has increased.

Banks also report increased use of hybrid fraud, where multiple fraud methods are combined against the same victim over time. In some cases, previous victims are contacted again by fraudsters posing as helpers offering to recover lost funds.

Based on shared experience, Norwegian banks have mapped a broad range of fraud methods and jointly assessed which are most likely to be relevant in 2026. This report presents 17 key fraud methods.

## Fraud Methods

Norwegian banks have identified a broad range of fraud methods that pose a risk to individuals and businesses. Many of these methods rely on deception and manipulation, often combining digital tools, social engineering and

psychological pressure. Below is an overview of the fraud methods considered most relevant for 2026.

## 1. Phishing (All Variants)

Phishing is a widely used fraud method in which fraudsters attempt to obtain sensitive information such as BankID credentials (Norway's most used type of digital ID), passwords or card details. Victims are typically contacted via phone calls, text messages, emails, online links or QR codes. The stolen information is subsequently used to carry out fraudulent transactions.

## 2. Fraud Involving Home Visits

This form of fraud often targets elderly or vulnerable individuals. Fraudsters first contact victims by phone, claiming that they have been exposed to fraud. Posing as police officers, bank employees or technicians, they announce that someone will visit the victim's home to provide assistance.

Shortly afterwards, a fake representative arrives, sometimes wearing false uniform or identification. The fraud can involve emptying bank accounts, stealing valuables, restricting the victim's movements, or using threats and physical force. Banks consider this a highly serious and increasingly organised form of fraud.

## 3. Gift Card Fraud

Fraud with gift card is often part of a larger scam. Victims are contacted through phone calls, messages, emails or social media. Fraudsters may impersonate romantic partners, friends, public authorities, technical support, employers or family members in distress.

Victims are instructed to purchase gift cards and share the codes. The fraudster then uses or resells the codes, making it difficult to trace the funds.

## 4. "Safe Account" Scams

Victims are contacted by individuals claiming to represent a bank or the police and are told that their funds are at risk. They are instructed to transfer money to a so-called "safe account". In reality, the account belongs to the fraudster or to a money mule.

In some cases, the funds are first transferred between accounts in the victim's own name to avoid detection, before being moved on.

## 5. Investment Fraud and Romance Scams

These are among the most serious forms of manipulation-based fraud. Victims often initiate contact through fake investment advertisements or fraudulent dating profiles.

The fraud may continue over long periods and result in substantial financial losses. Some victims take out loans to invest more money or to support a supposed romantic partner. Fraudsters frequently use remote-access software and increasingly rely on cryptocurrency, making detection and recovery difficult.

## 6. Loan Fraud

Loan fraud exploits digital lending processes and public data systems. It may involve falsified income information, manipulated business registrations or coordinated loan applications. This type of fraud is often linked to broader financial crime involving public authorities or insurance companies.

## 7. Buy Now, Pay Later (BNPL) Fraud

BNPL fraud involves misuse of "buy now, pay later" solutions. Common forms include account takeover, synthetic identity fraud, fraudulent account creation, purchases made with no intention of repayment, and abuse of refund systems.

## 8. Account and Identity Fraud via New Payment Providers

Fraudsters increasingly misuse new payment applications and digital wallets to gain access to victims' accounts. In some cases, stolen mobile phones, SIM swaps or eSIM misuse are used to gain full control over accounts and devices.

## 9. Card Fraud

Card fraud remains common and continues to evolve. It includes the use of stolen cards, misuse of card details and relay fraud, where NFC signals from a card or phone are intercepted and transmitted in real time to enable unauthorised purchases.

## 10. Fraud via the Internet and Social Media

Banks observe a rise in fake advertisements, false profiles and manipulated search results online. This increases the risk of online shopping fraud, investment scams, romance scams and phishing, while also undermining trust in digital services.

## 11. Recruitment of Money Mules

Criminal networks increasingly recruit individuals to provide bank accounts, identities or payment solutions. Recruitment often occurs through social media, messaging platforms or fake job advertisements. Young adults are particularly exposed.

## 12. Hybrid Fraud

Hybrid fraud combines several fraud methods against the same victim over time. The fraud may start with phishing or social manipulation, followed by "safe account" transfers, loan fraud and the movement of funds through money mule networks. Previous victims may also be contacted again under the pretence of offering assistance or recovery of lost funds.

## 13. Insider Fraud

Fraudsters increasingly target employees with access to financial systems, data or valuable resources. Employees may become involved voluntarily or be deceived or coerced into participating in fraud.

## 14. CEO Fraud

CEO fraud and invoice manipulation continue to cause significant losses in the corporate sector. Fraudsters impersonate executives, suppliers or trusted partners to pressure businesses into making urgent payments or changing bank account details. These attacks often occur without technical intrusion, relying instead on spoofing, social engineering, and exploiting internal routines.

## 15. “Friendly” Fraud

So-called “friendly fraud” involves acquaintances or friends abusing refund schemes by reporting legitimate transactions as unauthorised. Banks see this form of fraud increasing due to strong consumer rights and low perceived risk for perpetrators.

## 16. Malware

Malware is malicious software designed to exploit vulnerabilities in digital systems for financial gain. Banks observe increasing use of malware in fraud schemes in Sweden and expect this threat to grow also in Norway.

## 17. Use of Artificial Intelligence in Fraud

Fraudsters increasingly use artificial intelligence to make fraud more convincing. AI enables the creation of realistic fake images, videos and audio, including deepfake content. This is seen in fake advertisements, manipulated video meetings and impersonation of trusted individuals, making fraud harder to detect.

Banks view this development as a growing threat, as AI makes social engineering more convincing and significantly harder to detect in time.

# Measures to Combat Fraud

There is no single solution to the challenges described in this report. Fraud must be addressed through a combination of measures involving multiple stakeholders. Norway's National Authority for Investigation and Prosecution of Economic and Environmental Crime has introduced the concept of a total defence against fraud, where the private sector, public authorities, legislators and individuals all have a role to play. Norwegian banks are prepared to contribute actively to this effort.

Below is an overview of the measures that banks believe should be prioritised in 2026. Some measures are to be implemented by banks individually, while others require cooperation with other actors or efforts to encourage broader participation in the total defence against fraud. The measures vary in maturity: some are well established, while others are still under development. Priorities will evolve as fraud methods continue to change.

The measures address different stages of the fraud process. Some focus primarily on prevention, as effective prevention reduces the number of victims and limits financial losses for individuals, banks and society. Other measures aim to detect fraud while it is taking place, enabling rapid intervention. Additional measures focus on follow-up when fraud has already occurred.

# Measures Implemented by Norwegian Banks

## 1. Anti-Fraud Handbook

In 2024, Norwegian banks jointly developed the Banks' Anti-Fraud Handbook. The handbook serves as a practical toolbox to support each bank's work against fraud, based on individual risk assessments.

The measures are organised into six main categories:

- **Customer alerts:** Banks notify customers of suspicious activity in mobile and online banking so they can take action in time.
- **Contextual information:** Customers receive clearer information about what they are about to approve or sign, helping them identify fraud.
- **Time delays:** Built-in delays give banks and customers additional time to detect, investigate and stop attempted fraud.
- **Enhanced verification (step-up authentication):** Higher-risk actions require additional confirmation of identity or intent.
- **Anti-fraud systems:** Banks monitor transactions for suspicious activity and can apply blocks or restrictions when needed.
- **Periodic review:** Customers are encouraged to review account and security settings regularly to reduce fraud risk.

These tools can be combined and applied across different banking services. In spring 2026, an evaluation will assess how the handbook is being used and whether updates are needed.

## 2. Transaction Monitoring

All banks in Norway use transaction-monitoring systems, either developed internally or provided by external vendors. The purpose of transaction monitoring is to detect unusual or suspicious transactions and stop fraud in progress.

These systems require continuous maintenance and updating to remain effective as fraud methods change. New and upcoming EU regulations will place additional requirements on transaction monitoring, which may influence how such systems are designed and operated.

Finance Norway facilitates dialogue within the Norwegian banking sector on how future EU requirements should be implemented effectively.

## 3. Personnel Security

In 2024, Finance Norway published guidelines on personnel security to prevent internal fraud and other forms of economic crime. Strengthening personnel security remains a priority.

The guidance addresses how organisations can work systematically with personnel security throughout all phases of the employment relationship, with the aim of reducing the risk of insider threats.

## 4. Shared Guidelines, Guidance and Templates

Both existing national legislation and forthcoming EU regulations create a need for common guidelines, practical guidance and templates to support banks in performing specific tasks in a consistent and effective manner.

Finance Norway facilitates the development of such materials in close cooperation with banks, based on identified needs.

# Information and Data Sharing

## 5. Information and Data Sharing

Effective fraud prevention depends on improved sharing of information and data across sectors. Banks identify a need for stronger data flows between:

- Banks
- Banks and law enforcement
- Banks and public authorities
- Banks and telecom providers

Several banks have participated in regulatory sandbox projects led by the Norwegian Financial Supervisory Authority and the Data Protection Authority, exploring how data sharing can support fraud prevention. As a result, changes to financial legislation have been proposed to enable broader data sharing for the purpose of preventing and detecting fraud.

Data sharing is also a key topic in new EU payment regulations. Finance Norway will continue to facilitate and participate in further discussions regarding data sharing.

### 6. Secure Digital Sharing of Information and Data

Assuming that the opportunity to share more data arises, it will be essential to establish expedient and secure ways of doing so. Banks in Norway have identified the Nordic Financial CERT (NFCERT) as their preferred partner. NFCERT's scope of responsibility has been expanded to include the prevention of financial crime and data sharing. Through various ongoing projects, DSOP (Digital Cooperation Public–Private) has developed technical solutions for the digital sharing of data between financial institutions and public agencies. It is currently being assessed whether these solutions can also be utilized for data sharing between banks and the public sector in an anti-fraud context.

More general information, which is not categorized as personal or sensitive data, should also be shared continuously to ensure relevant anti-fraud measures. Under the DSOP umbrella, OPS ØK has been established — a public-private partnership between the financial industry and public actors designed to strengthen the fight against money laundering, terrorist financing, and fraud. Finance Norway assists here with administration, a shared collaboration platform, meeting arenas, and activities.

The banks exchange information through several different forums. The most central of these for anti-fraud efforts is the Banks' Anti-Fraud Committee (FAB), organized by Finance Norway.

Finance Norway will continue to support the work of securing the digital sharing of information and data through NFCERT and OPS ØK.

## Cooperation with Other Actors

### 7. Cooperation with the Police

Close and effective cooperation with the police remains a high priority. This is essential both for prevention and for ensuring proper investigation and follow-up of fraud cases.

Key priorities include:

- Cooperation with specialised fraud units
- Promoting the use of digital reporting of fraud cases
- Encouraging effective police handling of investigations and prosecution

- Prioritisation of serious fraud cases, including those involving coercion, violence or organised crime
- Development of clear cooperation routines between banks and law enforcement

## 8. Cooperation with the Telecom

A significant share of fraud begins with phone calls, text messages or emails. Cooperation with the telecom sector is therefore crucial.

Key priorities include:

- Stronger measures against spoofing from abroad
- Improved customer verification when phone subscriptions are created or modified, including use of eSIM
- Stronger safeguards against email-based fraud

## 9. Cooperation with Other Payment Service Providers

Banks are concerned that some payment intermediaries and providers of digital wallets lack sufficient anti-fraud mechanisms, making them vulnerable to misuse.

Banks will work together to address these risks through direct dialogue with relevant actors, as well as through engagement with regulators and policymakers.

## 10. Cooperation with Other Industries

Fraud affects many sectors beyond finance. Finance Norway engages with business organizations and industry groups to strengthen fraud prevention across value chains.

This includes dialogue with retail, e-commerce and second-hand marketplaces, where measures against gift card fraud and platform misuse are particularly important.

## 11. Cooperation with Public Authorities

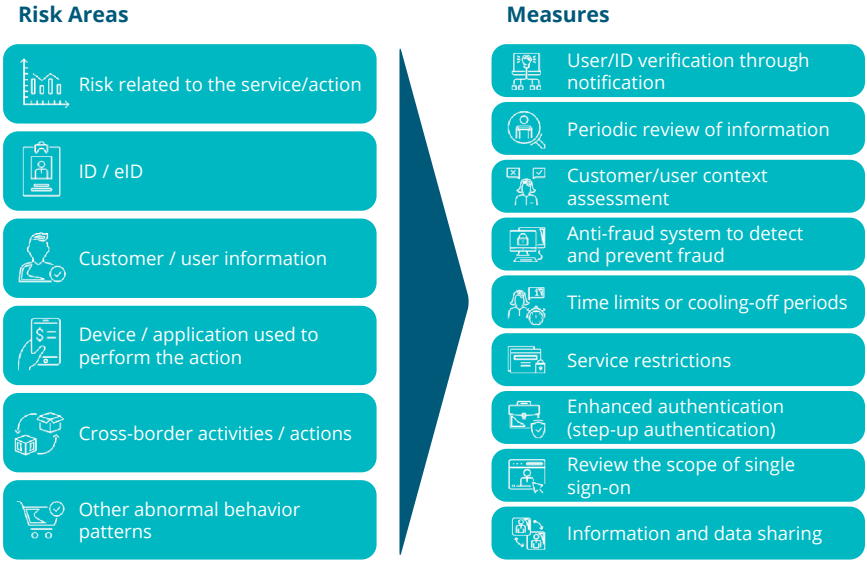
Banks play an important role in supporting public authorities in fraud prevention and detection, while also depending on strong public safeguards to reduce fraud risks related to public registers and systems.

The public-private partnership OPS ØK (Public Private Cooperation Against Economic Crime) remains a key cooperation arena and is prioritised as an effective tool in the fight against economic crime.

## 12. Anti-Fraud Handbook for the Public and Private Sectors

In 2025, Finance Norway, together with representatives from banks, insurance companies, public authorities and law enforcement, developed an Anti-Fraud Handbook for the Public and Private Sectors.

In 2026, Finance Norway will continue presenting and promoting this handbook to improve prevention efforts across sectors and strengthen cooperation.




## 13. Nordic Cooperation

Fraud challenges are largely similar across the Nordic countries, and many banks operate across borders. A more structured and regular Nordic cooperation has been established, strengthening information sharing and joint efforts.

Finance Norway will continue close cooperation with its Nordic counterparts.

# Legal Framework

## 14. EU Regulations and Implementation in Norwegian Law

Several current and upcoming EU regulations will significantly affect banks' ability to combat fraud. These include:

- the Instant Payments Regulation (IPR)
- the Payment Services Regulation (PSR)
- the revised eIDAS 2.0 regulation

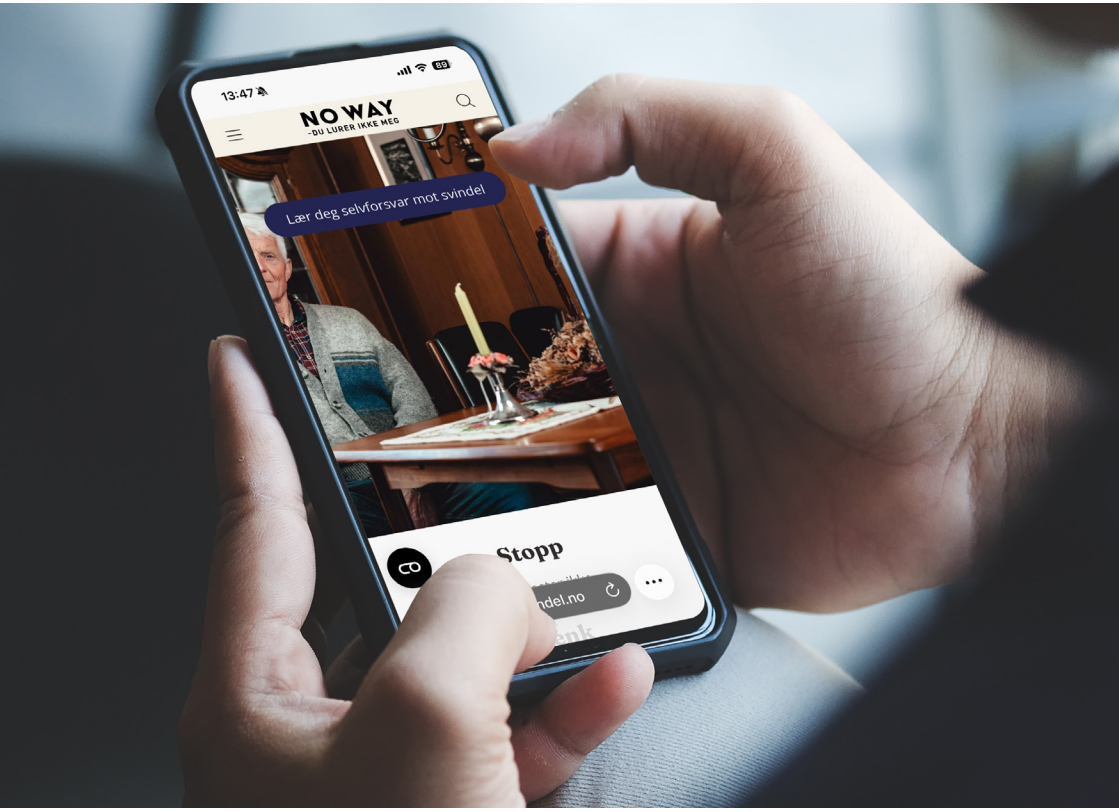
It remains uncertain to what extent these regulations will reduce fraud or affect banks' operational flexibility. Finance Norway will actively contribute to assessments and implementation efforts.

# Consumer Information

## 15. Joint Consumer Awareness Initiatives

In 2024, banks launched the joint campaign "No Way – You Won't Fool Me" to improve consumer awareness of fraud risks and prevention.

As part of the campaign, the website svindel.no was established as a central information hub. The content remains relevant and is actively maintained for continued use by banks and other actors. New joint initiatives may be considered for 2026.



# Electronic Identification (eID)

## 16. New eID Framework and Expectations

BankID currently serves as Norway's national electronic identity (eID) solution and is used by approximately 4.6 million people. The Norwegian Digitalisation Agency (Digdir) is now assessing which solution Norway should adopt to meet its obligations under the revised EU regulation, eIDAS 2.0.

**eIDAS 2.0** requires all EEA countries to provide residents with access to an electronic identity solution at a high level of security. BankID does not currently meet this requirement. The original eIDAS Regulation from 2014 aimed to facilitate digital interaction between businesses, citizens and public authorities across the EU and EEA, and was revised in 2024.

Under eIDAS 2.0, states are required to offer all citizens a free digital identity wallet with high assurance. The wallet will be provided as a mobile application and contain verified digital attributes such as digital driving licences, diplomas, certificates of residence, powers of attorney and prescriptions. These attributes may be issued by both public and private entities and must be usable across borders.

Regardless of which eID solution is chosen in Norway, the outcome will have significant implications for banks, both as owners and issuers of BankID and as major users of electronic identification and electronic signatures. It is therefore important to closely monitor developments and provide input to decision-makers.

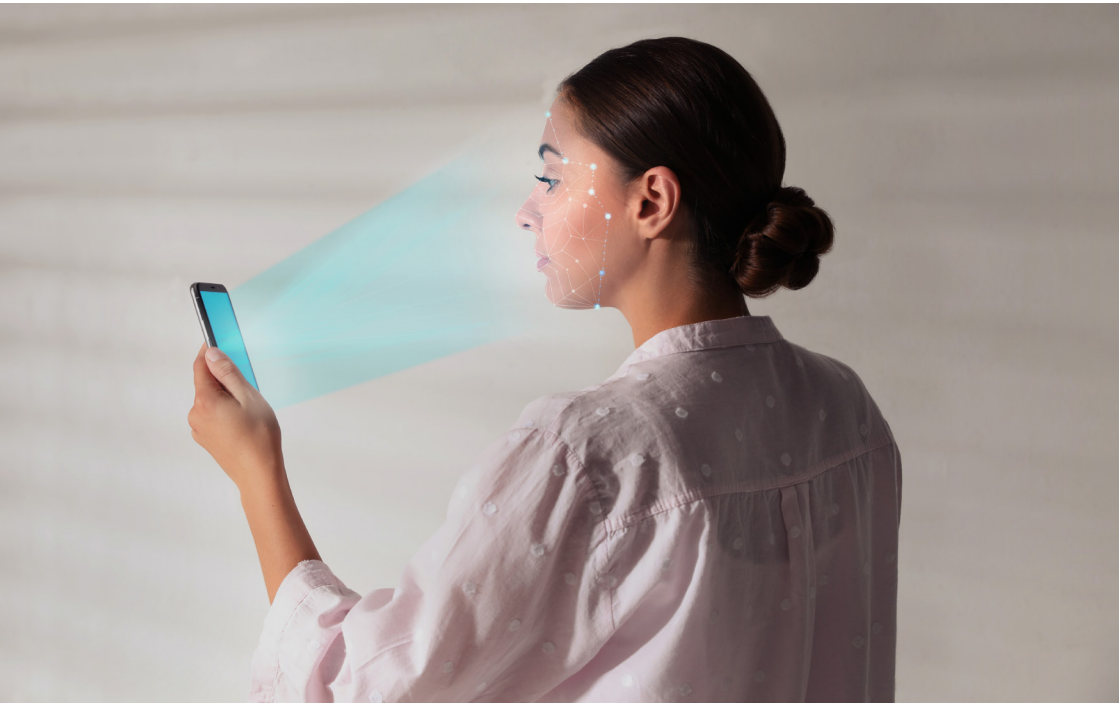
Fraud prevention has not been a central focus of the eIDAS discussions. However, when implementing the new framework in Norway, it is essential to ensure that the changes do not lead to increased fraud risk.

In recent years, BankID has introduced several measures to strengthen fraud prevention. These include a new anti-fraud system that enables faster alerts when a BankID is suspected of misuse, as well as improved contextual information to help users better understand what they are approving.

The new anti-fraud system provides banks with alerts when misuse is detected. Given that a large share of digital services in Norway rely on BankID, overall fraud prevention would be strengthened if other service providers were also notified through this system. This is particularly relevant for public service providers such as the Norwegian Labour and Welfare Administration (NAV) and the Tax Administration, but also applies to other public and private entities.

Through joint anti-fraud efforts, banks have submitted a number of requirements to BankID regarding measures considered necessary to reduce fraud. Some of these measures have already been implemented, while others remain outstanding. As a minimum, these requirements should be met in any future eID solutions that Norwegian consumers and businesses are expected to use.

Finance Norway will continue to provide input to the development of a new eID framework and contribute to the implementation of the regulation into Norwegian law.



# References


- **Financial Supervisory Authority of Norway. (2025). Fraud statistics for the first half of 2025.**
  https://www.finanstilsynet.no/publikasjoner-og-analyser/svindel-og-svindelstatistikk/2025/h1/svindelstatistikk-forste-halvar-2025/

- **The National Authority for Investigation and Prosecution of Economic and Environmental Crime. (2024). The Økokrim model: A preventive process and weighting model. Released 9 September 2024.**
  https://www.okokrim.no/veiledninger.6419850-565567.html

- **Finance Norway. (2024). svindel.no: Norwegian banks help you recognise and prevent fraud.**
  https://www.finansnorge.no/tema/personlig-okonomi/forbrukerinformasjon-slik-unngar-du-a-bli-svindlet/

- **The Norwegian Government. (2026). Over 80 million fraud attempts prevented in 2025 – focus now shifting to online fraud.**
  https://www.regjeringen.no/no/aktuelt/over-80-millioner-svindelforsok-stanset-i-2025-na-rettes-innsatsen-mot-svindel-pa-nett/id3152314/

- **Finance Norway. (n.d.). Expert Committee on Bank Fraud (FAB)**
  https://www.finansnorge.no/om-finans-norge/styrer-og-utvalg/fagutvalg-antisvindel-bank-fab/

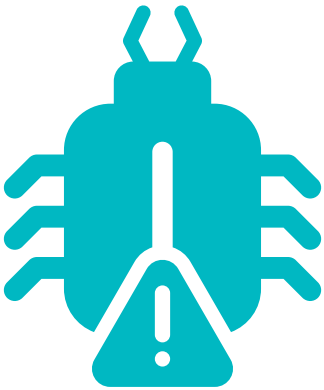
- **Finance Norway. (2024). Guidelines on personnel security for the financial sector.**
  https://www.finansnorge.no/bransjer/arbeidsliv/arbeidsrett/veileder-i-personellsikkerhet/

- **Financial Supervisory Authority of Norway. (2026). Final reports from projects on data sharing to combat economic crime.**
  https://www.finanstilsynet.no/nyhetsarkiv/nyheter/2026/sluttrapporter-fra-prosjekter-om-deling-av-data-for-a-bekjempe-okonomisk-kriminalitet/

- **The Norwegian Government. (2025). Consultation – information sharing by financial undertakings to combat economic crime.**
  https://www.regjeringen.no/no/dokumenter/horing-finansforetaks-informasjonsdeling-for-a-bekjempe-okonomisk-kriminalitet/id3118997/

- **The Norwegian Parliament. (2024). Shared values – shared responsibility: Strengthened efforts to prevent and combat economic crime (White Paper No. 15 (2023–2024).**
  https://www.stortinget.no/no/Saker-og-publikasjoner/Saker/Sak/?p=98244

- **Finance Norway. (n.d.). Cooperation against economic crime.**
  https://www.finansnorge.no/tema/okonomisk-kriminalitet/samarbeid-mot-okonomisk-kriminalitet/


Visiting Address: Finansnæringens Hus, Hansteens gate 2, 0253 Oslo, Norway
Telefon: +47 23 28 42 00 | firmapost@finansnorge.no | finansnorge.no