



**FINANSTILSYNET**

THE FINANCIAL SUPERVISORY  
AUTHORITY OF NORWAY

Financial Institutions' Use of Information  
and Communications Technology (ICT)

# RISK AND VULNERABILITY ANALYSIS

## 2021





# CONTENTS

<b>1</b>	<b>SUMMARY .....</b>	<b>3</b>
<b>2</b>	<b>FINANCIAL INFRASTRUCTURE .....</b>	<b>10</b>
2.1	The importance of the financial infrastructure .....	11
2.2	The financial infrastructure is robust .....	11
2.3	Changes in the financial infrastructure .....	12
2.4	Financial Infrastructure Crisis Preparedness Committee (BFI) .....	14
2.5	The Covid-19 pandemic .....	15
2.6	Cooperation in the area of security .....	16
<b>3</b>	<b>FINANSTILSYNET'S OBSERVATIONS AND ASSESSMENTS .....</b>	<b>17</b>
3.1	Supervision of ICT and payment services.....	17
3.1.1	Governance and control .....	17
3.1.2	Emergency preparedness.....	17
3.1.3	Money laundering and terrorist financing.....	18
3.1.4	Vendor management .....	18
3.1.5	Security .....	19
3.2	Risk associated with payment services .....	19
3.3	Institutions' assessments of risk and vulnerability .....	21
3.3.1	The institutions' assessment of important factors .....	21
3.3.2	Assessments of operational risk and security risk.....	23
3.4	Risk associated with customers' use of digital services.....	25
3.4.1	Responsibilities when using payment services .....	25
3.4.2	Risk associated with digital IDs.....	25
3.4.3	ID 'wear and tear' .....	26
3.4.4	Customer information .....	27
3.5	The threat picture and cybercrime.....	27
3.5.1	Threats to the financial services sector .....	28
<b>4</b>	<b>FRAUD AND FRAUD STATISTICS .....</b>	<b>34</b>
4.1	Reporting of fraud statistics.....	34
4.2	Losses associated with the fraudulent use of payment cards .....	34
4.3	Losses linked to account transfers .....	38
4.4	Losses from social engineering fraud .....	38
4.5	Losses from fraud where the fraudster issues the payment order.....	39
<b>5</b>	<b>INCIDENT REPORTING .....</b>	<b>40</b>
5.1	Incident statistics.....	40
5.2	Security incidents .....	41
5.3	Operational incidents.....	41

5.4	Analysis of incidents as a measure of availability .....	43
5.5	Reporting of non-conformance in dedicated interfaces (APIs) in line with PSD2 .....	44
	Duty to report non-conformance in dedicated interfaces .....	45
6	<b>OUTSOURCING .....</b>	<b>46</b>
6.1	Outsourcing notifications.....	46
6.2	Vipps' planned change of operations service provider for BankID .....	47
6.3	Nets' sale of account-to-account services to Mastercard.....	47
6.4	'Cash services in store' (KIB).....	49
6.5	Licence to provide payment services.....	50
7	<b>REGULATORY CHANGES.....</b>	<b>51</b>
7.1	Guidance on outsourcing .....	51
7.2	The EBA's guidelines on ICT and security risk management.....	51
7.3	EIOPA's guidelines on outsourcing to cloud service providers.....	52
7.4	EIOPA's guidelines on ICT security and governance.....	52
7.5	ESMA's guidelines on outsourcing to cloud service providers.....	53
7.6	Proposed regulations on digital operational resilience.....	53
7.7	Proposed amendments to the Regulations on Exemption from the Notification Obligation in Connection with Outsourcing .....	54
	<b>APPENDIX 1: THE INSTITUTIONS' ASSESSMENT OF VULNERABILITY .....</b>	<b>55</b>
	<b>APPENDIX 2: BASIS FOR THE RISK MATRIX .....</b>	<b>61</b>
	<b>APPENDIX 3: FINANSTILSYNET'S MONITORING ACTIVITIES.....</b>	<b>69</b>

# 1 Summary

Norway's financial infrastructure is robust. No ICT incidents impacted financial stability in 2020. There were more security incidents in 2020 than in 2019 but fewer operational incidents. Overall, the number of ICT incidents rose slightly. Given the duration and times of the incidents, as well as the number of users affected, Finanstilsynet's assessment is that the overall availability of payment and other customer services in 2020 was satisfactory, albeit marginally poorer than in 2019.

In addition to ICT incidents, several instances of non-conformance were reported concerning account servicing payment service providers' (ASPSPs) dedicated interfaces for third-party payment service providers. The instances of non-conformance concerned both the availability of the interfaces and deficiencies in the interfaces' functionality.

Finanstilsynet heads, and is the secretariat for, the Financial Infrastructure Crisis Preparedness Committee (BFI). The committee follows up preparedness and incidents in the financial infrastructure. During the Covid-19 pandemic, Finanstilsynet and the Financial Infrastructure Crisis Preparedness Committee (BFI) have paid particular attention to entities that support important functions, including critical social functions identified by the Norwegian Directorate for Civil Protection (DSB). The key institutions in Norway's financial infrastructure generally have good emergency response plans. The actors have maintained good control over the operational situation and have quickly implemented the required measures.

The scale of cybercrime continues to increase but so far it has not resulted in major incidents in institutions in the Norwegian financial services sector. However, incidents in 2020 did reveal serious vulnerabilities in some institutions. The institutions are constantly seeking to strengthen their defences and attacks are generally averted before they can have serious consequences. 21 of the 211 ICT incidents reported in 2020 were security incidents and included both cybercrime and detected vulnerabilities, such as the SolarWinds case, where the vulnerabilities appear not to have been exploited.

Through its supervisory activities, Finanstilsynet has noted vulnerabilities that represent a risk of serious incidents in the financial services sector. For example, Finanstilsynet has pointed out weaknesses in the institutions' approach to ICT risk, agreements with service providers that did not give institutions the right to audit service providers, and the inherent risk of service providers being responsible for application development while also having access to the production environment. Inadequate monitoring of employee access rights at service providers and deficiencies in the institutions' solutions for monitoring transactions to detect money laundering and terrorist financing have also been pointed out. Finanstilsynet has also noted challenges in the governance and control of ICT activities where an institution is part of a group. In addition, weaknesses have been identified

within business continuity and crisis management, including in the preparation of business impact analyses as a basis for disaster recovery systems. Furthermore, weaknesses have been identified related to tests and exercises that do not include scenarios covering both technical interruptions and malicious attacks, and insufficient testing of transferring operations to a secondary operating location.

Finanstilsynet believes that in order to ensure the financial infrastructure's resilience, institutions should improve their ICT efforts, with an emphasis on developments in the cyberthreat picture, both to reduce the likelihood of non-conformance and to enhance ICT security.

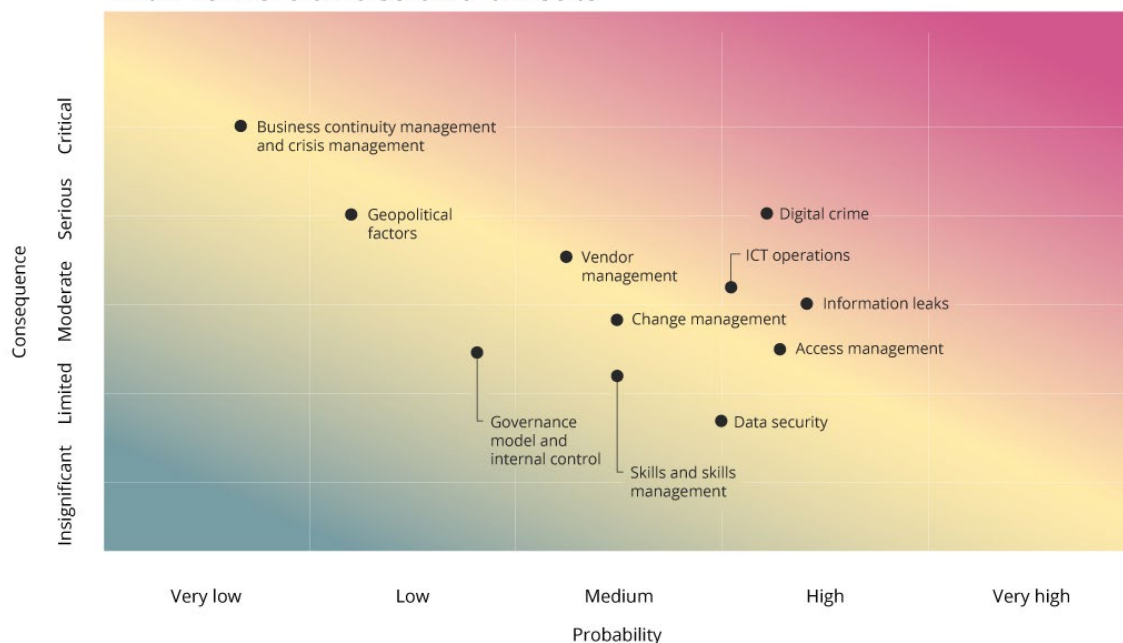
### ***Risk associated with threats and vulnerabilities in the institutions' ICT operations***

Finanstilsynet believes that vulnerabilities in the institutions' ICT operations and weaknesses in defences against cybercrime are the two most important threats related to the institutions' use of ICT. Overall, the associated risk is considered high. Information leaks are also a key threat, and the associated risk is considered moderate to high. While the risk associated with the institutions' defences against cybercrime was assessed as being marginally higher in 2020, the risk of information leaks was assessed as being slightly lower.








The risk associated with vulnerabilities in the institutions' business continuity and crisis management, geopolitical factors and access management is considered to be moderate to high. The risk associated with vulnerabilities in the institutions' vendor management, change management, governance model and internal control, skills and skills management, as well as data quality, is considered to be moderate.

The figure summarises Finanstilsynet's assessment of the most important threats and vulnerabilities in the financial services sector. The various risk areas are classified according to the probability of a serious negative incident occurring and the severity of the resulting consequences for the individual institution. The observations and assessments the classification is based on are provided in table 1.1 and discussed in more detail in chapters 3 to 6. The methodology and details on which the assessments are based are discussed in Appendix 2.

## Finanstilsynet's assessment of the risk associated with vulnerabilities and threats



Area	Vulnerabilities and threats that could represent a risk of adverse incidents (Degrees of risk, probability and consequences are stated in figure 1.1)	Trend
<b>Governance model and internal control</b>	An inadequate overview of which controls are included in the institution's internal control and how the controls should be performed, monitored and audited may result in factors that could represent an operational risk not being identified and risk-mitigating measures in line with the institution's risk tolerance not being implemented.	→
<b>Skills and skills management</b>	A scarcity of resources in Norway within operations, architecture, security and new technology, as well as inadequate skills management, may lead to institutions being unable to meet current and future skills needs. Problems and errors that occur may be difficult to resolve. Dependence on foreign assistance may increase.	→
<b>Vendor management</b>	Complex supply chains, with multiple service providers and subcontractors in the value chain, demanding cooperation models (strategic, administrative and operational) and a lack of expertise may result in weaker monitoring and oversight of critical and outsourced ICT services.	→
<b>Digital crime</b>	Inadequate security testing, security updating, training and awareness raising among employees, and insufficient monitoring of activities in its own technical infrastructure, including networks and systems, may result in criminals inflicting damage on the institution through digital attacks.	↗

<b>Information leaks</b>	Inadequate information classification, including documentation, and controls for monitoring information that is sent by email, copied to external storage devices or copied to private cloud services may cause the institution or its customers damage if unauthorised people get their hands on the information.	
<b>ICT operations</b>	Complex integration between systems from different service providers, integration between old and new systems, multiple integration points between systems, increased functionality in self-service channels, increased use of cloud services, inadequate follow-up of technical debt and insufficient monitoring of the IT environment may result in challenges in maintaining stable and secure operations.	
<b>Business continuity management and crisis management</b>	Inadequate analyses of the consequences of a crisis, inadequate training and exercises in crisis management, shortcomings in disaster recovery solutions/backup solutions and inadequate backup solutions may result in challenges for institutions when it comes to maintaining critical ICT services in the event of severe disruptions at normal operating locations.	
<b>Geopolitical factors</b>	Geopolitical factors or interruptions in communications with other countries, where service providers are prevented from maintaining deliveries of critical ICT services from abroad, may result in challenges in maintaining stable and secure operations.	
<b>Change management</b>	A fast pace of development, where quality is sacrificed at the expense of time, may result in functional errors in applications and systems, and security holes not being identified. Inadequate control of changes to operating configurations may result in interruptions to critical business processes and the institution being exposed to cybercrime.	
<b>Access management</b>	Inadequate control and monitoring of broader access rights, for employees and service provider personnel, may harm the institution as a result of deliberate or unconscious operational errors. It can also lead to information leaks.	
<b>Data quality</b>	Deficiencies or errors in data may result in analyses and controls being performed based on incorrect or insufficient information. This may include errors in credit ratings, errors in controls aimed at detecting money laundering or fraud and errors in risk assessments.	

### ***The institutions' assessment of risk***

The institutions' assessments of operational risk and security risk, as set out in their reporting and in the dialogue with the institutions, show that:

- the continued high level of complexity in the system portfolio and high technical debt entail risks in a number of areas. For example, the ICT portfolio is spread across multiple platforms and service providers, which makes vendor management more challenging.
- as in previous years, the risk associated with access to necessary expertise, especially within information security, is moderate to high.
- the risk associated with the scope of new or amended regulations that require changes to ICT systems has increased. Incident reporting shows that many of the errors were due to changes.



- half of the institutions believe that the risk of them not having an adequate overview of business-critical ICT equipment and software is moderate.
- a majority of the institutions believe that the risk of them not having an adequate overview of the various control measures in the organisation is moderate to high. Several of the institutions point out that where ICT operations are outsourced, much of the control work is also performed by the service provider.
- most of the institutions believe the risk of the transaction monitoring systems not catching all payment transactions is moderate to high.
- the institutions are seeing increasing sophistication in the cyberattacks by criminals and some institutions believe that the risk of cyberattacks remains high and that there is a need for further security testing. Several institutions also pointed out the need for further ICT security measures.
- many of the institutions have implemented or are planning measures to mitigate risks.
- a large number of the institutions see a need to implement further measures to protect users of payment services from fraud and other adverse incidents.

### ***Risk associated with customers' use of digital services***

Digitalisation is providing new and often better and cheaper services. At the same time, it is creating new risks, both for service providers and their customers.

The use of ID solutions is one of these risk areas. BankID has become a sort of 'universal key' for accessing both private and public services, without users being able to opt out of areas of use and reduce the opportunities for misuse. Due to the strong faith in ID solutions, supplementary controls are often not established to address certain risks, such as in the case of large loans. The combination of BankID being 'used everywhere, all the time' and varying login contexts entails a risk of users not being sufficiently vigilant and being tricked into fake logins.

Another risk area is payment services and services in which payment services are used, where an increasing range of functions are being automated and integrated into the payment services. It can be hard for users to maintain an overview of the consequences of changes in 'relationships' between, e.g. the payee, payee's service, payer and payment service. One example of this is parking apps where the payment card's number is linked to a car's number plate, which may later be sold without it occurring to the owner that they have to update their parking app.

Inadequate information about payment services with respect to, e.g. changes in their use may entail a risk of users being unable to complete purchases or other desired actions. One example of this was when users were unable to buy bus tickets in Ruter's app because of the requirement for strong customer authentication when paying by card online which was introduced on 1 January 2021.

### ***Losses from fraud***

Some changes were made in the reporting of fraud from the second half of 2019 due to the introduction of the revised Payment Services Directive (PSD2). Therefore, in some areas it will only be relevant to compare the figures for 2020 with the corresponding figures for the second half of 2019.

205,000 fraudulent card transactions were made in 2020, compared with 110,000 in the second half of 2019, which indicates that the scale was largely unchanged. Losses from card fraud amounted to NOK 148 million, compared with NOK 189 million in 2019, a decrease of 22 per cent. A total of just under 2.5 billion payments were made by card in 2020. Fraudulent transactions accounted for 0.008 per cent of these. The proportion was highest for cross-border transactions. Fraudulent transactions accounted for no less than 0.3 per cent of the total number of transactions with countries outside the EEA in 2020.

Losses due to account transfers, generally using online banks, amounted to NOK 355 million for the full year 2020, compared with NOK 301 million for the second half of 2019 alone. Fraud committed via social engineering, i.e. where the payer is tricked into carrying out the fraudulent transaction, accounted for NOK 250 million of this. Even though the number of cases of attempted fraud increased from 2019 to 2020, the total losses decreased by around 50 per cent. The decrease is probably a consequence of the banks intensifying their work on detecting this type of fraud and greater public awareness of social engineering fraud.

### ***Outsourcing of ICT and notifications about payment services***

In 2020, Finanstilsynet received more than 250 outsourcing notifications. Most of the notifications concerned changes relating to the service providers of the common payment infrastructure for banks, including Nets' sale of account-to-account services to Mastercard, Vipps' planned transfer of BankID's operations, and the start-up of 'cash services in store' (KIB). Extensive monitoring of the banks' notifications regarding Nets' sale of account-to-account services to Mastercard and change of operations service provider for BankID was required.

As in previous years, the outsourcing notifications show a growing trend towards the use of cloud services for both application and infrastructure services. This often entails an increase in the number of platforms the institutions have to deal with, e.g. systems at an operations service provider in combination with various cloud services. This increases the complexity and complicates the risk picture.

The quality of the institutions' analyses and assessments of risk prior to implementing ICT outsourcing appears to be improving. The quality of agreements with service providers and management's understanding of the institution's outsourcing agreements also show a positive development. Some institutions, however, need to improve their work related to outsourcing.

The applications for licences to provide payment services demonstrate that a number of institutions had an inadequate understanding of the regulations concerning outsourcing and significant weaknesses in their procedures.

### ***Finanstilsynet's monitoring of the institutions***

The main themes for supervisory activities in 2021 will be:

- the institutions' governance and control of ICT operations
- the institutions' organisation of ICT/cybersecurity work
- the security surrounding the institutions' ICT solutions
- the institutions' preparedness work and testing of business continuity and disaster recovery solutions
- the institutions' governance, control and monitoring of outsourced ICT operations
- the institutions' payment services, including compliance with the revised Payment Services Directive (PSD2), with a particular emphasis on the banks' interfaces for trusted third parties' access to customers' payment accounts
- major changes in the financial infrastructure
- the institutions' ICT solutions for detecting money laundering and terrorist financing, as well as the banks' range of cash services and cash preparedness

Finanstilsynet follows up ICT incidents at institutions. The emphasis is on the institutions identifying causes and implementing preventive measures. The threat picture for cybercrime is monitored and the institutions' preparedness work targeting digital vulnerability and digital security is reviewed.

Finanstilsynet believes that it is important that the institutions properly address the security of their services so that customers do not suffer losses. Finanstilsynet will also control that the institutions do not share their customers' data without consent and that these data do not fall into the hands of unauthorised parties.

Finanstilsynet heads, and is the secretariat for, the Financial Infrastructure Crisis Preparedness Committee (BFI). The committee follows up preparedness and incidents in the financial infrastructure. In special circumstances, such as the Covid-19 pandemic, BFI will monitor the ICT operations of the most important entities especially closely.

For further information about Finanstilsynet's monitoring of supervised institutions, see Appendix 3.

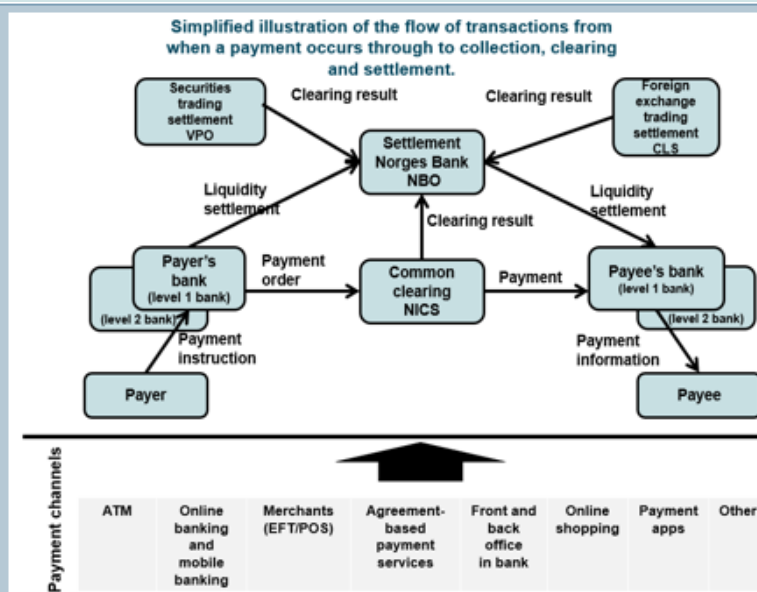
## 2 FINANCIAL INFRASTRUCTURE

The financial infrastructure consists of the payment system and the securities settlement system, as well as the Norwegian Central Securities Depository, marketplaces and key counterparties.

The payment system includes interbank systems and systems for payment services for transferring funds, with formal and standardised arrangements and common rules for processing, clearing, or settling payment transactions.

The payment system, including payment services, is regulated by legislation such as the Act relating to Payment Systems, Regulations on Payment Services Systems, and Regulations on Payment Services, as well as through the financial services sector's self-regulation administered by Finance Norway and Bits.

### Flows of transactions in the Norwegian payment system



A payment system is defined as a system based on common rules for clearing, settlement and transferring payments between two parties in a financial interaction. Legally, a distinction is made between an interbank system, which processes transactions between banks, and a payment system, which processes transactions between a customer and a bank. The figure illustrates the flow of transactions in Norwegian payment systems. The various payment channels used by customers are shown at the bottom of the figure.

Source: Finanstilsynet

The securities sector is regulated by legislation such as the Securities Trading Act, the Securities Trading Regulations and the Central Securities Depository Act. The securities sector includes actors involved in securities transactions related to equity instruments such as shares and equity certificates, including the execution of trades and related settlements.

## 2.1 The importance of the financial infrastructure

Effective, robust, and stable payment services are a fundamental prerequisite for financial stability and well-functioning markets. The financial infrastructure is designed to ensure that cash payments and transactions in financial instruments are registered, cleared and settled.

The Norwegian Directorate for Civil Protection (DSB)<sup>1</sup> has identified financial services as a critical social function. Furthermore, the Security Act states that financial stability and freedom of action, which includes the stability of the financial infrastructure and the financial markets, and society's basic functionality and the public's basic security, which includes infrastructure and objects that are crucial in the functioning of civil society, are national security interests<sup>2</sup>.

Failures by key actors in the financial services sector or in the infrastructure can have substantial societal consequences. If payments or securities trades cannot be executed or settled, important social functions will quickly stop working satisfactorily. Sensitive information going astray or breaches of the rules for processing inside information may undermine confidence in marketplaces and the financial system. If criminals gain access to large quantities of customer and account data and compromise them or make them unavailable, customers and institutions could face significant challenges. Such incidents could also impact financial stability. The societal consequences could be particularly severe if institutions operating on behalf of many or all institutions are affected. The financial services sector is also dependent on infrastructure such as power supplies and telecommunications, including networks.

Finanstilsynet and Norges Bank cooperate on the supervision and surveillance of the financial infrastructure in Norway, including through reports, risk assessments and joint supervision.

## 2.2 The financial infrastructure is robust

Finanstilsynet believes Norway's financial infrastructure is robust. There were no major ICT incidents that impacted financial stability in 2020. The operational stability of the services was satisfactory.

Overall, there were marginally more incidents in 2020 than in 2019. While there were more security incidents in 2020 than in 2019, there were fewer operational incidents. Even though slightly fewer operational incidents were reported, given the duration and times of the incidents, as well as the number of users affected, Finanstilsynet's assessment is that the availability of payment and other customer services was marginally poorer in 2020.

The reliability of the clearing and settlement systems was generally good in 2020, although there were some critical incidents. The reliability of the communication with SWIFT, the international payment system, and CLS, the international settlement system, was also good.

---

<sup>1</sup> [DSB: Vital functions in society](#)

<sup>2</sup> [Security Act Section 1-5 Definitions.](#)

The scale of cybercrime is increasing year-on-year, but so far has not resulted in major incidents in institutions in the financial services sector. Meanwhile, some serious vulnerabilities were identified in some institutions in 2020. Although vulnerabilities have been identified and serious operational failures with major consequences have occurred, systemic crises have so far been avoided.

A digital incident can occur without warning, lead to a collapse in the financial infrastructure and have far-reaching societal consequences. The institutions' ICT work, both with respect to reducing the likelihood of non-conformance and generally improving ICT security, is important for ensuring stable operational solutions. This includes business continuity solutions, disaster recovery solutions and emergency preparedness, recovery plans and ICT security work.

## 2.3 Changes in the financial infrastructure

Several significant changes were announced and implemented in the Norwegian financial infrastructure, including for key services, in 2020. Some of the changes will be realised in 2021 and 2022.

Nets<sup>3</sup>, which was a service provider for, among others, the Norwegian Interbank Clearing System (NICS), the common operational infrastructure (COI),<sup>4</sup> BankAxept, BankID and several of the banks' payment services, has sold its account-to-account services (clearing, real-time payments and payments of digital bills, including direct debit/eInvoice) to Mastercard. The changes came into force on 5 March 2021.

The remaining part of Nets, which includes Merchant Services and Issuer & eSecurity Services, Nets has signed a merger agreement with the Italian company Nexi<sup>5</sup>, with Nexi as the acquiring company. This means that other parts of the Norwegian payment infrastructure, owned by the banks up to 2014, have also seen significant changes in ownership. The changes are expected to be implemented in the second quarter of 2021. BankID, the central ID solution in the financial services sector, which is also widely used by the public sector's public services, has been operated by Nets since its inception. BankID is a part of the common operational infrastructure (COI)<sup>4</sup> that is still owned by the banks. In 2018, Vipps decided to change its service provider for the operation and administration of BankID infrastructure from Nets to DXC.<sup>6</sup> The transfer has been postponed several times and is now scheduled for completion in 2021.

---

<sup>3</sup> Nets Norge Infrastruktur AS and Nets Branch Norge, now Mastercard Payment Services Infrastructure (Norway) AS and Mastercard Payment Services Norge AS

<sup>4</sup> The common operational infrastructure (COI) includes eInvoice, the banks' joint account and address register (KAR) and solutions for instant payments. BankAxept and BankID were also included.

<sup>5</sup> Nexi S.p.A <https://www.nexi.it/en.html>

<sup>6</sup> DXC Technology Norge AS

Overall, these changes result in greater fragmentation of the ownership and operation of the financial infrastructure in Norway and may contribute to reduced concentration risk.

The banks in the Eika Alliance have used the Danish SDC's banking solutions since 2004. In 2020, the Eika Alliance entered into an agreement with TietoEVERY regarding delivery of core banking suites to the local banks in the alliance. The transition to TietoEVERY's solutions is expected to be implemented in 2022–2023. Once the transition has been completed, the proportion of Norwegian banks using TietoEVERY as their operations service provider in the financial services sector will increase significantly. This will result in higher concentration risk.

The banks that have left the Eika Alliance and formed a local bank partnership, Lokalbanksamarbeidet, will continue to purchase banking solutions from SDC. SDC is also used by some other Norwegian banks. This means that SDC will remain a key operations service provider in the Norwegian financial infrastructure.

DNB wound up its in-store postal outlet solution in 2020, meaning that it is no longer possible to carry out simple banking services, such as cash services, in Norway Post's outlets. With reference to the geographical spread of in-store postal outlets, in 2018, Finanstilsynet considered that the overall provision of cash services was satisfactory. In 2020, 'cash services in store' was established based on the use of BankAxept's infrastructure. More than 90 banks have joined the service, which to a large extent compensates for the closure of the in-store postal outlets.

The common operational infrastructure for instant payments ('Straks FOI') was established in 2013 and the solution has gradually been adopted by most banks. Before the end of 2021, the banks' instant payments will be sent directly to the clearing solution NICS Real,<sup>7</sup> and the 'Straks FOI' service from 2013 will eventually disappear.

Euronext, which also operates the stock exchanges in France, Belgium, Portugal, the Netherlands, Ireland and the UK, purchased the group Oslo Børs VPS Holding ASA<sup>8</sup> in 2019. The purchase included the regulated marketplace Oslo Børs ASA and VPS ASA. In autumn 2020, Oslo Børs adopted Euronext's trading venue solutions.

Introduction of the Own Pension Account<sup>9</sup> option resulted in a great need for interaction and information sharing between employers, employers' pension providers, any self-chosen providers, and employees for the simple transfer of pension capital certificates (PCCs) between actors in the market. A decision was therefore made to establish a pension account register as a common infrastructure for interaction. Pensjonskontoregisteret AS was established to administer operation of the pension account register.

---

<sup>7</sup> The clearing solution for instant payments in Norway

<sup>8</sup> [https://en.wikipedia.org/wiki/Oslo\\_Stock\\_Exchange](https://en.wikipedia.org/wiki/Oslo_Stock_Exchange)

<sup>9</sup> Accumulation of pension rights from defined contribution pensions in an Own Pension Account: <https://lovdata.no/dokument/NL/lov/2000-11-24-81>

## **2.4 Financial Infrastructure Crisis Preparedness Committee (BFI)**

The Financial Infrastructure Crisis Preparedness Committee (BFI)<sup>10</sup> was established in order to:

- prepare and coordinate measures for preventing and resolving crisis situations and other situations that may result in major disruptions to the financial infrastructure. In a crisis situation, the committee must notify and inform affected actors and authorities of the problems that have occurred, the potential consequences of the problems and the measures that must be implemented to resolve the problems.
- perform the necessary coordination of preparedness matters within the financial services sector. This includes, based on the civil preparedness system, coordinating the preparation and implementation of notification plans and preparedness measures in the event of national security policy crises and war.

Finanstilsynet obtains a good, broad picture of the status of the financial infrastructure through its work in BFI, which reviews severe and critical incidents that impact the infrastructure's various components.

---

<sup>10</sup> [Financial Infrastructure Crisis Preparedness Committee \(BFI\)](#)



## 2.5 The Covid-19 pandemic

Finanstilsynet has been monitoring the financial infrastructure very closely since the Covid-19 pandemic escalated in Norway. BFI held frequent meetings in March, April and May 2020, and has held more sporadic meetings since, to monitor the key institutions in Norway's financial infrastructure and how they are ensuring good, stable and secure operations, ref. the committee's mandate. The BFI meetings have contributed to the sharing of information on factors that could result in disruptions to the financial infrastructure or impact financial stability, as well as on measures that the institutions have taken or are planning to take. The actors demonstrated that they had good control over the operational situation and quickly implemented the required measures. Finanstilsynet finds this reassuring.

The institutions quickly established crisis management teams and measures were initiated in line with the development of the Covid-19 pandemic and government measures for curbing its spread. Experience shows that the key institutions in Norway's financial infrastructure have good emergency response plans that can be implemented rapidly.

Finanstilsynet and BFI have paid particular attention to entities that support critical functions, including those defined as critical social functions by the Norwegian Directorate for Civil Protection (DSB). This is the capacity to:

- i. maintain secure transfers of capital in the financial markets between national actors and to and from abroad
- ii. execute payments and other financial transactions securely
- iii. maintain the public's access to the necessary means of payment

As part of the infection control for their employees, several institutions reviewed critical roles, functions and staffing, and implemented measures such as splitting up the organisation and readying or using backup locations. The institutions' measures were revised throughout the year in accordance with the development of the pandemic. The institutions expanded capacity for linking up to systems from home and have paid particular attention to the higher risk associated with working from home during the pandemic. Permission was given to perform some functions when working from home that can normally only be reached from an office location, and strict security measures and enhanced monitoring were introduced to increase security. During the first few months, strict regimes involving restrictions or halts to changes in ICT systems were implemented, although the restrictions have since been gradually eased. Critical operations and service providers were monitored very closely. The banks' and their service providers' management of cash services was monitored. In line with the disaster recovery plans, some institutions brought operations back home from abroad and maintained, for contingency purposes, a limited amount of operational capability abroad. Several institutions reviewed their plans for the physical security of premises, including locations for ICT operations.

## 2.6 Cooperation in the area of security

Entities with critical social functions in the financial services sector

The Security Act<sup>11</sup> specifies financial stability and freedom of action as one of a number of national security interests<sup>2</sup> that must be monitored by the responsible sectoral ministry. Ministries must identify and maintain an overview of entities that are of crucial or significant importance for basic national functions (BNF) and report these to the Norwegian National Security Authority (NSM). For institutions that are of crucial importance for BNF, the responsible ministry must decide whether the Act shall fully or partly apply to the institution. No such decisions have been made in Finanstilsynet's area of responsibility. Ministries must also maintain an up-to-date overview of institutions of essential importance to BNF.

Institutions that support BNF may be at greater risk of threats from foreign intelligence services. Stricter requirements have, therefore, been set for the institutions' security work, including subcontractors and partners. Threats from foreign state actors are described in section 3.5.1.

Cooperation and information sharing result in a better understanding of risk

Cooperation on information security and sharing experiences between financial institutions in Norway through the Nordic Financial CERT (NFCERT)<sup>12</sup> help to improve knowledge about the relevant threat and risk picture, and better equip the institutions to handle cyberthreats and adverse incidents. NFCERT prepares regular threat reports. In Finanstilsynet's experience, institutions that do not take part in this partnership may be poorly equipped to manage cyberthreats and adverse incidents.

Finanstilsynet has been designated a sectoral response environment (SRE)<sup>13</sup> by the Ministry of Finance and tasked with handling ICT security incidents in that part of the financial services sector for which Finanstilsynet is responsible. Finanstilsynet performs this role in cooperation with NFCERT.

Finanstilsynet participates as a partner in the Norwegian National Cybersecurity Centre, which was established by the Norwegian National Security Authority (NSM) to strengthen the country's cyber resilience and preparedness. Participation provides Finanstilsynet with access to up-to-date knowledge about the risk picture in the area of cybersecurity. Finanstilsynet can use this centre to interact and share information with other partners and actors when managing cyberthreats and cyberattacks. Through the partnership, Finanstilsynet also participates in NSM's SIG<sup>14</sup> ICT, which is a cooperative forum for the authorities that supervise ICT security in their sector.

Finanstilsynet and Norges Bank are collaborating on the implementation and use of the framework for Threat Intelligence-Based Ethical Red-Teaming (TIBER)**Feil! Bokmerke er ikke definert.** for security testing in Norway and will establish the necessary forums for the overarching monitoring,

<sup>11</sup> Act relating to national security (Security Act)

<sup>12</sup> [Nordic Financial CERT](#)

<sup>13</sup> [Rammeverk for håndtering av IKT-hendelser NSM](#)

<sup>14</sup> SIG stands for special interest group

governance and involvement of business actors and other relevant authorities. The purpose behind TIBER-NO is to promote financial stability through increasing the resilience of critical functions in the Norwegian financial system against cyberattacks. See section 3.5.2 for further information.

## 3 FINANSTILSYNET'S OBSERVATIONS AND ASSESSMENTS

### 3.1 Supervision of ICT and payment services

In 2020, fewer inspections in which ICT and payment services were a theme were carried out than planned, largely due to the Covid-19 pandemic. Most of the inspections in 2020 were carried out on digital platforms. Five of the 18 inspections were conducted at banks, three at insurers, four at investment firms, two at debt collection agencies, one at a real estate agency, two at audit firms and one at an external accounting firm. Two of the inspections at banks were thematic AML inspections focusing on the banks' systems for electronically monitoring suspicious transactions.

#### 3.1.1 Governance and control

Through its inspections, Finanstilsynet has noted challenges relating to the institutions' governance and control of ICT activities when the institution is a part of a group and where the group is responsible for parts of ICT operations on behalf of the institutions. Being part of a group offers the institution advantages in the form of a common infrastructure and access to resources and expertise. However, Finanstilsynet notes that individual institutions in groups may not have a separate risk analysis of their ICT operations nor an IT strategy, and that there are several levels between the institution and the outsourced operations. There is a risk of roles getting mixed up and misunderstandings arising when it comes to responsibilities, roles and security levels. Irrespective of their group affiliation, institutions must ensure their own governance and control of IT activities. This must be documented through instructions and procedures that describe who should carry out what controls and tasks.

#### 3.1.2 Emergency preparedness

Inadequate emergency response plans and inadequate or insufficient testing of disaster recovery systems were identified at several inspections in 2020. Finanstilsynet noted that the basis on which

business impact analyses had been prepared was too weak and did not provide an adequate basis for establishing disaster recovery systems. It was also noted that there was no testing to ensure that communication would work as foreseen in a crisis situation, both internally in the institution and externally in relation to customers and members of trading venues.

Finanstilsynet also found that the transfer of operations to a secondary location had not been adequately tested. For some institutions, such a transfer would require a number of manual operations that are especially important to test, including to determine whether recovery time requirements could be met. As far as the trading venues in the securities sector are concerned, one should keep in mind how a transfer to a secondary location would impact the members of the trading venue.

Through its supervision, Finanstilsynet has highlighted the importance of carrying out exercises based on scenarios involving serious security incidents (cyber incidents). The institutions' emergency preparedness is intended to be a defence against both operational incidents and incidents due to cyberattacks. The consequences of the incidents may initially coincide, and it may take time before the institution knows whether the incident is operational or security related. Emergency preparedness and disaster recovery systems must cover both types of incidents. Similarly, tests and exercises must cover both scenarios where the cause proves to be technical interruptions and scenarios where the cause is a malicious attack.

### 3.1.3 Money laundering and terrorist financing

Supervision of banks' systems for monitoring suspicious transactions linked to detecting money laundering and terrorist financing in 2020 showed that the banks have established customer-specific rules. However, such rules have less effect when the risk classification of customers, which provides a basis for properly applying the rules, is inadequate. The inspections also revealed that the frequency of checks made using the customer-specific rules was not optimal and limited the effect of transaction monitoring. The risk of money laundering and terrorist financing going undetected increases when alarms are not triggered in real time.

### 3.1.4 Vendor management

At a number of inspections in 2020, Finanstilsynet found that the risk related to outsourced services did not appear to be adequately managed, including through monitoring of service providers. Agreements with service providers should make reference to the ICT Regulations and the institution's right to audit the service provider's activities. Even though audit firms and external accounting firms are not subject to the ICT Regulations, a corresponding duty applies pursuant to the Regulations on Risk Management and Internal Control.<sup>15</sup>

At a number of inspections, Finanstilsynet pointed out the increased inherent risk of giving a single service provider responsibility for application development and simultaneous access to the production

---

<sup>15</sup> See section 7.1 Guidance on outsourcing and point 6 of circular 3/2020.

environment. This must be managed through clear policies and strict controls in order to prevent adverse incidents, intentional or unintentional.

### 3.1.5 Security

#### *Access management*

As in previous years, Finanstilsynet also found weaknesses in access management in 2020. This was particularly true with respect to the institutions' monitoring of the access rights to outsourced services of service providers' employees. When ICT activities are outsourced, employees of the service provider are often assigned extended user rights. The incorrect use or misuse of extended user rights can cause great harm. Therefore, it is especially important for the institution to maintain an overview of such access rights.

#### *Security tests*

Through its supervision in 2020, Finanstilsynet observed that an increasing number of institutions were ordering security tests from third parties. The third parties are usually professional security companies. Finanstilsynet believes that this is an important contribution to the institutions' testing of their cyber resilience, but also points out that such testing should be carried out in line with recognised standards and best practice, and that the institution should have documented policies and procedures for this. The policies should, among other things, describe how and how often such tests should be carried out and the criteria for choosing the third-party provider.

Finanstilsynet also pointed out that the security level of email solutions should be improved by using recognised techniques and security solutions.

Finanstilsynet observed that institutions lack policies and procedures for raising employee awareness and instructing them on how to conceal their role and responsibilities in the institution from the outside world in order to mitigate the risk of social engineering and threats.

## 3.2 Risk associated with payment services

The public law, and to some extent the private law, part of the EU's revised Payment Services Directive (PSD2) was enacted in Norwegian law on 1 April 2019. PSD2 is designed to promote innovation and competition on equal terms and through this contribute to a well-functioning market for payment services.

The new rules define two new types of institution: payment initiation service providers and account information service providers, collectively called Third- Party Providers (TPPs). Statutory provisions have been introduced to make licences mandatory for two new payment services described as so-called 'initiation services': payment initiation services and account information services, respectively. Furthermore, rules for the secure authentication of payers, third- party payment service providers and

account servicing payment service providers (ASPSPs), as well as secure communication between them, are described in Commission Delegated Regulation (EU) 2018/389 (RTS), which has been incorporated into the Regulations on Systems for Payment Services.

Following the introduction of PSD2, Finanstilsynet has identified the following risks related to the area of payment services, including non-compliance with the new regulations:

### ***Competitive situation***

- Access to payment account: A number of banks do not offer third-party payment service providers interfaces, with the associated functionality and information, that match the functionality and information in their own user interfaces like they are required to.
- Authentication mechanisms: Banks do not give third-party payment service providers access to the same user-friendly authentication of the customer that the bank uses itself.
- Agreements: Banks have through agreements provided some third-party providers with advantages when it comes to easier authentication and better functionality in the interfaces.

### ***Potential vulnerabilities related to new services and new market entrants***

- New market entrants do not necessarily have the same level of experience as established ones. This may give rise to 'start-up risk' due to, e.g. inadequate knowledge of key legislation and expectations, less knowledge about the customer, less experience of providing payment services and challenges in relation to the operationalisation of new procedures. The requirements for obtaining a licence are designed to mitigate such vulnerabilities. After a licence has been issued, an institution is required to continuously report incidents and risk, as well as its current status.
- The rules for secure communication, authentication and supervision are the same for all actors in Europe, and institutions can operate across national borders. In order to ensure equal compliance with the regulations, the European Banking Authority (EBA) actively monitors the individual countries' supervisory authorities and their monitoring of the applicable rules and has initiated activities designed to harmonise the supervisory activities of the national authorities.
- New services increase the risk that criminals could go through third parties, which may have weaker control environments and lower levels of security in their portal, in order to circumvent the banks' security mechanisms. Ensuring the end-to-end security of a transaction (session security) has always been considered challenging. In principle, introducing third parties into a payment chain, where the user is routed from the third party to the bank for authentication, does not present new risks. Banks have a long tradition of authenticating users and merchants, including when the user is not in an online bank. What can be challenging for banks' security mechanisms is that the metadata they receive from the third party about the user may be inadequate or difficult to interpret.
- Finanstilsynet is aware that third-party payment initiation services have been used by criminals. The payer has been directed to a fake website and tricked into registering payments to a payee, where the payee's solutions also appear to have been used by the criminals.

- New market entrants entail a risk of invalid certificates, either that a certificate has been issued to a fraudster or that an expired certificate should have been revoked. Under the regulations, banks are obliged to check the certificates of third-party payment service providers. Any misuse will leave numerous traces, which means that such abuse will normally be detected. In addition, authorities will be notified of, or involved in, the process of revoking certificates. The risk of a large number of fake third-party payment service providers is considered low.
- New market entrants may have some risk related to compliance with the obligations under the Anti-Money Laundering Act if they do not receive sufficient information (such as customer names) from the bank in connection with payments.

### **3.3 Institutions' assessments of risk and vulnerability**

The institutions' assessments of risk and vulnerability are discussed below based on new annual reporting<sup>16</sup>, a cyber vulnerability survey answered by a number of institutions, and information obtained through dialogue with a number of institutions and providers of ICT services to the financial services sector.

#### **3.3.1 The institutions' assessment of important factors**

In their dialogue with Finanstilsynet, institutions and providers of ICT services highlighted numerous factors concerning ICT activities that are important for the institutions and measures implemented to mitigate risk.

ICT security resources are in high demand in the area of information security. Among other things, the institutions point out that a lack of resources can make it difficult to carry out ICT projects. It seems that the available resources prefer to work for institutions or groups that already have established security environments of a certain size.

The institutions have strengthened their internal expertise in both purchasing and monitoring outsourced ICT services. This has been prioritised because experience suggests that a high level of purchasing competence results in better deliveries and services from ICT service providers.

---

<sup>16</sup> The Regulations on Systems for Payment Services require payment service providers to report to Finanstilsynet, at least once a year, on the operational and security risks associated with the provider's payment services and give an assessment of whether the measures taken by the provider are adequate. The Regulations apply to banks, financial institutions, e-money institutions, payment institutions, account information service providers and branches of such institutions headquartered in another EEA state. Payment institutions with limited authorisation, cf. section 2-10(4) of the Financial Institutions Act, are specifically exempted from the scope of the Regulation.

Several institutions point out the importance of contact with ICT service providers on strategic, tactical and operational levels when it comes to ensuring that deliveries of ICT services meet the institutions' needs.

Institutions with multi-service provider strategies find that these are challenging with respect to both technology and security, and often require bespoke modifications that can lead to compatibility problems between different platforms.

The institutions believe it is important to have an adequate overview of one's ICT services' security architecture. Using this knowledge to set requirements for one's own organisation and to conduct risk and vulnerability analyses helps to improve general security.

Phishing remains the most common cybercrime method. There was some concern about whether the Covid-19 pandemic would result in more cybercrime but, so far, the institutions' experience does not suggest that this is the case.

The use of two-factor authentication is increasing and viewed as necessary and important for ensuring that the Active Directory accounts of users/employees are not taken over by unauthorised parties or criminals logging in from locations other than the VPN or office's network.

The institutions' experiences of cybercrime indicate that sabotage appears more harmful than espionage. In the case of sabotage, ransomware is the main tool that is used.

The criminals' attacks are becoming increasingly sophisticated, and several incidents have been noted where the infrastructure providers' systems have been compromised.

Greater use of network vulnerability scanning and barriers that prevent unauthorised apps are being used to avoid the installation of unwanted code.

The institutions emphasise that greater complexity and an ever more demanding threat picture have a negative impact on the risk picture within ICT operations. Most of the banks' ICT operations still run on mainframes, although the trend now is for new ICT services to be developed on other platforms such as Intel and Unix.

As far as information security is concerned, the institutions believe that it is important to have good processes for keeping the ICT infrastructure updated. It is important that the various components of the ICT infrastructure are documented (e.g. hardware, basic software and systems) to provide an adequate overview. Good documentation is also often considered a prerequisite for enabling recovery within the set timeframe after ICT incidents.



### 3.3.2 Assessments of operational risk and security risk

Finanstilsynet has collected assessments of operational risk and security risk from payment service providers and some other institutions. The form used contained some questions especially designed for payment service providers' reporting. For further details, please see Appendix 1.

#### ***Governance and control***

Half of the institutions believe the risk associated with not having an adequate overview of business-critical ICT hardware and software, including control over the valid configuration of ICT systems, is moderate to high. A majority of the institutions also indicate that the risk associated with not having a good enough overview of the various control measures in the business through the three lines of defence (frontline control, risk management/compliance and internal audits) is moderate to high. Several institutions explain this by saying that where ICT operations are outsourced, much of the control work is also performed by the service provider.

A large proportion of the institutions believe that the risk associated with deficiencies in security policies and in connection with risk analyses and risk assessments is moderate. For 2019, several institutions reported that this risk was rising, although for 2020, the institutions reported that the risk is stable or decreasing. The reason for this is that several institutions have introduced, or are planning, improvements in this area, including implementing an information security management system (ISMS) or improving an existing one.

A large number of the institutions believe further measures need to be taken to protect users of payment services.

#### ***Decision support***

A large number of the institutions point out that they have already taken measures designed to ensure good data quality, including through good causal analyses of errors that have occurred and continuous improvement of procedures. The risk associated with poor data quality has been reduced after it was seen as an increasing problem for the institutions in 2019. Overall, the institutions appear more convinced that their ICT systems provide adequate decision support than in 2019.

#### ***Operations and emergency preparedness***

A large majority of the institutions point out that changes in the infrastructure are implemented during low traffic periods in order to mitigate risk. Nevertheless, the institutions report that the risk associated with the complexity of the ICT systems, which contributes to a greater likelihood of operational problems, is moderate to high. The institutions attach great importance to good test procedures in order to compensate for this. Some institutions report continued high risk of cyberattacks and a need for further security testing.

The institutions have reduced the scope of changes in order to, among other things, ensure stable operations and avoid changes resulting in downtime, especially due to the extensive working from home during the Covid-19 pandemic. There has also been focus on having good fallback solutions.

The majority of the institutions say the risk associated with access to the required expertise was also moderate to high in 2020. Most of the institutions believe the risk associated with the ICT portfolio being distributed across multiple system platforms is moderate to high. A number of institutions state that they are working on moving ICT systems to cloud-based solutions to reduce complexity.

A large majority of the institutions state that the risk associated with new regulatory requirements that require changes to ICT systems is higher. This is also increasing the pressure to get these changes implemented in time. A number of institutions are managing this by contracting in external expertise or outsourcing tasks.

The institutions' incident reporting (see chapter 5) suggests that the causes of many of the adverse incidents are linked to software or infrastructure changes.

### ***Data protection***

A failure to classify data with regard to, e.g. sensitivity and confidentiality, still constitutes a risk for the institutions. However, there is a downward trend. Several institutes also point out that policies for classifying information were prepared during 2020 and that further measures linked to securing confidential information will be implemented in 2021.

The institutions that report that the risk associated with failure to protect confidential information is higher, also think that the risk associated with inadequate security mechanisms for securing data internally in their network (through network segmentation, access controls and encryption) is high.

### ***ID theft***

Most institutions believe that the risk associated with the misuse of user IDs is low and on a par with 2019. Most of the institutions also view the risk of 'card not present' and 'skimming' to be low, as they also did in 2017 and 2018. However, some institutions believe that the risk is high.

### ***Internal irregularities***

Several institutions report that the risk associated with internal irregularities, which can include both financial crimes and insider risk, is moderate. As far as financial crime perpetrated by their own employees is concerned, several institutions report that risk assessments related to irregularities are carried out regularly. Some institutions do not include irregularities in their risk assessments, instead they rely on screening and background checks prior to hiring people. However, very few institutions describe insider risk as part of their risk assessments.

It is worth noting that both the Norwegian Police Security Service (PST) and the Norwegian National Security Authority (NSM) point out that foreign state intelligence services are actively trying to recruit insiders, see section 3.5.1.2. The institutions should take account of this in their risk assessments.

### ***Money laundering***

Most of the institutions believe the risk associated with the systems for monitoring transactions failing to intercept all money laundering and terrorist financing transactions is moderate or high. For example, it can take time from when criminals start using new methods to when they are detected and blocked. Problems can also be caused by inadequate data quality, including where the various transaction types are not checked against the right parameters in transaction monitoring.

## **3.4 Risk associated with customers' use of digital services**

### **3.4.1 Responsibilities when using payment services**

Payment services, and services in which payment services are used, have embedded functionality and roles to an extent that can make it difficult for the user to foresee the consequences when the roles are changed. Changes in the relationship between the payer, payee or others must be reflected in the services. Who is responsible for ensuring that changes do not have unfortunate consequences will depend on in which relationship the changes occur.

One example of this involves a divorcee who four years after the divorce discovers an unexpected charge from a former electricity supplier. Further investigation showed that his/her former spouse had switched back to the electricity supplier they had had when they were together. The supplier revived the old agreement (direct debit) with the consequence that the wrong person was charged for the electricity delivery.

Direct debits are a register that connects payer and payee. The problem is that a service provider, in this case the electricity supplier, cannot see the account number to which the agreement is linked or who owns the account. The bank does not know who the actual electricity customer is. The only one with a full overview of the situation is the owner of the account being charged via the direct debit.

Another example of this is a car owner who registers his/her credit card number in a parking app and links it to the car's number plate. While the car has been sold, the former owner is still charged the new owner's parking charges.

The solution in both cases would be to terminate the agreements, although it is not always easy for people to remember which agreements have been signed and what they contain. Therefore, in line with the increase in automation, it would be appropriate for the account servicing payment service provider and issuing bank to regularly provide tips, advice and reminders linked to how a product works and the customers' responsibilities.

### **3.4.2 Risk associated with digital IDs**

Customers must not share login codes with others and have a duty to safeguard such codes to prevent their misuse. Issuers of such codes must facilitate solutions that safeguard the users' ability to shield

their codes. Views differ on where the boundary between the responsibilities of the customer and the issuer lies. The question has been discussed in connection with the drafting of a new Financial Contracts Act, in which issuers are assigned greater objective responsibility than before.

Issuers of security systems and codes for 26igital.g. digital IDs make decisions about the products offered. The same issuers contribute to security solutions being adopted in contexts other than their primary purpose, with the result being an ID solution that can cause great harm should it be compromised. For example, BankID has become a ‘universal key’ for accessing both private and public services. It could be argued that no one is forced to have a digital ID, although in today’s 26igitalized society, BankID has almost become a prerequisite for gaining access to, among other things, account and payment services. In practice, deciding to opt out of using BankID is difficult. The extensive use of BankID puts the owner at increased risk of criminals being able to gain access to and misuse a BankID in multiple contexts.

Little information is provided about the risk ID issuers are indirectly putting ID users at. ID users should be given greater freedom of choice when it comes to where an ID can be used. Users should have the option of setting policies/guidelines for their ID, e.g. that it can only be used for a limited set of services that does not include e.g. large loans.

Given that the vast majority of Norwegians are now at some risk of ID theft, ID issuers should be subject to especially stringent requirements. In today’s self-service society, ID issuers should establish solutions that allow users to opt out of areas of use and exercise greater control of the activity and reduce the opportunities for misuse.

In cases of misuse where serious harm has been inflicted on the victim, questions should be asked about whether the ID issuer or merchant has taken adequate measures to prevent harm. Are banks too confident in the ID that the bank (or another bank) issues so that further checks are not performed? For example, in loan cases where loans have been taken up by misusing someone else’s ID, questions could be asked about whether the bank has performed adequate additional checks, such as contacting the borrower by telephone or in some other manner.

### 3.4.3 ID ‘wear and tear’

BankID is important in today’s digital society in order to be able to log in to various financial and non-financial services via apps and web-based solutions. The login pages of various websites and apps look quite different and there is a risk that users, over time, will not be sufficiently vigilant and critical in their use of BankID. The combination of the extensive use of BankID and variation in login contexts results in a form of ‘wear and tear’ with respect to the ID and the user’s judgement. This suggests that it should be possible for users to opt out of areas of use for the ID and exercise greater control of its possible use and reduce opportunities for misuse.

### 3.4.4 Customer information

From 1 January 2021, the revised Payment Services Directive (PSD2) sets requirements for strong customer authentication in connection with payments for online shopping. Years have been spent preparing for the introduction of this. Banks and other card issuers have been consulted and involved in the preparations and have been well aware that the transition might have noticeable consequences for the customer and the customer experience in the purchasing situation. As part of the requirements, the banks and other card issuers were asked to inform their customers of the changes prior to their introduction.

Finanstilsynet reviewed a number of banks' websites in the run-up to the introduction. None of the banks that were examined had published information for customers at the time of the survey. Therefore, Finanstilsynet called on banks to inform their customers about the introduction of strong customer authentication. Subsequent inspections suggest that very few banks complied. Near the turn of the year, Finanstilsynet found that only one bank had provided its customers with information about the change.

Following the introduction of strong customer authentication, many reactions by members of the public were registered and the change was also a topic in the Norwegian parliament's questions time<sup>17</sup>. Finanstilsynet, therefore, published a description of the changes on its website together with clarifications of how the rules should be understood and what options are available.<sup>18</sup>

## 3.5 The threat picture and cybercrime

The scale of criminal attacks on financial institutions' digital systems continued to increase in 2020. At the same time, the institutions have refined their monitoring systems, their protection systems for averting attacks are better, and the attacks are usually averted before they have consequences for the institution. The institutions also have greater expertise. As described in section 2.6, good interaction in the financial services sector through NFCERT<sup>12</sup> is helping to improve knowledge about the relevant threat and risk picture, and better equip the institutions to handle cyberthreats and adverse incidents.

Over time, it has become difficult to distinguish between threats from organised crime and foreign intelligence services, and a number of criminal environments sell services to, among others, state actors. Both the Norwegian Intelligence Service (E-tjenesten) and the Norwegian Police Security Service (PST) point out that state actors are a significant threat, including through intelligence and network operations (digital mapping and sabotage of critical infrastructure), while the Norwegian National Security Authority (NSM) points out threats such as the recruitment of insiders.

---

<sup>17</sup> <https://stortinget.no/no/Saker-og-publikasjoner/Sporsmal/Skriftlige-sporsmal-og-svar/Skriftlig-sporsmal/?qid=83239>

<sup>18</sup> <https://www.finanstilsynet.no/nyhetsarkiv/nyheter/2021/mulige-unntak-fra-kravet-om-sterk-kundeautentisering-i-forbindelse-med-betaling-for-handel-pa/>

The institutions must continue their work of analysing risks and vulnerabilities, implement preventive measures, and prepare themselves to deal with attacks and the consequences of such attacks. One important job for the institutions is to ensure the protection of confidential information and raise their employees' awareness of the cyberthreat picture.

Finanstilsynet has observed major differences in the maturity of institutions when it comes to assessing the risk of inadequate data protection. For the sake of prevention, it is important that institutions analyse the assets that may be exposed. The financial infrastructure itself constitutes an asset since it supports society's basic functioning, which is defined by the Norwegian Security Act as a national security interest.<sup>2</sup>

### 3.5.1 Threats to the financial services sector

#### 3.5.1.1 Financial services sector assets exposed to threats from state actors

The financial services sector manages assets that could result in the institutions, their employees, institutions' systems, and institutions' service providers being exposed to various forms of threat from foreign actors. In its Fokus 2021<sup>19</sup> report, the Norwegian Intelligence Service describes security challenges due to a significant threat to Norwegian interests, including the financial services sector, from nations such as China and Russia in the form of intelligence and network operations.

In their preventive work it is important that the institutions map which assets<sup>20</sup> may be exposed to threats from state actors. Finanstilsynet has observed significant variations in maturity in the institutions' assessment of this risk and the risk associated with the inadequate protection of such data.

The financial infrastructure itself constitutes an asset.<sup>2</sup> Norwegian financial institutions, including their service providers, may be at risk of espionage aimed at gaining access to information in order to plan network attacks and sabotage financial infrastructure. In its threat evaluation for 2021<sup>21</sup>, the Norwegian Police Security Service (PST) points out that network operations are an important component of foreign intelligence activities targeting Norway. The network attack on the Norwegian parliament's computer systems in autumn 2020 and March 2021 are examples of the existence of a genuine threat to Norwegian security interests.

Finanstilsynet and Norges Bank are working on a draft framework for penetration testing financial institutions that will enable institutions to test their ability to withstand network attacks. See section 3.3.2 for further information.

#### 3.5.1.2 Insider recruitment and employee awareness

<sup>19</sup> Fokus 2021, <https://www.forsvaret.no/aktuelt-og-presse/publikasjoner/fokus>

<sup>20</sup> NS 5830:2012 – Societal security – Prevention of intentional undesirable actions – Terminology

<sup>21</sup> <https://www.pst.no/alle-artikler/trusselvurderinger/nasjonal-trusselvurdering-2021/>

In its threat evaluation for 2021<sup>21</sup>, the Norwegian Police Security Service (PST) states that Russian intelligence officers will spend a lot of time nurturing contact with people in Norway in order to recruit sources in various institutions. In connection with this, sensitive information about individuals, e.g. medical information obtained through network attacks on the healthcare sector, may be used to exert pressure on individuals in the financial services sector in order to gain access to information or influence decisions.

In its Risiko 2021<sup>22</sup> report, NSM describes how more intelligence services will try to recruit people through social media, e.g. by contacting them via LinkedIn. The person concerned may present him-/herself as working for a recruitment agency and gradually develop a relationship in which one is eventually asked to provide professional articles and opinion pieces for payment.

Making employees aware of possible recruitment attempts is very important since individuals are not always aware of the value state actors place on gaining access to information about systems, procedures, policy assessments and organisations. Therefore, it is important for employees to be aware of who they are sharing information with, who could acquire such information, and what communication channels can be used for sharing information. It is also important that institutions make their employees aware of this threat, as well as how employees should report the threat internally.

It is important, in order to reduce vulnerability, that the institutions limit access to sensitive information such as procedures, security measures and ICT infrastructure, and that they practise good internal logging of access and changes to such systems.

The financial services industry is a very international industry. Norwegians living in countries with authoritarian governments can be lured or pressured into working for the host country's intelligence services. Foreign nationals in Norway can also be pressured by their home country's intelligence services while working and living in Norway.

It is important to take account of human vulnerability when drawing up comprehensive threat pictures, also with respect to information security. Raising employees' awareness and preventive security measures should be part of the institutions' personnel procedures.

### **3.5.1.3 Targeted investments in Norwegian infrastructure**

The financial services sector should note that acquisitions of Norwegian companies can also constitute a threat to Norwegian interests. The Norwegian Intelligence Service describes China's targeted acquisitions abroad as a specific threat in its Fokus 2021<sup>19</sup> report. The trade war with the US underscored the vulnerability associated with being reliant on global markets, and in 2020, China prioritised technological self-sufficiency. The strategy is also to make China indispensable in international trading chains in order to resist external pressure. The Norwegian Intelligence Service

---

<sup>22</sup> <https://nsm.no/aktuelt/risiko-2021-helhetlig-sikring-mot-sammensatte-trusler>

also points out that companies that have got Chinese owners are used to make further acquisitions and that investments are channelled through third countries.

In its threat evaluation<sup>21</sup>, the Norwegian Police Security Service (PST) points out that such acquisitions can lay the groundwork for a dependency relationship and put a foreign state in a position to pressure Norwegian decision-makers to act contrary to Norwegian security interests. Such acquisitions can also provide direct access to technology used in the acquired companies. There were several examples of such conflicts of interest during the past year.<sup>23</sup>

This is a trend of which the financial services sector should also be aware. Acquisitions of smaller companies can also enable foreign states to gain insights into and access to digital infrastructure, including financial infrastructure.

#### **3.5.1.4 Phishing**

There were periods of high phishing activity during 2020, which resulted in some losses, see the discussion under section 4.5. Phishing is often targeted and tailored to the current situation. The Covid-19 pandemic provided a basis for new phishing attacks in 2020.

The following methods were some of those detected in 2020:

- **Fake identity verification requests**  
The fraudsters present themselves as being from the bank by sending a text message or email to the customer and trying to trick them into disclosing their national identity number, code, password and/or card information, which the fraudsters can then use to register payments from the customer's account.
- **Fake messages saying payment cards have been suspended**  
The customer receives a text message or email saying that a payment card has been suspended for technical or security reasons. In order to reactivate the card the customer has to click on a link and then state his/her codes and password, which the fraudsters can then use to register payments from the customer's account.
- **'Olga' scam**  
Fraudsters call elderly people and present themselves as being from the bank in order to trick them into disclosing codes, password and/or card information. The fraudsters thereafter use the information they have acquired to register payments from the customer's account(s) or use the card information online.
- **Fake messages about packages in the post**  
The number of packages being sent has increased during the Covid-19 pandemic. The customer receives a text message or email saying that a package is on its way. To track the

---

<sup>23</sup> The sale of Bergen Engines to a Russian controlled company, TMH International, was stopped <https://e24.no/naeringsliv/i/PRngK0/derfor-er-salget-av-bergen-engines-saa-kontroversielt>. The leasing company BOC Aviation, owned by the Bank of China, which in turn is wholly owned by the Chinese state, purchased stock in the airline Norwegian in 2020.



package they can click on a link where they are asked to log in using codes and a password, which the fraudsters thereafter can use to make payments from the customer's account.

- **Fraud linked to support schemes due to the Covid-19 pandemic**

Fraudsters have acquired government guaranteed loans based on fake information, ref. the Norfund case.<sup>24</sup>

- **Fraudulent debt collection**

Fraudsters have acquired lists of customers from gambling companies and send fake debt collection claims to legal debt collection agencies.

### **3.5.1.5 Vulnerabilities associated with using service providers and 'standard' software**

In its report<sup>22</sup>, NSM points out that threat actors can exploit software and service providers in order to gain access to the systems of the company's customers. Attacks on the supply chain, where the actor impacts a third party or adjoining organisation either through an attack or by exploiting vulnerabilities in software, also occur in Norway. Entities further down the value chains may also be exposed to security threats, either as targets themselves or as a link in reaching institutions higher up the value chains.

Weaknesses in networks and applications will, until they are known by the institution developing or using the solution, constitute a vulnerability in that potential attackers could learn about them and exploit them for criminal acts.

Two global security incidents discussed below, the SolarWinds case from 2020 and the Microsoft Exchange case from 2021, also impacted Norwegian institutions. Also see section 5.2.

#### **Data breach in the product SolarWinds Orion**

In December 2020, an IT security firm, FireEye, detected a data breach after the network monitoring product SolarWinds Orion was compromised after a so-called backdoor, which has been named 'Sunburst', was included in software updates distributed to customers.

The backdoor was probably installed towards the end of 2019 and provided access to compromised networks. It is assumed that this was done primarily for the purpose of extracting information. SolarWinds Orion is a very widely used product, including in the financial services sector. Finanstilsynet received reports from a number of financial institutions that themselves, or through subcontractors, use SolarWinds Orion to monitor their network infrastructure. The institutions carried out thorough checks but found no traces of the backdoor having been exploited. A number of parameters would have had to be fulfilled in order for the backdoor to become usable and it is assumed that the attackers have only exploited the backdoor in a very small number of compromised networks. Most of the known cases are in the US.

---

<sup>24</sup> <https://www.norfund.no/no/norfund-er-utsatt-for-alvorlig-svindel/>

### **Exploited vulnerability in Microsoft Exchange software**

At the beginning of March 2021, Microsoft published a so-called zero-day security update<sup>25</sup> after vulnerabilities in Microsoft Exchange Server software, which is server software mainly used for email, had been exploited. The vulnerabilities had probably been present since the end of 2020. The vulnerabilities could be exploited to extract information, as well as to plant malicious code. Exploitation of the vulnerabilities was detected in the US, EU states and other countries. According to ENISA's publication, Microsoft Exchange Vulnerabilities,<sup>26</sup> there were around 250,000 vulnerable servers on a global basis as of 5 March 2021. After patching, the number of vulnerable servers decreased to around 60,000 over the following ten days. The European Banking Authority (EBA)<sup>27</sup> was exposed to attempts to exploit the vulnerabilities, as was the Norwegian parliament.<sup>28</sup> For the individual institution, analysing whether the exploitation of such vulnerabilities has had an impact in the form of information being extracted or systems being misused in some other manner requires comprehensive work. Finanstilsynet received reports from some financial institutions that they use this type of server but that after thorough checks there were no traces of the vulnerabilities having been exploited.

### **3.5.2 TIBER-NO**

In the first half of 2020, Norges Bank and Finanstilsynet decided that, based on the positive feedback from the financial services sector and other factors, a draft framework should be prepared for use in testing cybersecurity in the Norwegian financial services sector.<sup>29</sup> The tool will be based on a framework prepared by the European Central Bank (TIBER-EU<sup>30</sup>). The draft national framework for testing cybersecurity, 'TIBER-NO', was circulated for consultation in March 2021 with a deadline for submissions of 12 May.

TIBER-NO's objective is to promote financial stability through increasing the resilience of critical functions in the Norwegian financial system to cyberattacks. TIBER-NO is not intended to be a tool for supervising or monitoring institutions and individual systems, although Finanstilsynet will be able to ask institutions for information about the results from tests they have conducted.

In order for TIBER-NO to contribute to increasing resilience to cyberattacks, and through this help to strengthen financial stability in Norway, key critical functions in the financial services sector must be tested. Therefore, it will be important for the institutions responsible for such functions to take part in TIBER-NO. In addition to covering institutions in the financial services sector, it has been suggested

---

<sup>25</sup> Zero-day security updating means updating to patch a vulnerability that has been exploited before it becomes public knowledge

<sup>26</sup> <https://www.enisa.europa.eu/news/enisa-news/statement-on-microsoft-exchange-vulnerabilities>

<sup>27</sup> [Cyberattack on the European Banking Authority - UPDATE 3 | European Banking Authority \(europa.eu\)](https://www.eba.europa.eu/en/press/updates/cyberattack-on-the-european-banking-authority-update-3)

<sup>28</sup> <https://www.stortinget.no/no/Hva-skjer-pa-Stortinget/Nyhetsarkiv/Hva-skjer-nyheter/2020-2021/stortinget-utsatt-for-it-angrep/>

<sup>29</sup> <https://www.finanstilsynet.no/en/news-archive/news/2020/framework-for-testing-cyber-resilience-tiber-no/>

<sup>30</sup> <https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html>

that TIBER-NO should facilitate the inclusion of central ICT service providers and data centres in the testing.

Finanstilsynet and Norges Bank are collaborating on the implementation and use of TIBER-NO and will establish the necessary forums for the overarching monitoring, governance and involvement of business actors and relevant authorities. Norges Bank will organise and staff a ‘TIBER-NO Cyber Team’ (TCT-NO) to manage and operationalise TIBER-NO.

### **3.5.3 The IMF’s assessment of cyber maturity in the financial services sector**

As part of the IMF’s financial sector assessment programme (FSAP) for the Norwegian financial system in 2019 and 2020, the IMF also assessed the Norwegian framework for managing cyber risk.<sup>31</sup>

The Norwegian framework for managing cyber incidents and Norway’s work on cyber risk is characterised by the IMF as advanced, although there are also areas that could be improved in order to mitigate the risk associated with cyberthreats. The IMF highlights that the system for sharing information between the authorities is well established in this field. Nevertheless, the reporting of cyber incidents should be strengthened by establishing clearer threshold values for reporting and specifying more clearly what should be reported. The IMF also recommends that supervision of the cyber risk for payment systems should be intensified, including more structured and comprehensive approaches. For further information please refer to the IMF’s reports.

---

<sup>31</sup> <https://www.imf.org/en/Publications/CR/Issues/2020/08/07/Norway-Financial-System-Stability-Assessment-Press-Release-and-Statement-by-the-Executive-49670>  
<https://www.imf.org/en/Publications/CR/Issues/2020/08/07/Norway-Financial-Sector-Assessment-Program-Technical-Note-Cybersecurity-Risk-Supervision-and-49673>

## 4 FRAUD AND FRAUD STATISTICS

### 4.1 Reporting of fraud statistics

According to section 2 of the Regulations on Systems for Payment Services, banks, financial institutions, e-money institutions, payment institutions and branches of such institutions headquartered in another EEA state must report fraud statistics to Finanstilsynet at least once a year. Finanstilsynet has decided that the institutions' reporting on fraud should take place semi-annually, which is in line with the revised Payment Services Directive (PSD2)<sup>32</sup>.

Some changes were made in the reporting of fraud following the introduction of PSD2, and these came into effect from and including the second half of 2019. 2020 was the first year in which the reporting of fraud was in line with PSD2's guidelines for both the first and second half of the year. Therefore, in some areas it will only be relevant to compare the figures for 2020 with the corresponding figures for the second half of 2019. Nevertheless, reference is made to the fraud figures for 2019, which are a combination of reporting using the earlier format defined by Bits and the new PSD2 format, where this has been possible. References are also made to previous years to some extent.

The reporting covers the total volume of both transactions and fraudulent transactions. This makes it possible to estimate fraud as a proportion of the total transaction volume. Both the value of the transactions and the number of transactions must be reported. The reporting distinguishes between domestic transactions, cross-border transactions within the EEA, and cross-border transactions outside the EEA. Furthermore, fraudulent transactions are classified into three categories based on whether the fraudster issues the payment order, changes/modifies the payment order or manipulates the payer into issuing the payment order.

### 4.2 Losses associated with the fraudulent use of payment cards

Payment card fraud is primarily fraud in which the fraudster issues the payment order. The largest subcategory is the theft of card details.

Issuing banks reported that losses due to fraudulent card payments amounted to around NOK 143 million in 2020. The losses were roughly equally split between the first and second half of the year at NOK 69.6 million and NOK 73.4 million, respectively. In addition to this come losses of NOK 4.5

---

<sup>32</sup> Article 96 no. 6, with the associated guidelines on fraud reporting: <https://eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-fraud-reporting-under-psd2>

million through the misuse of payment cards to withdraw cash, which split between the first and second half of the year at NOK 3.3 million and NOK 1.2 million, respectively. Overall, total losses through the misuse of payment cards amounted to NOK 147.5 million. This represents a decrease from 2019 of 22 per cent. It also represents a decrease in relation to the second half of 2019, when fraud was reported using the same format as in 2020.

Table 4.1 shows total losses for payment cards owned by Norwegian customers in recent years, irrespective of whether the loss was covered by the customer, the bank or the payment card company.

Table 4.1 Losses from fraudulent use of payment cards

Type of payment card fraud (amounts in NOK 1,000)	2015	2016	2017	2018	2019	2020
Total	188,659	206,503	145,591	148,732	189,147	147,602 <sup>33</sup>

Source: Finanstilsynet

Total losses in 2020 linked to fraudulent payments using payment cards amounted to 0.02 per cent of the total value of transactions. The proportion of fraud was highest for cross-border transactions outside the EEA. In this category, fraud accounted for 0.3 per cent of the value of transactions.

Losses from card payments that were not initiated electronically<sup>34</sup>, amounted to around NOK 20 million of the total losses of NOK 143 million in 2020. These are card transactions in which the payment card details have been communicated by the purchaser to the seller verbally, over the telephone, or via email. The proportion of fraud here was more than 0.1 per cent and for cross-border transactions outside the EEA it was no less than 0.6 per cent.

The proportion of fraud is higher when using payment cards for remote purchases, typically online shopping, than for in-person shopping (using a payment card in a terminal in person at the merchant's). Fraud accounts for 0.07 per cent of the total value of transactions in the case of payments without strong customer authentication and for 0.35 per cent of cross-border transactions outside the EEA.

In total, just under 2.5 billion payments were made via cards in 2020. Of these transactions, approximately 205,000 were fraudulent. This represents 0.008 per cent. Compared with the second half of 2019, where the number of fraudulent transactions was 110,000, the scale was approximately unchanged from 2019 to 2020.

The fraud rate is significantly higher for cross-border transactions than for domestic transactions. Fraud accounts for 0.3 per cent of cross-border transactions outside the EEA (three in every 1,000

<sup>33</sup> Payments and cash withdrawals by card

<sup>34</sup> The card transactions are initiated manually using the payment card details that were communicated verbally, via telephone, or via email.

transactions). For card payments initiated non-electronically, fraud accounts for 0.5 per cent (one in every 200 transactions).

The average value of a fraudulent transaction with a payment card was NOK 699, while the average value of a transaction with a payment card was NOK 372.

Table 4.2 Value of transactions and fraudulent transactions with payment cards reported by card issuer.  
 Figures for 2020

Transaction value (amounts in NOK 1,000)	Transactions in Norway	Cross-border transactions in the EEA	Cross-border transactions outside the EEA	Total transactions
<b>Card payments (issuer)</b>				
Total	731,878,546	163,656,849	11,212,122	906,747,517
- Of which fraud	6,235	103,977	32,828	143,040
Fraud in per cent	0.001	0.064	0.293	0.016
<b>Of which not initiated electronically<sup>35</sup>:</b>				
Total	9,776,674	10,271,445	1,391,905	21,440,024
- Of which fraud	437	14,867	7,899	23,203
Fraud in per cent	0.004	0.145	0.567	0.108
<b>Of which initiated electronically:</b>				
Fraudster issues the payment order, of which	5,806	81,001	23,182	109,989
- Lost or stolen card	1,400	2,802	810	5,012
- Card not received	706	1,351	121	2,178
- Counterfeit card	159	554	1,104	1,817
- Theft of card details	1,946	61,063	18,377	81,386
- Other	1,595	15,231	2,770	19,596
Fraudster changes or modifies the payment order	146	908	142	1,196
Fraudster manipulates the payer into making a card payment	117	7,435	1,616	9,168
<b>Remote payment (e-commerce)</b>				
Total	69,648,557	98,666,610	6,201,971	174,517,138
- Of which fraud	2,850	82,446	21,788	107,084
Fraud in per cent	0.004	0.084	0.351	0.061
<b>In-person payment</b>				

<sup>35</sup> The card transactions are initiated manually using the payment card details that were communicated verbally, via telephone, or via email.

(at a physical merchant)				
Total	652,453,314	54.718.793	3,618,245	710,790,352
- Of which fraud	2,943	6,664	3,142	12,749
Fraud in per cent	0.000	0.012	0.087	0.002
<b>Remote payment without strong customer authentication (SCA)</b>				
Total	44,748,384	56,725,513	4,781,138	106,255,035
- Of which fraud	2,399	56,027	16,698	75,124
Fraud in per cent	0.005	0.099	0.349	0.070

Sources: Finanstilsynet and Bits AS

Table 4.3 Number of transactions and fraudulent transactions with payment cards reported by card issuers in 2020

Number of cases	Transactions in Norway	Cross-border transactions in the EEA	Cross-border transactions outside the EEA	Total
<b>Total</b>	1,986,894,640	433,122,094	20,470,498	2,440,487,232
Of which fraud	9,711	140,576	54,318	204,605
Fraud in per cent	0.001	0.032	<b>0.265</b>	0.008
<b>Not initiated electronically:</b>	19,340,195	42,062,726	2,591,058	63,993,979
- Of which fraud	935	15,012	13,560	29,507
Fraud in per cent	0.005	0.036	<b>0.523</b>	0.046
<b>Remote payment</b>	194,433,015	236,867,520	12,394,085	443,694,620
- Of which fraud	3,751	116,485	37,934	158,170
Fraud in per cent	0.002	0.049	<b>0.306</b>	0.036
<b>In-person payment</b>	1,773,121,430	154,191,848	5,485,355	1,932,798,633
- Of which fraud	5,015	9,079	2,824	16,918
Fraud in per cent	0.000	0.006	0.052	0.000

Source: Finanstilsynet

## 4.3 Losses linked to account transfers

Fraud involving account transfers is fraud where the fraudster issues or modifies the payment or manipulates the payer to issue the payment order.

Table 4.4 Transactions and fraudulent transactions – account transfers (online banking, etc.) 2020

Account transfers initiated electronically (amounts in NOK 1,000)	Transactions in Norway	Cross-border transactions in the EEA	Cross-border transactions outside the EEA	Total	Fraud (%)
Total	189,996,583,878	27,582,143,072	5,972,119,064	223,550,846,014	
- Of which fraud	118,672	97,570	139,245	355,487	0.00016
Of which different types of fraud:					
- Fraudster issues the payment order	36,777	12,758	6,888	56,423	
- Fraudster modifies the payment order	721	34,456	11,891	12,363	
- Fraudster manipulates the payer into issuing the payment order	81,155	49,019	120,467	285,344	

Source: Finanstilsynet

Losses due to account transfers, generally using online banks, amounted to around NOK 355 million in 2020, compared with NOK 301 million for the second half of 2019. This indicates a significant fall in relation to the second half of 2019. The figures show total losses for online banking fraud for Norwegian customers in recent years, irrespective of whether the loss was covered by the customer or the bank.

## 4.4 Losses from social engineering fraud

The reported figures for social engineering fraud, i.e. where the fraudster manipulates the payer into carrying out a transaction, amounted to around NOK 295 million for 2020, NOK 285 million of which involved online bank transactions and NOK 10 million payment cards. This is on a par with 2018, where reported losses were just under NOK 300 million, although considerably lower than reported figures for 2019, which indicated losses of more than NOK 500 million.

The scale of social engineering fraud is uncertain because payers must bear the losses themselves and many instances of fraud of this type are probably not reported to banks. It is assumed that the actual losses are substantially higher than the reported losses. The defrauded customers often contact their bank to ask them to stop transactions and reverse the transfer of funds. Banks also alert customers when, based on their knowledge of a customer, they identify repeated transactions that are extraordinary for that customer.



Based on figures from the largest banks, Finanstilsynet is aware that the number of attempted cases of social engineering fraud is steadily increasing. The sum involved in attempted fraud (attack amount) is many times greater than the customers' actual losses. The banks are preventing an ever-larger proportion of attempted fraud and the percentage share of the attack amount that results in actual losses is falling. The fact that banks are stopping an increasing proportion of the attempts is probably the main reason why the number of reported fraud cases for 2020 is lower than in 2019. It is also assumed that greater public awareness of social engineering fraud is contributing to the fall.

Social engineering fraud still appears to be the most profitable method for criminals. The type of social engineering criminals consider the most profitable is changing. Reporting in line with PSD2's guidelines does not distinguish between various types of social engineering, although Finanstilsynet had received figures for subcategories from some of the larger banks. In 2020, the highest losses due to fraud involved changing payee accounts and investments in fake companies.

## **4.5 Losses from fraud where the fraudster issues the payment order**

In the PSD2 reporting, social engineering is defined as payment transactions where the fraudster manipulates the payer into carrying out a transaction. However, phishing scams also include some elements of social engineering. In phishing, the payer is tricked into disclosing contact and payment information that the fraudster uses to issue a payment order on behalf of the payer. In PSD2 reporting, this is reported as fraud where the fraudster issues the payment order. The losses in this category in 2020 were NOK 56 million for transactions in online banks and NOK 110 million for payment cards.

## 5 Incident reporting

### 5.1 Incident statistics

Overall, there were marginally more incidents in 2020 than in 2019. While there were more security incidents in 2020 than in 2019, there were fewer operational incidents. 21 of the 211 reported incidents were security incidents (10 per cent). Finanstilsynet did not observe the Covid-19 pandemic having any influence on the pattern of incidents in 2020.

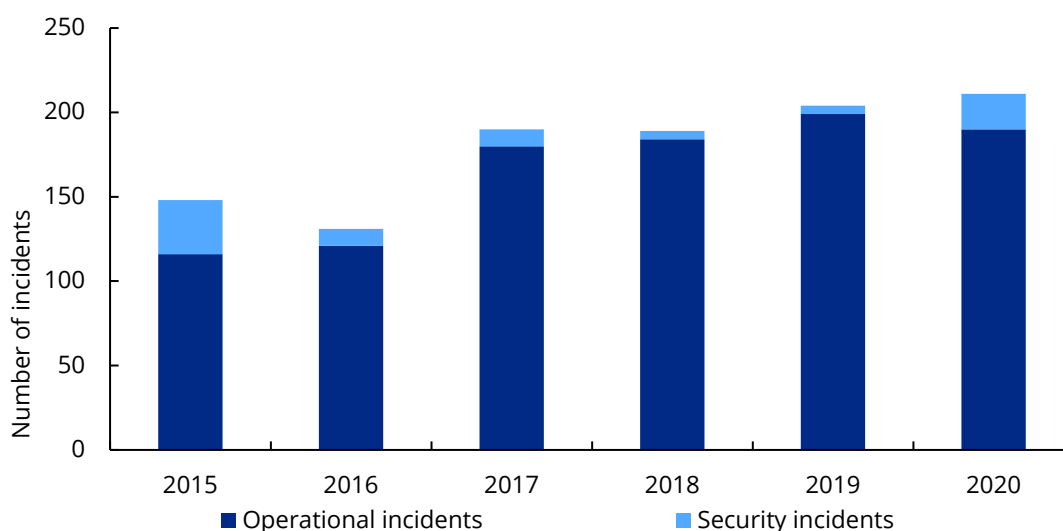


Table 5.1 Number of incidents reported

Year	Operational incidents	Security incidents	Total number of incidents
2015	116	32	148
2016	121	10	131
2017	180	10	190
2018	184	5	189
2019	200	6	206
2020	190	21	211

Source: Finanstilsynet

## 5.2 Security incidents

Most security incidents involved cybercrime, including crime for financial gain. Ten of the security incidents reported to Finanstilsynet in 2020 involved DDoS attacks, where some of the reports concerned DDoS attacks on common service providers. Two different variants of attacks using infected software were reported in 2020, at the start and at the end of the year, respectively. One of them was the SolarWinds case in 2020; for further details see section 3.3.1.5. The attacks made it possible to get inside a network and destroy or extract data. None of the institutions that reported these incidents found any signs that harm had occurred. Reports were also received on the exploitation of vulnerabilities in self-developed applications that were identified by the institution's customers, extensive phishing campaigns involving the misuse of the institution's name and logo, and fake password distribution.

In addition to these security incidents, Finanstilsynet received four reports where the institutions themselves had identified vulnerabilities through security tests or similar without these having been exploited.

## 5.3 Operational incidents

### *Reporting of incidents by banks and payment institutions*

In 2020, Finanstilsynet received the highest number of incident reports from banks and payment institutions. Most of the reports were to do with operational incidents. These are incidents that generally impact payment services in different ways, usually in the form of the payment services being unavailable, although they can also involve delays and errors in payments. Operational incidents predominantly occur on Mondays following maintenance and upgrades at weekends. Finanstilsynet classified several of the operational incidents as very serious in 2020. The incident that received most attention was an operational incident in DNB in June that caused several days' delay in salary and holiday allowance payments to a large number of customers. Nets also experienced an operational incident in July that affected many institutions' payment services for several hours one afternoon/evening. Other incidents also occurred at common service providers in the spring and summer of 2020 that resulted in repeated interruptions to payments services. Two incidents involving the non-delivery of data to debt registers were reported.

### *Reporting of incidents related to systems for detecting money laundering and terrorist financing*

The Anti-Money Laundering Act requires banks, mortgage companies and finance companies to have electronic monitoring systems (AML systems) in place to detect potential indications of money laundering and terrorist financing. Finanstilsynet considers errors and non-conformance in these systems serious incidents that must be reported in line with the ICT Regulations. Finanstilsynet received eight incident reports about various types of non-conformance in AML systems in 2020. Several of the instances of non-conformance in 2020 involved the incorrect processing of international

transactions that resulted in them being inadequately monitored. There are a limited number of AML system providers, meaning that a system error at one of the providers can impact multiple institutions.

### ***Reporting from debt collection agencies***

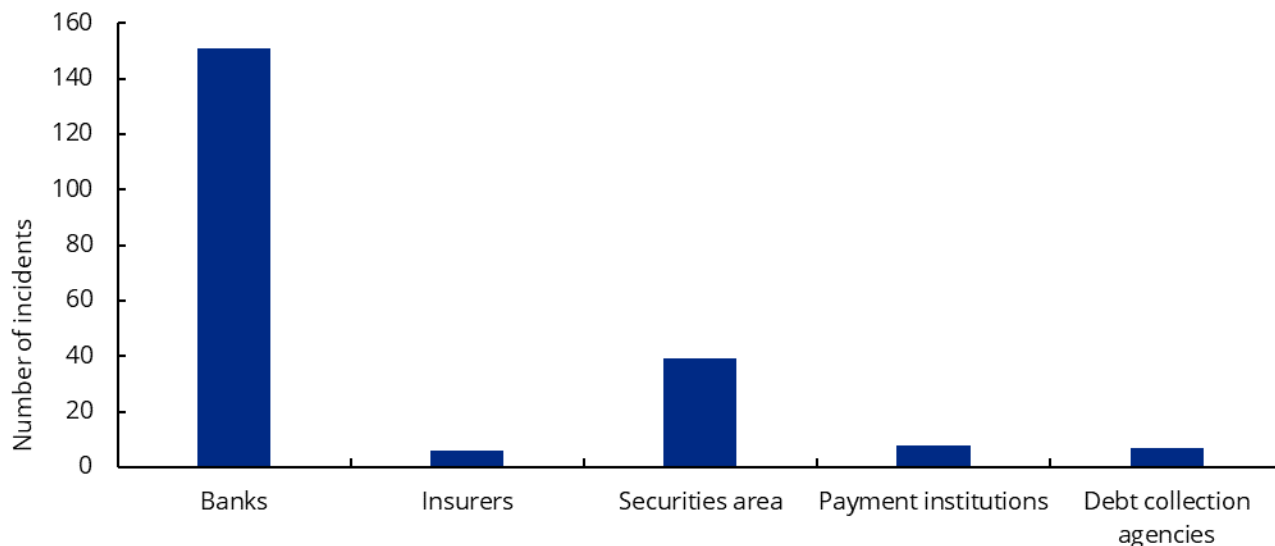
Debt collection agencies reported seven incidents in 2020, which is more than in previous years. Finanstilsynet has previously received relatively few reports of incidents from debt collection agencies and has questioned whether the sector's understanding of the duty to report pursuant to the ICT Regulations is good enough. In 2020, Finanstilsynet sent letters about this to the debt collection agencies with examples of incidents that must be reported, and the number of reports has subsequently increased. Finanstilsynet considers system interruptions and system errors that cause delays and deviations from statutory deadlines for contact points with the debtors in the payment process, as particularly serious incidents.

### ***Reporting from the securities area***

In 2020, Finanstilsynet received 15 reports from central trading venues and infrastructure entities. A few incidents reduced access, although there were no prolonged interruptions linked to trading venues in 2020. Finanstilsynet received 22 incident reports from investment firms and management companies, most of which described operational problems with reduced access to web-based equities brokerage or a lack of audio recordings. Finanstilsynet also received two reports related to the transfer of Oslo Børs' trading system to Euronext. These two reports dealt with problems that had relatively little impact on the services.

### ***Reporting from insurers***

Finanstilsynet received six reports from insurers in 2020. These involved breaches of confidentiality with the exposure of customer data to other customers and breaches of integrity whereby insurance certificates were sent to customers who had been refused insurance.



## 5.4 Analysis of incidents as a measure of availability

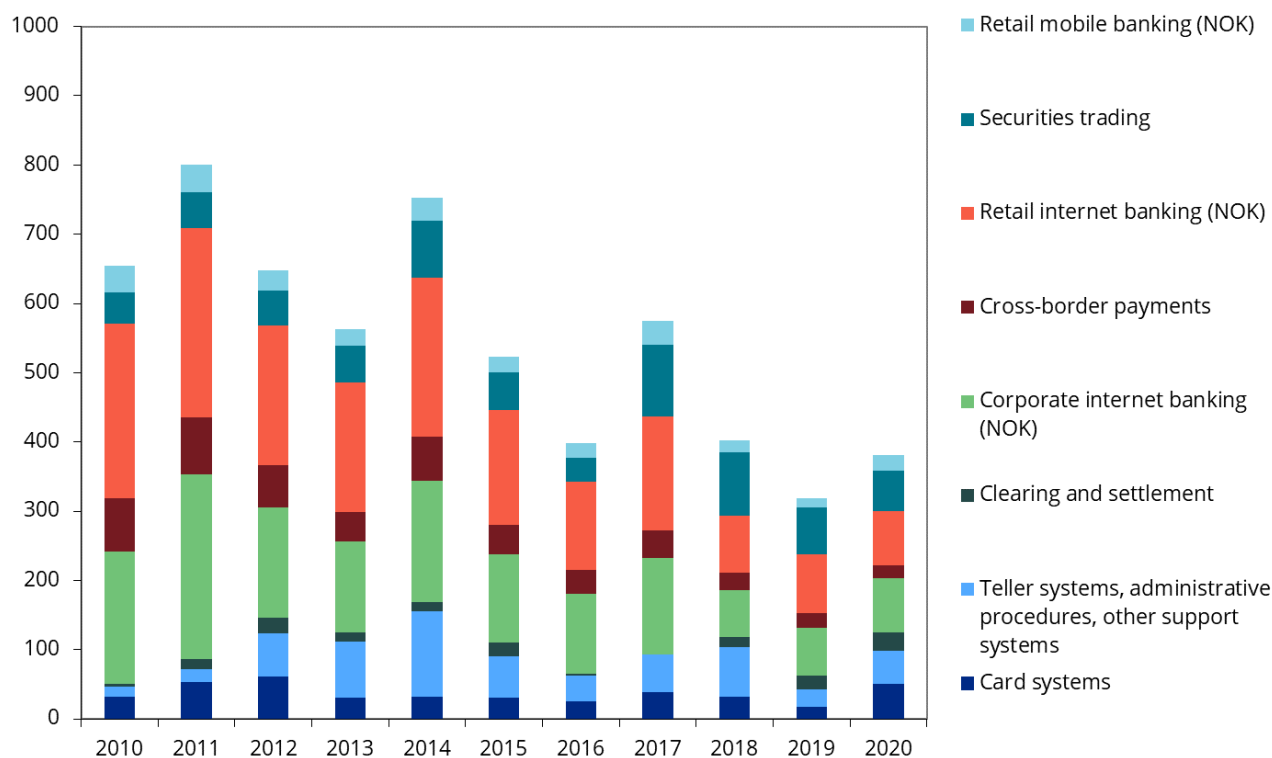
The reported incidents were of varying degrees of severity. For incidents that caused reduced availability, Finanstilsynet has considered the duration of the disruption, the number of institutions affected, the number of customers affected, and whether there are alternative services that can meet customer needs (such as when the mobile banking service is unavailable, but the online bank is available). The incidents are weighted on the basis of the number of affected users, incident duration, time, and access to replacement services. The findings are collated in a time series so that the trend can be monitored over time.

Figure 5.3 shows that payment systems and other customer services were less available to customers in 2020 than in 2019, but more than in previous years. Overall, service availability was considered satisfactory in 2020. The scale on the y-axis is an index based on the weighting of each incident. A lower index value indicates fewer business disruptions with consequences for users.

Figure 5.3 ‘Service not available’ incidents weighted by impact

The following has been assessed:

number of affected users, duration of the incident, any harm inflicted on customers as a consequence of the incident, access to alternative services



Some incidents were serious and impacted a large number of users. Several of the incidents were related to the category 'Card systems', which saw reduced availability in 2020.

The category 'Clearing and settlement' includes all incidents that can affect payments after the customer has approved them such as delays, double reservations and double entries. There were more errors in this category than there has been in previous years.

Incidents linked to the category 'Securities trading' include incidents relating to, e.g. online equities trading solutions and incidents in the Norwegian Central Securities Depository (VPS). The category 'Retail mobile banking (NOK)' includes apps and online mobile banks. This category is weighted up somewhat because the use of PC-based banking is falling and mobile-based banking is rising. Correspondingly, incidents related to the category 'PC banking' has been weighted down somewhat.

The category 'Teller systems, administrative procedures, other support systems' also covers reporting systems. The reduction in availability in this category was due to incidents that had a wide-ranging impact on the bank's systems.

## **5.5 Reporting of non-conformance in dedicated interfaces (APIs) in line with PSD2**

Finanstilsynet received several reports of non-conformance related to dedicated interfaces in 2020. Most of these were reported by third-party payment service providers and just a few were reported by account servicing payment service providers. The instances of non-conformance were related to both a lack of access to the interfaces, prolonged in some cases, and deficiencies in the interfaces' functionality.

Where the non-conformance was not remedied within a reasonable period of time after the third-party providers had reported the non-conformance to account servicing payment service providers, Finanstilsynet followed up the non-conformance with the account servicing payment service providers.

In several instances of non-conformance, the account servicing payment service provider did not inform the third-party provider about the non-conformance, reestablishment measures or possible alternative solutions.

## Duty to report non-conformance in dedicated interfaces

Payment service providers, both account servicing payment service providers and providers of the new payment services, payment initiation and account information, must immediately report problems concerning dedicated interfaces (APIs) to Finanstilsynet.<sup>36</sup>

Furthermore, in the event of such non-conformance, account servicing payment service providers must inform third-party providers about the non-conformance, reestablishment measures and possible alternative solutions.

The threshold for reporting problems concerning dedicated interfaces must be lower than for incidents pursuant to the ICT Regulations.

Payment service providers must establish their own procedures for fulfilling their regulatory duties.

---

<sup>36</sup> <https://www.finanstilsynet.no/tema/psd-2---eus-reviderte-betalingstjenestedirektiv/psd2---presiseringer-og-avklaringer-om-regelverket/>

## 6 Outsourcing

### 6.1 Outsourcing notifications

In 2020, Finanstilsynet received more than 250 outsourcing notifications. Finanstilsynet also assessed outsourcing agreements for ICT operations when considering licence applications.

Most of the outsourcing notifications were related to providers of the common payment infrastructure for banks, including Nets' sale of account-to-account services to Mastercard and the planned transfer of BankID's operations. Extensive follow-up was required of banks' notifications concerning Nets' sale of account-to-account services to Mastercard, as well as Vipps' planned change of operations service provider for BankID. A considerable number of notifications were also received in connection with the start-up of 'cash services in store' (KIB). Some of the notifications came from cooperating groups of banks on behalf of several banks. Of the other reports, 36 were from insurers and 13 from finance companies.

The notifications received by Finanstilsynet have become more comprehensive and detailed. The quality of the institutions' analyses and assessments of risk prior to implementing ICT outsourcing appears to be improving. The quality of agreements with service providers and management's understanding of the institution's outsourcing agreements also show a positive development. However, not all new institutions are equally familiar with the regulations. Finanstilsynet has also received notifications in which the institutions regard a processor agreement as adequate as an outsourcing agreement when it comes to the right to access and supervision under the regulations. This is not the case.

In recent years, outsourcing notifications have indicated a trend towards the use of cloud services, for both application and infrastructure services. Outsourcing also means institutions have to deal with more platforms, e.g. systems at an operations service provider in combination with various cloud systems. This results in greater complexity and a more complicated risk picture. At the same time, the use of cloud services can also have a number of positive effects such as better ICT security and cheaper services.

The institutions have a responsibility to ensure that ICT operations, including outsourced services, satisfy all of the requirements set out in the ICT Regulations, cf. section 12 of the Regulations. Other sector legislation may also include detailed rules on outsourcing. The institutions must establish service provider agreements that comply with the regulations and ensure that the service provider and any subcontractors provide ICT services in line with these requirements. Finanstilsynet gains insights into the institutions' outsourcing agreements when considering outsourcing notifications, cf.



section 4(c)<sup>37</sup> of the Financial Institutions Act, and processing licence applications, and as part of its supervisory activities.

## **6.2 Vipps' planned change of operations service provider for BankID**

Vipps, as the owner of BankID, is planning to transfer the operation of BankID from the current operations service provider Nets to DXC, also see section 2.3. In connection with the change, Finanstilsynet has received and considered change notifications from the banks.

The extensive use of BankID within both the financial services sector and public services has resulted in the service being designated critical to society. The ICT Regulations require institutions in the financial services sector that purchase BankID services to have an insight into and understanding of the risk associated with the outsourced service. While BankID may be viewed as a common service, the individual institutions that purchase the service are responsible for the associated risk and its proper operation.

Finanstilsynet has asked both Vipps and the banks that purchase BankID services to conduct risk and vulnerability analyses. Finanstilsynet has also followed up to ensure that both Vipps and the banks have contingency plans in place in case the BankID service does not function as planned in connection with the transfer operation.

Given the significant delays in completing the transfer project, Finanstilsynet has ensured that Vipps has conducted thorough assessments of the operations service provider and that Vipps will monitor the deliveries closely once the transfer has been completed.

## **6.3 Nets' sale of account-to-account services to Mastercard**

In 2019, Mastercard signed an agreement to purchase Nets' account-to-account services business area, which includes real-time payments (COI instant payments), digital invoice payments (eInvoice/direct debit) and interbank clearing (NICS), also see section 2.3. The sale included the operations of the Norwegian company Nets Norge Infrastruktur AS and parts of the operations of Nets Branch Norway (NUF). The purchasers of the business areas were the Mastercard companies Mastercard Payment Services Infrastructure (Norway) AS (MPSI) and Mastercard Payment Services Norway AS (MPSN), respectively.

The transfer to Mastercard resulted in changes to the banks' outsourcing situation with respect to both their direct purchases of payment services and their entry into agreements on a common operational

---

<sup>37</sup> Finanstilsynet has proposed, and circulated for consultation, changes to the duty to notify, also see section 7.7.

infrastructure (COI) signed by Bits AS.<sup>38</sup> The banks were, therefore, obliged to report the changes to their outsourcing situation to Finanstilsynet.

From and including autumn 2019 up to and including January 2021, Finanstilsynet received and considered advance notifications and ordinary notifications concerning changes to outsourcing agreements. A total of 15 banks did not notify Finanstilsynet and were reminded to do so by Finanstilsynet in summer 2020.

In connection with the consideration of outsourcing notifications, Finanstilsynet has had an extensive dialogue with a series of individual banks and banking alliances, as well as with Bits AS, concerning the COI agreements. Finanstilsynet has also had a dialogue with nine branches of Norwegian banks.

Finanstilsynet's consideration of the banks' notifications identified major differences in the banks' internal processes for managing ICT outsourcing agreements.

Many of the notifications contained good risk assessments of the new service provider, including assessments of the service provider's owners, country risk, and specific risk assessments of the new contractual relationship with a specification of risk-mitigating measures. The notifications also contained information about the operating environment of the ICT systems covered by the agreement.

Finanstilsynet's consideration process also revealed that several of the banks had not adequately ensured fulfilment of the ICT Regulations' requirements concerning board consideration or assessed whether the agreement fulfilled the ICT Regulations' requirements concerning the content of the agreement. A number of banks had also not complied with the Financial Supervision Act's duty to report the signing of agreements.

The deficiencies that were uncovered resulted in extensive guidance work for Finanstilsynet, and the banks in question had to make extensive revisions to their internal procedures, including procedures for board consideration, conduct risk assessments and ensure board consideration of the bank's risk assessment and agreements, as well as follow up the dialogue with Finanstilsynet. The banks were also asked to submit further supplementary documentation such as:

- risk assessments of services providers and subcontractors, as well as the new agreements, with a specification of risk-mitigating measures. An assessment of whether the agreement ensured that the bank had control over the operation of the service, and whether the bank had ensured that it would be notified in the event of services being outsourced to subcontractors, including intragroup outsourcing.
- board consideration of the risk assessments and agreements.

---

<sup>38</sup> <https://www.bits.no/>

- quality assurance that section 12 of the ICT Regulations was addressed in the agreement, including that the outsourcing agreement ensures that a service provider's subcontractors are obliged to comply with the regulatory requirements.
- exit and emergency response plans and assessments of whether these should contain requirements that ensure that the services covered by the agreement can be operated from Norway if necessary.

Finanstilsynet had, as part of its consideration process, questions concerning several banks' follow-up of the new service provider's temporary outsourcing of operations and the management of any future changes in operating conditions, including control over the new service provider's possible future intragroup outsourcing of operations. Several of these were asked to revise/clarify agreement annexes that provide information about the service provider's subcontractors.

Most of the notifications Finanstilsynet received lacked information about the banks' COI agreements, with references to the fact that Bits AS managed this agreement through a separate process. This revealed, among other things, deficiencies in the banks' procedures, deficiencies in the banks' own risk assessments and a lack of board consideration of the COI agreements. Finanstilsynet's consideration and follow-up of the banks' notifications resulted in several banks changing their procedures and processes, which is reflected in subsequent ICT outsourcing notifications.

In its dialogue with Bits AS and the banks, Finanstilsynet has pointed out that Norwegian banks' previous exclusive rights to the Norwegian payment systems ended with the establishment of the new COI framework agreement and that this could potentially weaken Norwegian influence on the solutions.

## **6.4 'Cash services in store' (KIB)**

In 2020, Vipps, via BankAxept, established 'cash services in store' (KIB) in cooperation with Norwegian banks, also see section 2.3. The service was established in order to comply with the Financial Institutions Act's requirement that 'Banks shall in accordance with customers' expectations and needs accept cash from customers and make deposits available to customers in the form of cash'. This service partly replaces the agreement between DNB and Norway Post on in-store banking services, which ended in September 2020.

More than 90 banks have joined the partnership and offer the service to their customers.<sup>39</sup> 'Cash services in store' are currently available in NorgesGruppen's grocery stores and make it possible to withdraw and deposit cash in a total of 1,431 grocery stores, which represents a coverage ratio of 98 per cent of Norway's population.

---

<sup>39</sup> <https://vipps.no/produkter-og-tjenester/privat/kontanter/kontanttjenester-i-butikk/>

During the establishment of the service, Finanstilsynet received and considered outsourcing notifications from banks about adopting the service, where the notifications covered the bank's role as the account holding and/or merchant's bank. During its consideration of the notifications, Finanstilsynet asked the banks to confirm that a series of conditions related to the outsourcing had been addressed prior to start-up. Finanstilsynet attached particular importance to ensuring that the notifications had been considered and approved by the bank's board and that the account holding bank had implemented AML monitoring of cash transactions in order to comply with the anti-money laundering legislation's requirements and that AML training of parties involved in providing the cash services had been established and carried out.

## **6.5 Licence to provide payment services**

Finanstilsynet also received six applications for a licence to provide payment services in 2020. The legislation stipulates a strict requirement that the institutions must have well-documented procedures in areas related to ICT and payment services. Although some of the institutions had good procedures in place in areas related to ICT and payment services, there were also some institutors that had an inadequate understanding of the legislation, significant weaknesses in their procedures and a need for extensive guidance. The observations showed that the requirements designed to help mitigate the risk associated with payment service providers are important.

## 7. Regulatory changes

The following describes approved or proposed new regulations and policies that impose new or changed requirements concerning institutions' ICT-related work, as well as guidelines describing what Finanstilsynet expects of the institutions.

### 7.1 Guidance on outsourcing

On 2 October 2020, Finanstilsynet published a guidance on outsourcing, including the outsourcing of ICT operations, see circular 3/2020.<sup>40</sup> The circular provides guidance on what is considered to be outsourcing, restrictions on the right to enter into outsourcing arrangements and how supervised institutions must identify, assess and manage the risks associated with outsourcing. The circular also refers to Section 4c of the Financial Supervision Act on outsourcing and the obligation to notify Finanstilsynet.

The circular annulled circular 14/2010 on the outsourcing of banks' ICT duties.

### 7.2 The EBA's guidelines on ICT and security risk management

The EBA published Guidelines on ICT and Security Risk Management on 28 November 2019<sup>41</sup> and these came into effect on 30 June 2020. Finanstilsynet has confirmed that the guidelines will be followed in Norway and has updated its supervisory practice and requirements for considering ICT security risks in line with the new guidelines.

The guidelines target banks, payment institutions and electronic money institutions and include detailed requirements for how institutions can protect themselves against the ICT security risk to which they are exposed. At an overarching level, the ICT Regulations have regulated the areas covered by the guidelines since 2003. One of the main objectives of the guidelines is to clarify the requirements for how ICT security risks should be managed in institutions.

---

<sup>40</sup> <https://www.finanstilsynet.no/nyhetsarkiv/rundskriv/2020/veiledning-om-utkontraktering/>

<sup>41</sup> <https://www.finanstilsynet.no/nyhetsarkiv/nyheter/2020/eba-har-fastsatt-retningslinjer-om-ikt-sikkerhet-og-risiko/>

### **7.3 EIOPA's guidelines on outsourcing to cloud service providers**

EIOPA published Guidelines on Outsourcing to Cloud Service Providers<sup>42</sup> on 6 February 2020. The guidelines came into effect on 1 January 2021. Finanstilsynet has confirmed that the guidelines will be followed in Norway and has updated its supervisory practice in line with the new guidelines.

The guidelines are aimed at insurers and will apply to all outsourcing agreements with cloud service providers that are entered into or amended from 1 January 2021 onwards. Existing outsourcing agreements for critical/important tasks must be adapted to the new guidelines by 31 December 2022. Finanstilsynet must be notified if an institution cannot adapt existing agreements to the new guidelines by the deadline. The notification must include a timetable of planned measures for bringing the outsourcing relationship into line with the new guidelines, or a winding-up strategy for terminating the outsourcing agreement.

The objective of the guidelines is, among other things, to clarify the requirements for outsourcing to cloud service providers and conditions related to cloud services for customers and service providers in order to avoid regulatory arbitrage (institutions must be subject to the same regulatory requirements for services in all EU/EEA states).

### **7.4 EIOPA's guidelines on ICT security and governance**

EIOPA published Guidelines on Information and Communication Technology Security and Governance<sup>43</sup> on 12 October 2020. The guidelines will apply from 1 July 2021. Finanstilsynet assumes that the guidelines will be followed in Norway and will update its supervisory practice in line with the new guidelines.

The guidelines are aimed at insurers and include detailed requirements for how institutions should protect themselves against the ICT security risk to which they are exposed. At an overarching level, the ICT Regulations have regulated the areas covered by the guidelines since 2003 and the guidelines will provide useful elaboration on the provisions of the ICT Regulations. The main objectives of the guidelines are to clarify the requirements for the consideration of ICT security risks in the institutions, set minimum requirements for expected levels of information and cybersecurity and avoid potential regulatory arbitrage (institutions must be subject to the same regulatory requirements for the services in all EU/EEA states).

---

<sup>42</sup> <https://www.finanstilsynet.no/nyhetsarkiv/nyheter/2020/nye-retningslinjer-fra-eiopa-for-utkontraktering-til-skyleverandorer/>

<sup>43</sup> [https://www.eiopa.europa.eu/content/eiopa-finalises-guidelines-information-and-communication-technology-security-and-governance\\_en](https://www.eiopa.europa.eu/content/eiopa-finalises-guidelines-information-and-communication-technology-security-and-governance_en)

## 7.5 ESMA's guidelines on outsourcing to cloud service providers

ESMA published Guidelines on Outsourcing to Cloud Service Providers<sup>44</sup> on 18 December 2020. The guidelines will apply from 1 July 2021. Finanstilsynet assumes that the guidelines will be followed in Norway and will update its supervisory practice in line with the new guidelines.

The guidelines are aimed at infrastructure companies, investment firms and management companies. The objective of the guidelines is, among other things, to help institutions identify, address and monitor the risks posed by outsourcing to cloud service providers. Among other things, they provide the institutions with guidance on which risk assessments and due diligence procedures they should carry out, which management, organisational and control frameworks should be introduced, and how the outsourcing of cloud services can be terminated, what contractual elements the agreements should contain, what outsourcing agreements should include, and what information should be reported to the supervisory authorities.

## 7.6 Proposed regulations on digital operational resilience

The European Commission's proposed new Digital Operational Resilience Act (DORA)<sup>45, 46</sup> is intended to ensure that all participants in the financial system have the necessary measures in place to reduce the risk of cyberattacks and other risks. The proposed legislation will require all institutions to be able to deal with all types of interference and threats to information and communication technology (ICT). The proposal also introduces a supervisory framework for ICT service providers, such as providers of cloud services. The proposed regulations are considered EEA-relevant, and it is assumed that they will be enacted in Norwegian law when they are agreed upon.

In order to ensure the comprehensive implementation of the requirements for the financial services sector's management of ICT risk, the proposed Regulations cover various types of institutions regulated at the EU level, which will make it possible to achieve a homogeneous application of the requirements for risk management in ICT-related areas, taking into account that there are significant differences between institutions in terms of size, business profiles and exposure to digital risk. The proposed legislation sets requirements for the management and control of ICT operations, requirements for the management of ICT risk, the reporting of ICT incidents, the testing of operational resilience and the follow-up of service providers. The ICT Regulations already include a number of these requirements, so the changes will probably entail little significant change for Norwegian institutions. The proposed legislation also allows for the sharing of information and intelligence related to cyberthreats and vulnerabilities, as Norwegian institutions already do through their interaction with Nordic Financial CERT (NFCERT).

---

<sup>44</sup> <https://www.esma.europa.eu/press-news/esma-news/esma-publishes-cloud-outsourcing-guidelines>

<sup>45</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0595&from=EN>

<sup>46</sup> <https://www.regjeringen.no/no/sub/cos-notatbasen/notatene/2020/des/forslag-til-forordning-om-digital-operasjonell-motstandsdyktighet-i-finanssektoren/id2791266/>

In connection with the proposed new legislation for digital operational resilience, a directive containing supplementary provisions has also been proposed<sup>47,48</sup>. These deal with amendments to several directives, either concerning changes in operational risk or risk management requirements or cross-references, including in the Capital Requirements Directive (CRD), the Markets in Financial Instruments Directive (MiFID II), the Undertakings for the Collective Investment in Transferable Securities Directive (UCITS) and the directive concerning the taking-up and pursuit of the business of insurance and reinsurance (Solvency II).

## **7.7 Proposed amendments to the Regulations on Exemption from the Notification Obligation in Connection with Outsourcing**

Finanstilsynet has consulted on proposed amendments to the Regulations on Exemption from the Notification Obligation in Connection with Outsourcing, with a deadline for submissions of 31 March 2021.<sup>49</sup>

### ***Main features of the proposal***

Finanstilsynet believes that more types of institutions should be covered by the notification obligation in connection with outsourcing. This is partly due to requirements in EU Directives, and partly due to Finanstilsynet's need for ongoing information about the institutions' outsourcing. Furthermore, it has been proposed that the notification obligation should only apply to outsourcing of operations that are critical or important to the institutions and means that for some agreements exemptions from the notification obligation can be granted.

In addition, a clarification of what information outsourcing notifications must include has been proposed, as has a provision requiring all institutions subject to supervision to maintain an up-to-date overview of all their outsourcing agreements.

---

<sup>47</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0596&from=EN>

<sup>48</sup> <https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2020/des/digital-finans-forslag-til-endringsbestemmelser-knyttet-til-kryptoaktiva-og-operasjonell-sikkerhet/id2791267/>

<sup>49</sup> <https://www.finanstilsynet.no/nyhetsarkiv/horinger/2021/forslag-til-endringer-i-forskrift-om-unntak-fra-meldeplikt-ved-utkontraktering-av-virksomhet/>



# Appendix 1: The institutions' assessment of vulnerability

Payment service providers' assessment of operational risk and security risk is summarised below, along with the assessments of a few other institutions. Finanstilsynet has used the same form for both purposes, but some questions are specific to payment service providers' reporting of operational risk and security risk.

The summary includes assessments from 124 institutions. The questions are divided into seven themes:

1. Governance and control
2. The value of ICT as decision support
3. Operations and emergency preparedness
4. Data protection
5. ID theft
6. Internal fraud
7. Money laundering

The institutions have been asked to assess their situation/maturity relating to each of the risks described in the form and indicate whether the associated risk is assessed to be high, moderate or low. If the risk is assessed to be high, the institution is asked to state the reason for this. The institutions have also been asked to assess whether the risk is considered to be increasing, decreasing or stable. Furthermore, the institutions must provide a brief description of the measures implemented during the past year, and an assessment of whether the measures are deemed sufficient. In addition, the institutions are asked to specify which factors entail the highest risk. A further description of how to complete the questionnaire can be found below the final table.

The tables summarise the results of the survey. The institutions' responses are indicated by colour codes. Green expresses low vulnerability, yellow medium vulnerability and red high vulnerability. No colour indicates that the institution did not reply.









The trend, i.e. whether the vulnerabilities are considered to be increasing, stable or decreasing, is expressed in the far right column of the tables and represents the average of the institutions' assessments. A horizontal arrow (where the interval is -0.2 to +0.2) indicates a stable trend. Arrows that point up indicate that vulnerability is considered to be increasing (the interval +0.2 to +1), and arrows that point down indicate that vulnerability is considered to be decreasing (the interval -0.2 to -1). For each question, an arithmetic mean of the institution's responses is calculated. The 'N/A' in the column for 2019 means that the question was not included in last year's survey.

## Governance and control

Governance and control	Vulnerability	The institutions' responses	Trend 2019	Trend 2020
1	We comply with the principle of three lines of defence.		→	→
2	We have a well-established risk analysis process. Employees are familiar with the process and make active and ongoing contributions.		→	→
3	We have an adequate overview of business-critical ICT equipment and software, including licences. We have an adequate overview of valid configuration of technical solutions.		N/A	→
4	Information forming the basis for risk assessments is collected systematically on an ongoing basis. The information may be analyses of deviations and incidents, information from external sources, results of penetration testing and observations from customers and		↗	→
5	Employees have job descriptions. Employees' responsibilities for control and reporting are set out in their job descriptions.		→	→
6	We have a process for working out and improving procedures for development and operations and for overseeing that the procedures are complied with.		N/A	→
7	Outsourcing agreements give us audit rights to all aspects of the delivery.		→	→
8	We have good security guidelines. We make detailed risk assessments of payment services operations and provide a description of security controls and measures to protect users of the payment services against identified risks, including fraud and illegal use of sensitive information and personal data.		N/A	→
9	We have good legal and technical procurement competence.		N/A	→
10	We monitor our service providers and deliveries on an ongoing basis.		N/A	↗
11	We have documented the controls performed in the first line of defence, risk management/compliance and internal audit (the three lines of defence), disaggregated to ensure integrity, confidentiality and availability. There is a specification of who, and which institution, is responsible for carrying out the controls.		N/A	↘
12	We focus on raising the awareness of and training employees.		N/A	→

Green: low vulnerability. Yellow: medium vulnerability. Red: high vulnerability. White: N/A.

## Decision support

Decision support	Vulnerability	The institutions' responses	Trend 2019	Trend 2020
1	The ICT systems retrieve relevant information from external and internal sources and compile and synchronise the information into a picture of the institution's risk for the purpose of management and reporting to the authorities.		↗	→
2	The ICT systems automatically provide an overall risk picture, so that if a cornerstone enterprise goes bankrupt, for example, the system automatically issues an alert about loans to the enterprise's employees and suppliers, so that we can consider writing these off as losses.		→	→
3	The ICT systems reflect customers' debt servicing capacity.		↗	→
4	The information in our systems and registers is correct (data quality).		↗	↘
5	Integration between the systems is automated to the extent possible.		→	↘
6	The scope of deficiencies and errors in the systems is decreasing.		→	→
7	We collect statistical information about operations, transactions and fraud in payment services and use the information to make the services more secure.		N/A	→
8	We continuously consider measures to protect customers, e.g. by 1) enabling the customer to turn off features of the payment service (e.g. blocking special regions or internet access), 2) notifying the customer (by sms or email) about movements on the customer's accounts/cards or of cases where attempts to access the customer's accounts/cards are rejected, 3) giving the customer easy access to customer support.		N/A	→

Green: low vulnerability. Yellow: medium vulnerability. Red: high vulnerability. White: N/A.

## Operations

Operations	Vulnerability	The institutions' responses	Trend 2019	Trend 2020
1	There is risk associated with non-existent or deficient procedures for change management and compliance. The root cause of errors is not uncovered and/or corrected.		N/A	→
2	When new IT systems are to be developed, we take the needs and systems of all departments that may be affected into account. We do this to avoid the challenges associated with 'silo solutions', such as extensive software maintenance, complicated operations and challenges associated with data synchronisation.		N/A	→
3	The test systems are 'production-like', i.e. test data (anonymised), applications, software, control systems and hardware are the same for testing as for production.		→	↘
4	We make changes to the infrastructure (non-functional changes) during periods with little traffic and can quickly reverse the change and roll back if necessary.		→	→
5	Security tests are carried out prior to production setting. The testing is performed by persons who have not been involved in the development of the service being tested.		→	→
6	We perform regular tests to test the security of our services, (e.g. penetration testing, testing according to the TIBER standard, vulnerability scanning).		N/A	→
7	There is a high degree of complexity in the IT systems.		N/A	→
8	We implement extensive measures to protect ourselves against attacks (Advanced Persistence Threat, trojans, ransomware, DDoS, email attacks). Examples of measures: Intrusion detection and intrusion prevention, firewall, antivirus, control of web traffic, securing of email, patching and other measures to ensure stable operations.		→	→
9	We make extensive use of logging, and we have a procedure for responding quickly and adequately to 'extraordinary aspects' in the log.		→	→
10	We monitor 'ticking bombs', i.e. components that gradually wear out, or assets that gradually reach levels requiring intervention, such as memory leakage, expired certificate dates, worn out electronic components, an energy supply that is running down (batteries, fuel for emergency generator etc.)		→	→
11	We have good measures for detecting irregularities (abnormal load, abnormal ports/protocols, irregular response times) in data traffic and take action before damage occurs.		→	→
12	We test our disaster recovery systems to an extent that makes us feel confident that they function as intended.		→	→
13	We have carried out risk analyses, identified areas with a high risk of downtime (e.g. single point of failure) and implemented measures to ensure ongoing operations.		N/A	↗
14	Cooperation procedures and the division of responsibilities between us and our service providers are clear-cut and detailed.		→	→
15	There is heavy pressure to deliver.		→	→
16	We have insufficient access to expertise, including the expertise to stipulate requirements for service providers and to monitor deliveries.		↘	→
17	Large 'technical debt' entails unnecessary risk with respect to change management and operations.		N/A	→
18	Due to a number of new regulatory requirements we frequently have to change our systems.		↘	↗
19	We have a good overview of where data transmission lines go. We have ample redundancy with respect to data transmission lines.		→	→
20	We have good access management and access control procedures for our employees, hired employees and service provider staff.		→	↘
21	Our employees undergo training on threats and attack scenarios.		↗	→
22	The interfaces used by third parties to access payment accounts have been tested and approved in cooperation with third parties.		N/A	→
23	The interfaces used by third parties have been secured in accordance with the provisions of the RTS.		N/A	→

Green: low vulnerability. Yellow: medium vulnerability. Red: high vulnerability. White: N/A.

## Data protection

Data protection	Vulnerability	The institutions' responses	Trend 2019	Trend 2020
1	We have good guidelines for classification and protection of structured (databases) and unstructured (text documents, emails, personal file areas) data and protection of the data.		→	→
2	We have good access controls for employees, consultants, service providers, application accesses, software accesses and administrator accesses.		↗	→
3	We log access to data and systems and can turn on alerts in the event of unauthorised access or attempted access.		→	→
4	We have divided the network into security zones based on a security rating of data and functions. The rating determines how data and functions in the zone are secured physically and logically (access controls, encryption, etc.).		→	→
5	We protect data on portable devices.		→	↗
6	On termination of data storage agreements, the service provider must document that data have been completely deleted.		→	→
7	We have procedures for storing and monitoring sensitive payment information (information that can be misused to commit fraud, e.g. card details and login information), as well as restrictions on and an overview of access to this information.		N/A	→

Green: low vulnerability, Yellow: medium vulnerability, Red: high vulnerability, White: N/A.

## ID theft

ID theft	Vulnerability	The institutions' responses	Trend 2019	Trend 2020
1	We have good measures in place to prevent that an attacker takes over a user ID and uses it fraudulently.		→	→
2	We have good control of the issue, use and deletion of login IDs and passwords to customers.		→	→
3	We use controls that prevent skimming and card-not-present fraud.		→	→
4	We require strong customer authentication in connection with payments for online transactions.		→	→

Green: low vulnerability, Yellow: medium vulnerability, Red: high vulnerability, White: N/A.

## Internal fraud

Internal fraud	Vulnerability	The institutions' responses	Trend 2019	Trend 2020
1	We have carried out a detailed risk assessment and defined fraud scenarios.		N/A	→
2	We use dual control as far as possible.		→	→
3	We have established special logging and alert procedures in connection with situations, scenarios or account movements where the risk assessment referred to in point 1 concludes that fraud is likely to occur. This could be in the form of backdating, movements on internal accounts, movements on passive accounts, transfer from a customer to an employee and back, employees who are in a squeezed financial situation or have a high debt-to-income ratio.		→	→
4	We monitor employees' own-account trading.		→	→

Green: low vulnerability, Yellow: medium vulnerability, Red: high vulnerability, White: N/A.

## Money laundering

Money laundering	Vulnerability	The institutions' responses	Trend 2019	Trend 2020
1	We cooperate with other institutions to identify the origin and use of the funds.		N/A	→
2	Our IT systems provide a complete picture of the customer, customer relations and customer behaviour (KYC – Know Your Customer).		→	→
3	We use electronic monitoring of transactions and transaction patterns.		↗	→
4	We have an increasing level of precision in flagging suspicious transactions.		N/A	→
5	There is a risk that the transaction monitoring system does not intercept all payment transactions.		N/A	↘
6	The AML systems makes extensive use of data from other systems.		N/A	→
7	The AML systems recognise suspicious patterns over time.		N/A	→
8	The AML systems intercept that a person has multiple customer relationships across business units.		N/A	→
9	The hits made by the sanction screening system on listed persons and entities have a high level of precision.		N/A	→

Green: low vulnerability. Yellow: medium vulnerability. Red: high vulnerability. White N/A.

## Guidance to the institutions

‘Finanstilsynet asks the institution to assess the risks described in the table below. The first column gives a description of the overall risk. The second column gives a description of factors that may affect the risk. The institution should assess the institution’s situation/maturity and indicate in the third column whether the risk associated with the various statements is assessed to be high, moderate or low. If the risk is considered to be high, we ask the institution to state, in the fourth column, four reasons why the risk is assessed as high. In the fifth column, the institution should indicate whether the risk is considered to be increasing, decreasing or stable. In the sixth column, we ask the institution to provide a brief description of the measures implemented during the past year, and an assessment of whether the measures are deemed sufficient. If certain factors are not relevant to the institution, you should leave the cell blank or give an N/A response.

Example: The institution has experienced several incidents that have come as a surprise to the institution. It took four hours to determine the cause of the error and another two hours to correct it. The institution finds that the statement ‘We have a well-established risk analysis process. Employees are familiar with the process and make active and ongoing distributions’ does not give an adequate description of the situation in the institution, which writes ‘High’ in the third column. Based on an analysis of the incident, the institution should state the four main reasons why the incidents occurred and why they came as a surprise to the institution, in the fourth column. In the sixth column, the institution should give a brief description of the improvement measures implemented during the past year.

Finally, the institution is asked to specify the factors that it considers to represent the highest risk, i.e. one or more risks that are particularly relevant for the institution. Please provide this information in the comment field below the tables.’

## Appendix 2: Basis for the risk matrix

Finanstilsynet's assessment of risk in the different areas, classified according to probability and the seriousness of the consequences, is discussed in this attachment. Along with the observations and assessments in chapters 3 to 6, this forms the basis for the risk matrix in figure 1.1 in chapter 1.

The following definitions are used:

**Vulnerability:** Weakness in technical infrastructure, functions and processes that may result in undesirable incidents.

**Threat:** Factor with the potential to cause an undesirable incident.

**Risk:** The risk of an undesirable incident occurring as a consequence of inadequate internal processes or systems or failure thereof, human error or external incidents.

**Consequence:** Possible result of an undesirable incident.

**Risk assessment:** Identification, analysis and evaluation of risk. A risk assessment lays the foundation for an institution's risk-mitigating measures and the priority given to them.

### ***Governance model and internal control***

Finanstilsynet assesses the overall risk associated with vulnerabilities in the **institution's governance model** and **internal control** as **medium**. The probability of the three lines of defence not revealing serious weaknesses in the institution's internal control through their activities is assessed as *low* to *medium* and the consequences as *moderate*. This is based on the following assessments:

- The probability of failure to comply with laws and regulations not being detected as a result of inadequate supervision by an institution's operational management is assessed as *low* to *medium* and the consequences as *serious*.
- The probability of important requirements in governing documents not being implemented and operationalised, including controls, is assessed as *medium* and the consequences as *moderate*.
- The probability of the compliance function not detecting serious weaknesses in operational units' control is assessed as *medium* and the consequences as *moderate*.
- The probability of the institution's board and executive management not possessing information that confirms or disproves compliance with internal and external requirements is assessed as *medium* and the consequences as *moderate*.
- The probability of the institution's board and executive management not having sufficient expertise and insight to help to ensure that IT investments support the institution's strategy and

needs, and the necessary understanding of the risk picture in the ICT area to ensure stable and secure ICT operations is assessed as *medium* and the consequences as *moderate*.

- The probability of unclear roles in the institution's first and second lines of defence leading to serious weaknesses in the surveillance and control of the institution's governance is assessed as *low to medium* and the consequences as *limited*.
- The probability of serious vulnerabilities not being detected as a result of deficient risk management between the operational unit and the risk management function in the second line of defence is assessed as *low to medium* and the consequences as *moderate*.
- The probability of serious weaknesses in internal control not being detected by the internal audit as a result of inadequate competencies and understanding of risk on the part of the institution's internal audit is assessed as *low* and the consequences as *moderate*.
- The probability of serious organisational challenges as a result of weak change management is assessed as *medium* and the consequences as *moderate*.

### ***Skills and skills management***

At present, Finanstilsynet assesses the overall risk associated with vulnerabilities in connection with **skills and skills management** as **medium**. The probability of adverse incidents occurring or not being adequately managed as a consequence of a lack of skills in Norway is assessed as *medium* and the consequences as *limited to moderate*. This is based on the following assessments:

- The probability of the board and the executive management not maintaining a sufficient overview of employee skills and current and future needs as a result of inadequate skills management is assessed as *low to medium* and the consequences as *limited*.
- The probability of inadequate skills management in institutions resulting in the loss of and/or an inadequate supply of the skills necessary for sound operations is assessed as *medium* and the consequences as *moderate*.
- The probability of inadequate security expertise in institutions resulting in significant operational risks is assessed as *medium to high* and the consequences as *moderate to serious*.
- The probability of business disruptions and unavailable services as a result of insufficient skills is assessed as *low* and the consequences as *moderate*.
- The probability of breaches of information security as a result of inadequate access to security skills is assessed as *medium* and the consequences as *moderate*.
- The probability of institutions' inadequate competence in services developed and operated by service providers resulting in breaches of laws and regulations is assessed as *low to medium* and the consequences as *limited*.
- The probability of increased dependence on foreign service providers as a result of lack of resources and rising needs in Norway is assessed as *medium* and the consequences as *moderate*.
- The probability of inadequate understanding of the risks attending the use of cloud services resulting in adverse incidents is assessed as *medium* and the consequences as *moderate*.
- The probability of inadequate competence in new technology, such as RPA, AI and blockchain, resulting in failure to identify significant operational risks when using such technology is assessed as *medium* and the consequences as *limited to moderate*.



### ***Vendor management***

Finanstilsynet assesses the overall risk associated with vulnerabilities in **vendor management** as **medium**. The probability of adverse incidents is assessed as *medium* and the consequences as *moderate*. This is based on the following assessments:

- The probability of major irregularities in the service provider's internal control not being discovered by the institution is assessed as *medium* and the consequences as *moderate to serious*.
- The probability of security breaches occurring as a result of inadequate supervision and commitment to the security requirements by the service provider is assessed as *medium* and the consequences as *moderate*.
- The probability of an unacceptably long restoration time in the case of serious business disruptions due to unclear roles and responsibilities in the cooperation with the service provider and between service providers is assessed as *medium* and the consequences as *serious*.
- The probability of service unavailability as a result of inadequate monitoring of service quality is assessed as *low* and the consequences as *moderate*.
- The probability of undesirable dependence on service providers as a result of inadequate regulations (e.g. exit rules) in the agreement is assessed as *medium to high* and the consequences as *moderate*.
- The probability of undesirable dependence on service providers as a result of inadequate expertise on the part of the institution concerning the outsourced services is assessed as *medium to high* and the consequences as *limited*.
- The probability of inadequate (regular) risk assessments failing to detect weak sustainability on the part of service providers as a consequence of a difficult liquidity situation (bankruptcy risk), a challenging resource situation or other factors that may threaten the service provider's ability to deliver, is assessed as *low* and the consequences as *moderate*.
- The probability of serious weaknesses in a service provider's internal control not being detected through the work of a service provider's chosen auditor on an independent audit report is assessed as *medium* and the consequences as *moderate*.
- The probability of inadequate quality assurance of services acquired from different service providers and subcontractors as a result of deficient follow-up, lack of competence and failure by the service provider and subcontractors to acknowledge and comply with the institution's requirements, is assessed as *medium* and the consequences as *moderate*.

### ***Digital crime***

Finanstilsynet assesses the overall risk associated with vulnerabilities and threats causing damage as a consequence of **digital crime** as **high**. The overall grade has not changed in this year's report, but Finanstilsynet considers the risk to be somewhat higher than in 2020 as a result of increased criminal activity. The probability of adverse incidents is assessed as *high* and the consequences as *serious*. This is based on the following assessments:

- The probability of serious weaknesses in an institution's defences not being uncovered as a result of non-existent or deficient security testing is assessed as *high* and the consequences as *serious*.
- The probability of an institution having serious faults in its security configuration of critical systems as a result of failure to classify its systems is assessed as *medium* and the consequences as *serious*.
- The probability of an institution having serious faults in its security configuration of cloud services is assessed as *medium* and the consequences as *serious*.
- The probability of institutions being hit by a ransom virus with loss of critical business data as a result of malware (encryption) is assessed as *moderate* and the consequences as *critical*.
- The probability of an institution not detecting criminals who have established a digital foothold inside the network before damage is averted is assessed as *medium* and the consequences as *critical*.
- The probability of criminals succeeding in exploiting vulnerabilities in networks and applications before being discovered (security patch applied) is assessed as *medium to high* and the consequences as *serious*.
- The probability of serious security flaws not being patched in time as a consequence of inadequate security updates (patch management), including at service providers and subcontractors, is assessed as *medium* and the consequences as *serious*.
- The probability of new applications or changes in existing applications being released into production with serious security flaws is assessed as *medium* and the consequences as *serious*.
- The probability of third-party applications integrated by a third party between the institution's systems and its customers resulting in adverse security incidents is assessed as *medium* and the consequences as *moderate*.
- The probability of employees or service provider personnel representing a significant vulnerability as a result of negligence and inadequate competence in secure use of the institution's systems is assessed as *high* and the consequences as *serious*.
- The probability of criminals or foreign intelligence services attempting to recruit employees or service provider personnel to gain access to information about vulnerabilities in the digital infrastructure or other information about the institution, or of the institution's employees or service provider personnel being used involuntarily, through threats, as an instrument for a cyberattack, is assessed as *medium* and the consequences as *serious*.
- The probability of employees being used involuntarily, through social engineering, as a medium for a cyberattack is assessed as *high* and the consequences as *serious*.
- The probability of criminals succeeding in entering the institution's premises as a result of inadequate visitor control procedures is assessed as *low* and the consequences as *limited*.
- The probability of criminals succeeding in forcibly entering the institution's premises is assessed as *high* and the consequences as *serious*.
- The probability of disloyal employees exploiting vulnerabilities in the system for financial gain is assessed as *low to medium* and the consequences as *limited*.

- The probability of disloyal employees in the institution or personnel at service providers' development units planting malicious code in critical business applications is assessed as *low* and the consequences as *moderate*.
- The probability of employees or service provider personnel helping criminals to channel criminal transactions through an institution's systems is assessed as *medium* and the consequences as *serious*.
- The probability of personal data, including information about an institution's employees and service provider personnel who have roles that may be of interest to and exploited by criminals, falling into the hands of criminals is assessed as *medium to high* and the consequences as *serious*.

### ***Information leaks***

Finanstilsynet assesses the overall risk associated with vulnerabilities and threats causing damage as a consequence of **information leaks** as **medium to high**. Finanstilsynet observes that the institutions have improved their efforts to prevent information leaks and are actively working on this to safeguard their values. The probability of adverse incidents is assessed as *high* and the consequences as *moderate*. This is based on the following assessments:

- The probability of classified documentation being sent from the institution in an unauthorised manner as a result of lack of classification and control is assessed as *high* and the consequences as *moderate*.
- The probability of confidential information going astray as a result of failure to control outgoing emails is assessed as *high* and the consequences as *moderate*.
- The probability of confidential information going astray as a result of failure to control the use of USB storage media is assessed as *medium* and the consequences as *moderate*.
- The probability of confidential information going astray as a result of failure to control service provider personnel is assessed as *moderate* and the consequences as *serious*.
- The probability of confidential information that may be used to harm the institution intentionally or unintentionally being sent to or shared with external parties in an unauthorised manner is assessed as *high* and the consequences as *moderate*.
- The probability of employees or service provider personnel operating as insiders and handing over or sending confidential information, such as lists of email addresses and login information, to criminals, is assessed as *medium* and the consequences as *moderate*.
- The probability of confidential information going astray as a result of lack of control or errors made when submitting information to customers, is assessed as *medium* and the consequences as *moderate*.
- The probability of confidential information going astray as a result of use of portable equipment outside the office network is assessed as *medium to high* and the consequences as *moderate*.

### ***ICT operations***

Finanstilsynet assesses the overall risk associated with vulnerabilities in **ICT operations** as **high**. The probability of adverse incidents is assessed as *medium to high* and the consequences as *moderate to serious*. This is based on the following assessments:

- The probability of unstable and/or unavailable services as a result of increased integration among different service providers is assessed as *high* and the consequences as *serious*.
- The probability of operational problems as a result of errors in shared infrastructure is assessed as *medium to high* and the consequences as *serious*.
- The probability of operational problems as a result of inadequate competence and a lack of comprehensive understanding and overview of the institution's architecture and digital business processes is assessed as *medium* and the consequences as *moderate to serious*.
- The probability of impaired data quality as a consequence of complex integration among service providers is assessed as *low* and the consequences as *moderate*.
- The probability of operational problems as a result of inadequate change management (hardware applications, databases, operating systems etc.), is assessed as *medium* and the consequences as *moderate*.
- The probability of the agreed time for correcting critical errors not being adhered to as a result of the complexity of the system portfolio, entailing integration between new and old systems, is assessed as *medium* and the consequences as *serious*.
- The probability of monitoring of the IT environment not uncovering operational irregularities (e.g. expired certificates, databases, memory leaks and electronic components) is assessed as *medium* and the consequences as *serious*.
- The probability of operational problems as a result of inadequate follow-up of technical debt is assessed as *medium* and the consequences as *moderate*.
- The probability of the test systems not being sufficiently similar to the production system is assessed as *medium to high* and the consequences as *moderate*.

### ***Business continuity management and crisis management***

Finanstilsynet assesses the overall risk associated with vulnerabilities in **business continuity management and disaster management** as **medium to high**. The probability of adverse incidents resulting in the activation of disaster recovery systems for critical business processes is assessed as *very low to low* and the consequences as *critical* if the system does not function as intended. This is based on the following assessments:

- The probability of the institution's disaster recovery system not being established in accordance with its needs as a consequence of the absence of or inadequate business impact analyses and requirements is assessed as *medium* and the consequences as *critical* if the system has to be activated.
- The probability of institutions not being adequately prepared to respond to a serious situation as a result of deficient training and exercises is assessed as *high* and the consequences as *critical*.
- The probability of the emergency response management of an institution and its service provider being inadequately coordinated in the event of a serious incident is assessed as *medium* and the consequences as *critical*.
- The probability of institutions failing to handle a serious incident effectively as a consequence of unclear roles and responsibilities internally and between the institution and the service provider is assessed as *low to medium* and the consequences as *serious*.

- The probability of the disaster recovery system not functioning as intended owing to deficiencies in the technical set-up and infrastructure and testing of the system, as well as in the evaluation of the tests, is assessed as *low to medium* and the consequences as *critical*.
- The probability of inadequate updates, including security updates, of the disaster recovery system is assessed as *low to medium* and the consequences as *serious*.
- The probability of an institution affected by a serious digital attack not being capable of handling the situation effectively as a consequence of the lack of a business continuity plan to handle cyber attacks and inadequate training and exercises is assessed as *medium to high* and the consequences as *critical*.

### ***Geopolitical factors***

Finanstilsynet assesses the risk associated with vulnerabilities in relation to foreign operators that deliver critical ICT services to Norwegian institutions as **medium to high**. Although there were major changes in geopolitical factors in 2020, partly due to the Covid-19 pandemic, the institutions have implemented measures showing that they are handling the consequences of the pandemic in a good way. The probability of adverse incidents when foreign service providers are cut off from delivering their services is assessed as *low* and the consequences as *serious*. This is based on the following assessments:

- The probability of an institution's disaster recovery personnel being able to maintain secure and stable operations in situations where foreign service providers are unavailable, is assessed as *low* and the consequences as *serious*.
- The probability of an institution's disaster recovery personnel not being able to maintain secure and stable operations in the event of serious ICT incidents where foreign service providers are unavailable, is assessed as *medium* and the consequences as *serious*.
- The probability of a breakdown in communication with foreign operators, whereby the foreign provider will be cut off from performing critical ICT services, is assessed as *low* and the consequences as *serious*.

### ***Change management***

Finanstilsynet assesses the overall risk associated with vulnerabilities in connection with **change management** as **medium**. The probability of adverse incidents is assessed as *medium* and the consequences as *moderate*. This is based on the following assessments:

- The probability of service unavailability as a result of non-functional changes (changes in the configuration of operating components) is assessed as *medium* and the consequences as *moderate*.
- The probability of weaknesses in change management procedures (including inadequate testing) is assessed as *medium* and the consequences as *moderate*.
- The probability of failure to establish adequate controls for identifying functional and non-functional changes that have been released into production without monitoring the change process, so-called unauthorised changes, is assessed as *medium to high* and the consequences as *serious*.

- The probability of functional changes (software) introducing vulnerabilities into institutions' defences is assessed as *low* and the consequences as *moderate*.
- The probability of a high rate of change due to new business functionality and regulatory requirements resulting in solutions being put into production without the necessary quality assurance is assessed as *high* and the consequences as *moderate*.

### ***Access management***

Finanstilsynet assesses the overall risk associated with vulnerabilities in **access management** as **medium to high**. The probability of adverse incidents is assessed as *medium to high* and the consequences as *moderate*. This is based on the following assessments:

- The probability of employees with extended access rights performing illegal actions is assessed as *low* and the consequences as *moderate*.
- The probability of service provider personnel with extended access rights performing illegal actions is assessed as *low* and the consequences as *serious*.
- The probability of employees or service provider personnel having administrative rights without the executive management being aware of it is assessed as *low to medium* and the consequences as *moderate*.
- The probability of confidential information going astray as a result of inadequate access management and control of employees' accesses is assessed as *medium to high* and the consequences as *moderate*.
- The probability of confidential and/or classified information going astray as a result of a service provider's security breaches is assessed as *medium to high* and the consequences as *moderate*.
- The probability of service provider personnel, or a service provider's subcontractor's personnel, breaking rules while performing operating tasks is assessed as *medium* and the consequences as *serious*.

### ***Data quality***

Finanstilsynet assesses the overall risk associated with vulnerabilities in connection with **data quality** as **medium**. The probability of adverse incidents is assessed as *medium* and the consequences as *limited*. This is based on the following assessments:

- The probability of decisions being based on the wrong premises is assessed as *medium to high* and the consequences as *moderate*.
- The probability of the AML system not intercepting all payment transactions is assessed as *medium* and the consequences as *limited to moderate*.
- The probability of risks not being identified is assessed as *medium* and the consequences as *limited*.

## Appendix 3: Finanstilsynet's monitoring activities

### ***Key areas for Finanstilsynet's ICT supervision***

Supervisory activities are risk-based, and Finanstilsynet gives priority to institutions that have the greatest influence on financial stability and well-functioning markets. ICT risk is assessed, and the institutions' own annual assessments of ICT risk are reviewed. Emphasis is placed on monitoring the organisation of ICT/cyber security work, the security of institutions' ICT systems and the organisation of surveillance activities. Inspections include institutions' control of access to systems, particularly those containing sensitive information, and the institutions' testing of penetration of their systems. Other prioritised topics for supervision will be overall governance of ICT activities, the institutions' emergency response work in connection with business continuity and disaster recovery systems and the testing thereof, outsourcing, the institutions' payment services and ICT systems for detecting money laundering and the financing of terrorism. Finanstilsynet places emphasis on the institutions having procedures in place for ensuring complete data extracts to anti-money-laundering systems. The use of new technology, major changes in the ICT area and extensive changes in the financial infrastructure are also topical subjects.

The institutions' management and control, and regular risk assessment, of outsourced ICT activities, the quality of agreements and the institutions' follow-up of agreements between the institution and service providers will also be followed up.

### ***Work with payment systems***

The EU's revised Payment Services Directive (PSD2) has been transposed into Norwegian legislation and will form the basis for the supervision of institutions' payment services. Institutions will be monitored with respect to their compliance with the new regulations relating to payment service systems<sup>50</sup>, risk related to payment services and compliance with the duty to report new or changes to existing payment services. Account servicing payment service providers' interfaces (APIs) for account access will also be followed up, cf. opinion from the European Banking Authority (EBA)<sup>51</sup>. When processing concessions, care will be taken to ensure that the institutions have well-documented procedures in areas relating to ICT and payment services.

The cooperation with Norges Bank on the payment system and financial infrastructure will continue.

---

<sup>50</sup> [Lovdata: Regulations on payment services systems \(Norwegian text\)](#)

<sup>51</sup> <https://www.eba.europa.eu/eba-calls-national-authorities-take-supervisory-actions-removal-obstacles-account-access-under>

### ***Follow-up of incidents***

Following up ICT incidents is a prioritised part of supervisory activities. Finanstilsynet will continue to closely monitor developments in 2021. When incidents occur, emphasis will be placed on whether the institution identifies causes and takes steps to prevent recurrence. Incidents involving serious irregularities will be monitored throughout the life of the incident. Special measures will be considered.

Finanstilsynet will continue to make an annual review of incident reporting with the largest institutions.

It will also be followed up that both account servicing payment service providers and third-party payment service providers report instances of non-conformance in accordance with PSD2 and that the account servicing payment service providers correct the discrepancies and inform the third-party providers.

### ***Outsourcing of ICT activities***

Finanstilsynet will continue to monitor institutions' outsourcing of ICT activities and ensure that the institutions, when entering into a new or changing an existing outsourcing agreement, reports this to Finanstilsynet, as required by Section 4c of the Financial Supervision Act.

Supervisory activity includes monitoring that the institutions prepare risk analyses and make a prudent assessment of the outsourcing relationship, that the agreements are in line with regulations and that the outsourcing is handled in a proper manner by the institution, cf. Section 2 of the ICT Regulations.

### ***Contingency preparedness***

The work of the Financial Infrastructure Crisis Preparedness Committee (BFI) will continue. BFI reviews incident scenarios and determines whether the responsibilities associated with crisis situations are sufficiently clear. Emergency response exercises are planned for 2021 as well, and measures linked to findings from previous exercises will be followed up.

Special incidents, such as the Covid-19 pandemic and the institutions' organisation of their ICT activities, will be closely monitored, particularly at key operators in the financial infrastructure. Finanstilsynet participates in relevant contingency preparedness work initiated by other sectors and cooperation within the national regulatory framework for managing ICT security incidents, partly through the National Cyber Security Centre (NCSC), established by the Norwegian National Security Authority (NSM).

Finanstilsynet will align its contingency work and handling of ICT security incidents with NSM's framework for handling ICT security incidents<sup>52</sup>. Finanstilsynet has been designated as sectoral response environment (SRE) in the financial market area. Finanstilsynet will exercise its role in

---

<sup>52</sup> [NSM: Rammeverk for håndtering av IKT-hendelser \(in Norwegian only\)](#)



collaboration with Nordic Financial CERT according to agreed information exchange rules. The NSM framework forms the basis for the interaction between Finanstilsynet and Nordic Financial CERT.

### ***Monitoring of the cybercrime threat picture***

Finanstilsynet will remain constantly informed of institutions' use of ICT and developments in payment services, including special developments relating to:

- the cybercrime threat picture
- contingency preparedness work targeting digital vulnerability and security
- institutions' organisation and follow-up of security work
- changes in payment services due to the use of new technology (fintech)
- cross-border activities

In cooperation with Norges Bank, Finanstilsynet has circulated for consultation a draft framework for testing cybersecurity in the financial services sector (TIBER-NO) and, together with Norges Bank, aims to implement this during 2021.

Through regular meetings with institutions and Nordic Financial CERT and participation in the Norwegian Cyber Security Centre (NCSC), Finanstilsynet remains updated on developments in the threat picture.

### ***Consumer protection***

Finanstilsynet stresses the importance of institutions safeguarding their customers' security. It will also monitor that institutions do not share customer data without consent, and that data do not fall into the hands of unauthorised third parties.

Finanstilsynet will control that institutions establish digital solutions in compliance with the regulations, and that the solutions launched have built-in security and functionality in line with consumer expectations.

Payment service systems will be controlled to ensure that they do not require users to accept additional functionality in order to be able to use the service, and that users are given the opportunity to protect themselves against adverse incidents, such as the ability to block their cards against online use. Based on new requirements for reporting fraud relating to the use of payment services, cf. Section 2 of the regulations on payment services systems, Finanstilsynet will examine the total extent of fraud and, when needed, also individual operators.

If incidents occur, Finanstilsynet will follow up that the institutions provide customers with information on how they become affected and how the institution or customers themselves can mitigate the situation.

Finanstilsynet will continue to follow up that banks discharge their responsibilities with respect to compliance with the provisions of the Financial Institutions Act<sup>53</sup> regarding the provision of cash. Special attention will be given to new cash in-store solutions. Finanstilsynet will also control that banks have established solutions in line with the provisions of the Financial Institutions Regulations regarding solutions to meet increased demand for cash in a crisis situation<sup>54</sup>.

---

<sup>53</sup> [Act on financial institutions and financial groups \(Financial Institutions Act\)](#)

<sup>54</sup> [Regulations on financial institutions and financial groups \(Financial Institutions Regulations\)](#)



**FINANSTILSYNET**

Revierstredet 3  
P.O. Box 1187 Sentrum  
NO-0107 Oslo

Tel. + 47 22 93 98 00  
[post@finanstilsynet.no](mailto:post@finanstilsynet.no)  
[finanstilsynet.no](https://finanstilsynet.no)

