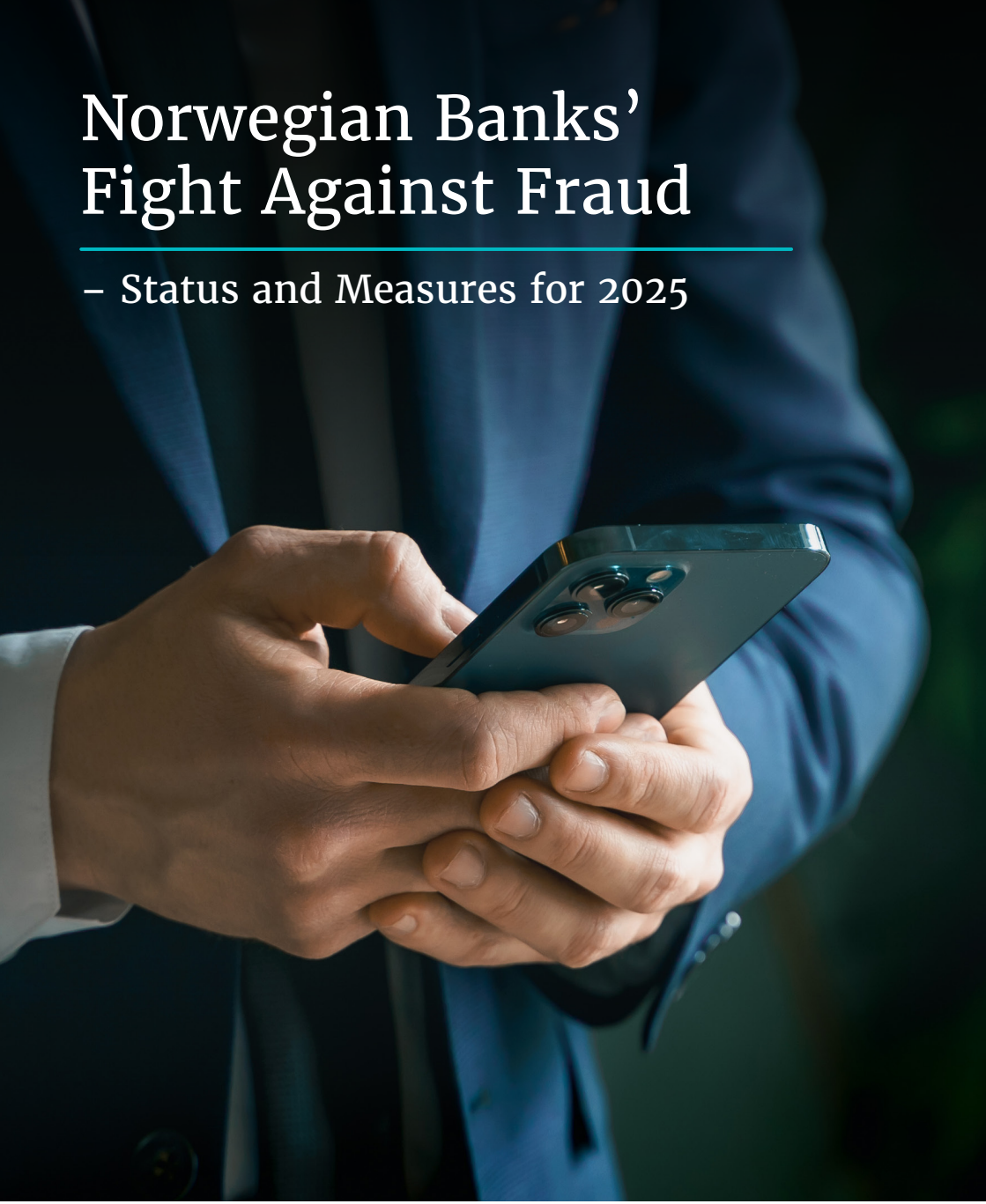
Norwegian Banks' Fight Against Fraud

– Status and Measures for 2025



Finance Norway

Contents

Foreword

Fraud in digital channels has reached a scale that challenges us as a society. It affects individuals and banks, which suffer significant losses. Equally serious is that society's losses become the fraudsters' income, which is used to finance even more serious crime. A rapidly growing criminal sector, both domestic and abroad, can eventually undermine society. Therefore, we must defend ourselves. Fraud must be combated with a combination of measures from multiple actors.

The Financial Supervisory Authority's (FSA) fraud statistics for the first half of 2024 show that the total loss for banks due to fraud with account transfers and the use of payment cards increased by NOK 85 million to NOK 607 million, an increase of 16 percent from the second half of last year. This is only a piece of the overall picture. In addition, there are losses not recorded in these statistics, where losses from fraud are not covered by statutory requirements for banks.

Amounts in million NOK	Fraud Transactions - Account Transfers (Online Banking, etc.)	Fraud Transactions with Payment Cards Reported by Card Issuer	Total Losses	Losses as a Share of Total Transaction Value
H1 2024	414	193	607	0,002
H2 2023	352	170	522	0,0016
H1 2023	296	111	407	0,0012
H2 2022	233	121	354	0,0015
H1 2022	162	79	241	0,0011
H2 2021	159	83	241	0,0014
H1 2021	188	79	267	0,0014

Source: The Financial Supervisory Authority

Fraud via account transfers accounted for the largest increase, particularly cases where the customer is manipulated into carrying out the transactions themselves. At the same time, losses decreased in cases where the fraudster performs the transfer. Although fraudsters manage to deceive significant amounts, banks still succeed in preventing large sums from entering the criminal economy. In the first half of 2024, banks prevented fraud attempts on account transfers and card payments amounting to NOK 1,341 million.

Finance Norway, together with experts from the Anti-Fraud Banking Committee (FAB), has assessed the status and measures against fraud in the banking sector as of October 30, 2024. Simultaneously, recommendations have been proposed across sectors to prevent, detect, and follow up on fraud.

The committee consists of experts representing most banks in Norway. The committee's area of responsibility includes issues related to the financial sector's work to prevent and detect fraud and scams. The committee is an advisory body for Finance Norway in this area and formally reports to the Banking and Capital Market Industry Board (BBK).

Finance Norway and the committee hope that the measures in this brochure will be important in the fight against fraud. In this brochure, you will get an overview of the fraud challenges banks and society face, and what banks believe is necessary to improve the prevention, detection, and handling of fraud in 2025.

Gry Nergård, Consumer Policy Director at Finance Norway

Status of Fraud Methods from Norwegian Banks

The status of fraud methods was assessed in October 2024 and consists of a review of methods used by fraudsters, and development patterns to watch. It shows where banks believe there is a need to increase efforts to minimize the impact of criminal activity.

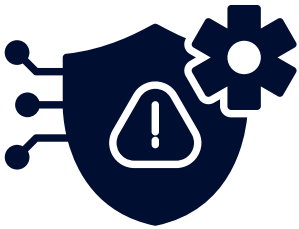
The various fraud methods can target different groups, but all age groups are exposed to one or more types of methods. The losses for victims can range from small amounts to significant sums, depending on the fraud method used. Some methods are particularly intrusive and can cause significant human suffering in addition to financial losses.

While some fraud methods are widespread right now, others are in early development. The committee believes it is important to focus on these emerging trends to be better prepared if they increase in scope. Therefore, these are included at the end of the list.

Fraud Methods

1. "Safe Account" Fraud

Fraud victims are increasingly being manipulated into carrying out the entire fraud themselves, for example in so-called "safe account" fraud. Here, the victim is called by "the bank" or "the police," who say that the victim is about to be defrauded and must transfer money to a secure account. However, this account is one that the fraudster controls. In such cases, the victim is often defrauded of large amounts.



2. Fraud with Home Visits

Fraudsters call the victim, typically elderly and living alone, and claim that the victim has been defrauded. They pose as police and say that an officer will come to their home to help. Shortly after, a fake police officer appears, often with a uniform and fake ID. The fraudsters empty the victim's accounts and may hold them captive, either at home or elsewhere. The National authority for Investigation and Prosecution of Economic and Environmental Crime (Økokrim) warns of the risk of increased physical violence, and the fraud causes significant psychological stress and substantial financial losses.

3. Phishing in All Variants

A commonly used fraud method is phishing. Here, the victim is tricked into giving away information such as BankID, username and password, credit card numbers, and other sensitive personal information. This occurs via phone calls, QR codes, and by clicking on links in text messages, emails or online. The information the victim provides is used for fraud.

4. "Hi Mom and Dad" Fraud

A fraudster pretends to be someone you know, such as a friend or family member, and asks for financial aid via text messages, email, social media, or phone calls. They may say their phone is broken and that they are using another device to reach them. The fraudster asks you to pay a bill or send money to an account they control.

5. Lending Fraud

Fraudsters simultaneously apply for loans from multiple banks or credit companies, using stolen or purchased BankID and manipulated information such as income. The purpose is often to buy or lease a car. The cars are driven out of the country, and the loan is either never paid or paid with laundered money. Banks that offer unsecured loans are more vulnerable to this type of fraud.

6. Fraud with Consent-Based Loan Applications

Fraud with consent-based loan applications (Samtykkebasert lånesøknad – SBL) is a type of lending fraud that is often part of a larger scam and may be linked to fraud in the Tax Administration, The Norwegian Labour and Welfare Administration (NAV), and insurance. SBL is part of a system where income and tax data can be retrieved from the Tax Administration with consent via Altinn (an internet portal for digital dialogue between businesses, private individuals and public agencies). The fraud, a form of register manipulation, exploits public digital solutions and undermines trust in the systems.

In SBL fraud, several suspicious actions often occur:

1. False "A-meldinger" (salary reports) are reported for several months at once, just befwsore a loan application is submitted.
2. These "A-meldinger" are deleted shortly after the loan is granted.
3. "A-meldinger" may also be reported for months before the business is registered in the Business Register.
4. Businesses can change information in the Brønnøysund Register Centre (responsible for the management of numerous public registers, and governmental systems for digital exchange of information in Norway) back in time to make it look like they have been in operation longer.
5. Several employees in the same business apply for loans at the same time.
6. Salary reports may be in round amounts and not match what is reported to NAV or the Tax Administration.

7. Card Fraud

Several banks report an increase in card fraud after several years where fraud with payment transfers has been dominant. From 2021 to 2024, the number of fraud transactions with payment cards increased by NOK 114 million.

8. Fraud on the Internet and Social Media

There is an increase of fake ads, fake profiles, and fake search results on the internet. This contributes to more online store fraud (buying and prepaying on a fake online store, no goods are sent), investment fraud (being tricked into investing in something that does not exist), romance fraud (being tricked into sending money to a fake persona who build a personal relationship with the victim), and phishing. In addition, confidence and the trust in digital solutions may be affected.

9. Fraud with New Actors in the Payment Market

Actors such as Vipps MobilePay AS (Scandinavian Mobile payment app), digital wallets, and other payment services that consumers and businesses can use for online and in-store purchases are increasingly being used for fraud. In these cases, the bank has limited control over the customer, which fraudsters exploit. Many of the solutions from these new actors have weaker security systems, yet the bank remains responsible for reversing transactions and bearing the financial burden if the customer is defrauded.

10. Account and Identity Fraud

Banks are particularly seeing an increase in fraudsters who manage to gain access to the victim's account and set up an app in the victim's name, such as the BankID app or mobile banking app. This allows the fraudster to perform actions without the victim's knowledge. In some cases, the fraudster also manages to take over the victim's phone, giving them access to many fraud opportunities. This occurs when the fraudster steals phones, buys phones, or sets up e-SIMs.

11. Insider Fraud

Fraudsters are increasingly targeting employees in various businesses, such as bank employees or others who have access to payment systems or valuable resources. This can include money, goods, services, or data. Employees can become involved in fraud either voluntarily (they agree to it willingly) or involuntarily (they are tricked or pressured into doing it).

12. Friendly Fraud

Fraud where friends or acquaintances collaborate to exploit the banks' strict rules on reversing transactions in cases of fraud. This can involve false transactions reported as unauthorized to get money back. Due to strong consumer rights and low risk for fraudsters, banks are seeing an increase in this type of fraud. This type of fraud also resembles patterns seen in insurance fraud.

13. New Communication Platforms

As mobile operators and email providers succeed in reducing fraud, banks are seeing fraudsters move to other platforms such as WhatsApp, Messenger, and Telegram. This is a development banks fear since control over these platforms is more limited.

14. Artificial Intelligence and Software

Banks have identified technologies such as artificial intelligence, including "deepfake," and malicious software such as "malware" on mobile phones, as well as "remote control" on both computers and phones, as potential fraud threats. Although such threats do not yet pose a significant problem, banks are closely monitoring developments. Both methods represent advanced threats in the digital landscape and have implications for fraud development.

Deepfake

Deepfake is a technology that uses artificial intelligence to create manipulated videos, images, and audio files that look or sound real. This makes it easy to be deceived by fraudsters who can pose as trusted individuals.

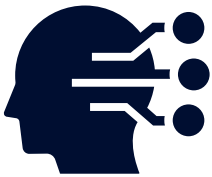
Malware

Malware (short for "malicious software") is harmful software that exploits weaknesses in computer systems for financial gain and can be used in various ways to defraud individuals and organizations.

Remote Control

Remote control of computers and phones gives fraudsters the ability to control both what is displayed on the screen and what happens in the background. By getting the victim to install specific software, the fraudster can override the device and use it for their own purposes.





Measures to Combat Fraud

Unfortunately, there is no simple solution to handle the described threats. Fraud must be combated with a combination of measures from multiple actors. Økokrim has launched the idea of a total defence against fraud, where both the business community, public authorities, legislators, and individuals must contribute. Norwegian banks are already doing their part in this effort and are ready to do even more.

Many of the banks' measures involve collaboration with other actors or influencing others to contribute to the total defence. Some of the banks' measures are very specific, while others are more overarching. This reflects that some have been in the works for a long time, while others are new and in development. The measures, and the priorities among them, will likely also change as fraud methods evolve. The main focus of the measures is to prevent fraud, as reducing its occurrence will minimize the number of people affected. Many of the measures also involve detecting fraud as it happens so that it can be stopped as quickly as possible. For cases where fraud still occurs, there are also follow-up measures.

Here is an overview of the 20 measures that banks believe are necessary to work on in 2025. The measures are not listed in order of priority, as which measures are prioritized at any given time depends on various factors, including the evolving fraud landscape:

The Banks' Own Measures Against Fraud

1. Anti-Fraud Handbook

In 2024, banks jointly developed the "Banks' Anti-Fraud Handbook" – a toolbox designed to strengthen each bank's efforts against fraud. The handbook contains measures and methods that banks can use based on their own risk assessments. The tools are divided into six main categories:

1. ***Alert:*** The bank alerts the customer about suspicious activity in mobile and online banking so that the customer can react in time.
2. ***Context:*** Customers receive more information about what action they are about to carry out, confirm, or sign, so they can detect fraud.
3. ***Time Limits:*** The bank and the customer get extra time to detect, investigate, and stop fraud attempts.
4. ***Enhanced Confirmation (Step-Up):*** For high-risk activities, the customer is asked for extra confirmation of identity or intent.
5. ***Anti-Fraud System:*** The bank monitors transactions to detect suspicious activity and can impose blocks if necessary.
6. ***Periodic Control:*** The bank encourages the account holder to regularly review settings that may affect fraud risk.

These tools can be used in various areas of the bank and combined in different ways to suit each situation.

2. Updating the Anti-Fraud Handbook

New measures for updating the anti-fraud handbook are planned for autumn 2025. It will be assessed whether specific measures against card fraud and fraud targeting the corporate market are needed. Today, the handbook is primarily designed to handle fraud with account transfers in the private market.

3. Industry Standard for the Credit Market

In 2021, Finance Norway launched the industry standard "How to Prevent, Detect, and Follow Up Cases of Misuse of BankID for Unsecured Consumer Credit." In autumn 2024, a checklist to prevent fraud in consent-based loan applications was also created under the DSOP (a cooperation between the public and private sectors in Norway to digitize processes) initiative. Compliance with the industry standard and checklist is important in the fight against fraud.

4. Personnel Security

In 2024, Finance Norway developed a guide on personnel security to prevent insider issues. Following up on this guide is a priority measure to avoid fraud and other financial crime.

Collaboration with Other Actors

5. Collaboration with the Police

A close and good collaboration with the police will continue to be highly prioritized. This is important both to prevent fraud and to ensure quick and effective follow-up of fraud cases through good investigation.

The following areas will be particularly prioritized:

- Establishing good cooperation with the Fraud Unit (Økokrim) for fraud prevention.
- Accelerating the work on digital police reports, which has already been initiated by the National Police Directorate (POD).
- Developing clear and effective routines for cooperation between banks and the police across the country.

6. Collaboration with the E-Com Sector

A good collaboration with the electronic communication services (e-com) sector, among others through the National Expert Group Against E-Com Fraud, will continue to be highly prioritized. A large part of today's fraud starts with emails, phone calls, or text messages. The more the e-com actors can stop this traffic, the harder it will be to carry out fraud in Norway.

The following areas will be particularly prioritized:

- Introducing more measures against spoofing (forging sender information).
- Blocking numbers that are not in use so that they cannot be misused for fraud.
- Better customer control when creating or changing phone subscriptions, including when creating e-sim.

7. Collaboration with Social Platforms

Many cases of fraud start on social platforms, where there is little control over what is published and who is behind it. Many ads are fake and can, for example, mimic real online stores, represent non-existent companies or profiles, or contain false endorsements, often using celebrity names. Platforms can crack down on fraud attempts after tips from the public, often after the damage has been done. However, it is unclear if and how quickly fraudulent

content is removed after such tips. The EU is discussing new rules that could give platforms greater responsibility, but it may take some time before these rules apply in Norway. To address the problem more swiftly, Finance Norway should establish contact with the most used social platforms to explore ways to collaborate on removing fraudulent content as quickly as possible.

8. Collaboration with Other Actors in the Payment Market

Banks will establish contact with other actors in the payment market, such as digital payment solutions, payment intermediaries, and digital wallets, to ensure that they have sufficient focus on anti-fraud mechanisms. Today, many of these actors are vulnerable to being exploited in fraud contexts, either knowingly or unknowingly. It is uncertain to what extent new EU regulations will help solve these challenges, and it may take time before the regulations are implemented in Norway. Therefore, banks will collaborate to address these problems both directly with the relevant actors and through dialogue with legislators in Norway and the EU.

9. Collaboration with Public Agencies

Banks play an important role in helping others, such as public agencies, to prevent and detect fraud. At the same time, banks depend on public agencies also having effective anti-fraud measures. In 2024, it was decided that OPS AT (Public-Private Cooperation Against Money Laundering and Terror Financing), which already brings together the financial sector and public agencies to combat financial crime, will be expanded to also work against fraud. Ensuring that this cooperation forum becomes a strong and effective actor in the fight against fraud is a priority task.

10. Strengthened Nordic Cooperation

The fraud situation is largely similar in the Nordic countries, and many banks operate throughout the Nordic region. Therefore, it is recommended that banks, through Finance Norway, establish closer and more regular cooperation with Nordic banking organizations. This will contribute to better information exchange and more effective cooperation across borders.

11. Broadly Composed Cooperation Body

Financial crime has also received increased political attention in Norway, especially after several TV documentaries that reveal serious cases of fraud and money laundering. This has resulted in a Norwegian parliamentary report with over 40 measures against financial crime, including several measures against fraud and scams. It may be valuable to consider establishing a broader cooperation body that brings together various industries and public agencies so that more measures can be seen in context and have a greater impact in the fight against fraud.

Data Sharing

12. Information and Data Sharing

To build a strong total defence against fraud, sharing information and data is crucial. The flow of information must be improved both between banks, but also between banks, the police, public agencies, and e-com providers. Both legal clarifications and secure technical solutions are necessary.

13. Common System for Transaction Monitoring and Data Sharing

It is being considered to develop a common system for transaction monitoring and analysis, and/or a data sharing system between banks. Such a common system can help detect ongoing fraud more rapidly and help prevent similar fraud in other banks. The possibility of establishing this will be assessed, and Nordic Financial CERT (Computer Emergency Response Team) is one of the potential actors that can contribute to better data sharing.

Several Legal Issues

14. Financial Responsibility for Fraud

Banks have significant financial responsibility for fraud that occurs in their systems. This gives banks a strong incentive to work preventively against fraud. Although the financial loss appears in the bank, there are several other actors that offer services exploited in fraud contexts. Banks therefore believe that these actors, such as e-com providers, should also be legally required to bear financial responsibility. This will give them a similar incentive to prevent fraud.

15. Early Implementation of New EU Payment Rules

One of the EU's priority tasks is to introduce new rules through the Instant Payment Regulation (IPR), which will, among other things, establish a system for verifying payment recipients. This will likely make several of today's fraud methods more difficult to carry out.

It should be considered to accelerate the implementation in Norway, as a delayed implementation could make us a more attractive country for fraud during the period when the Norwegian payment system lacks this protection.

16. The Duty of Restitution – Need for Change

According to the Financial Contracts Act, banks have significant financial responsibility, and they have adapted to this regulation. However, the Norwegian implementation of the duty of restitution places an additional burden on banks. Banks believe that this arrangement should be adjusted to give banks better leeway to assess the facts of the case and to prevent new types of fraud against the bank..

17. EU Regulations and Influence in Norway

The EU is developing a lot of new regulations that can affect the fight against fraud in Norway in several ways. Some of these regulations are already finalized and are nearing national implementation. Finance Norway should, on behalf of the banks, work to influence the development of regulations in the EU where possible, and ensure that the implementation in Norway is as appropriate as possible.

Consumer Information

18. Joint Information Campaign Against Fraud

In 2024, the banks launched a joint campaign, "No Way – You Won't Fool Me!", to teach consumers how to protect themselves against fraud. The campaign material was distributed on TV, radio, social media, online newspapers, and billboards in cityscapes. The banks also used the material in their own customer communications. As part of the campaign, the website *svindel.no* was launched. It provides useful and updated information to consumers on how to avoid fraud. The content of the campaign is still relevant and should be

actively used by the banks in 2025. It should also be considered to have a new campaign period under the direction of Finance Norway.

eID

19. Recommended Measures for BankID

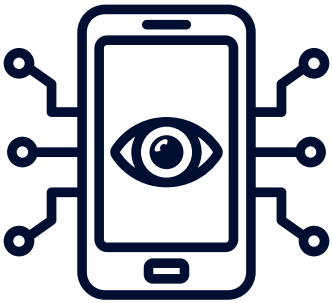
The report from the banks' anti-fraud project in 2023-2024 titled "Safe Consumers" contains several recommended measures that BankID should implement to strengthen security, but several of these have not yet been prioritized. Banks should therefore encourage BankID to implement these measures, including:

- Limiting to one OTP per certificate.
- Providing better context information in the BankID app.
- Launching a new anti-fraud system.
- Offering a better solution for blocking BankID that has been used in fraud.
- Introducing self-managed BankID and MyPage for customer history.

20. The Future of eID

In autumn 2024, The Norwegian Digitalisation Agency (Digdir) started a concept selection study to determine which solution the public sector should choose to fulfil the responsibility in eIDAS 2.0, which requires all EEA countries to provide citizens with access to an eID at a high security level.

It is uncertain what role BankID will play in a new eID regime. Regardless of the path chosen, the result will have significant implications for banks – both as owners of BankID and as key users of eID and e-signature. It is therefore important to closely follow the development.



Reference List:

Financial Supervisory Authority, "Fraud Statistics for the First Half of 2024" Released 19.11.2024.. https://www.finanstilsynet.no/publikasjoner-og-analyser/svindel-og-svindelstatistikk/2024/h1/svindelstatistikk-forste-halvar-2024/

Økokrim, "The Økokrim Model; A Preventive Process and Weighting Model" Released 09.09.2024. https://www.okokrim.no/veiledninger.6419850-565567.html

Finance Norway, "Guide on Personnel Security for the Financial Sector" Released 2024.
https://www.finansnorge.no/bransjer/arbeidsliv/arbeidsrett/veileder-i-personellsikkerhet/

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