



FINANSTILSYNET

THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

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

RISK AND VULNERABILITY ANALYSIS

2015

Risk and Vulnerability Analysis 2015

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

Finanstilsynet, 28 April 2016

CONTENTS

1	INTRODUCTION.....	5
2	SUMMARY	6
2.1	Finanstilsynet's findings and observations.....	6
2.2	Financial institutions' assessments.....	8
2.3	Regulatory amendments	9
2.4	Current areas of risk	9
3	FINANSTILSYNET'S FINDINGS AND ASSESSMENTS.....	11
3.1	Financial technology trends	11
3.2	Payment systems.....	12
3.2.1	General comments regarding payment systems.....	12
3.2.2	Management of risk and vulnerability in payment systems.....	12
3.2.3	Notifications regarding payment service systems.....	13
3.2.4	Use of mobile phone functions and mobile payment solutions	14
3.2.5	Blocking use of payment cards for internet transactions	16
3.2.6	Attacks on payment services	16
3.2.7	Overview of annual losses related to payment services.....	18
3.3	Banking.....	23
3.3.1	Follow-up of internet service providers (ISP)	23
3.3.2	Access control	23
3.3.3	Test environment	24
3.3.4	Online security.....	24
3.3.5	Follow-up of internal ICT audit reports.....	24
3.3.6	Data quality – reporting to the Norwegian Banks' Guarantee Fund.....	24
3.4	Securities	25
3.4.1	Information leaks	25
3.4.2	Monitoring of voice recording systems	26
3.4.3	Outsourced order systems.....	27
3.4.4	Suppliers' ability to deliver in critical situations	27
3.4.5	Risk assessments and system ownership	27
3.4.6	Ransomware attacks	28
3.5	Insurance.....	28
3.5.1	Risk related to complex insurance systems	28
3.5.2	Failure to comply with the ICT Regulations' requirements regarding incident reporting	29
3.5.3	Inadequate risk assessments	29
3.6	Accounting firms	29

3.7	Joint efforts by the financial industry	30
3.8	Changes and outsourcing	31
3.8.1	Changes in the service provider market	31
3.8.2	Outsourcing notifications	32
3.9	Incidents reported in 2015.....	33
3.9.1	Incident statistics.....	33
3.9.2	Analysis of incidents as a measure of availability	35
3.10	Observations of digital crime (cybercrime)	35
3.10.1	CEO fraud	36
3.10.2	Ransomware.....	36
3.10.3	The Dyre Trojan.....	37
3.10.4	Targeted police actions successful	37
3.11	Blockchain	37
4	OPERATORS' ASSESSMENT OF RISK FACTORS	39
4.1	Interviews	39
4.1.1	Societal changes affect security	39
4.1.2	Infrastructure disruptions	39
4.1.3	Shortage of expertise.....	40
4.1.4	Risks associated with personnel	40
4.1.5	Undertakings' supply chain complexity	41
4.1.6	The undertakings' views concerning cybercrime	41
4.1.7	Breach of confidentiality.....	43
4.1.8	Use of cloud and file-sharing services	43
4.1.9	Penetration testing.....	44
4.1.10	Internet faults have a global impact	44
4.1.11	Other risks pointed out by institutions	44
4.2	Questionnaire	45
4.2.1	Support for strategic decisions	45
4.2.2	Operational irregularities	46
4.2.3	Data are not adequately protected	47
4.2.4	ID theft.....	47
4.2.5	Misuse of access to IT systems	48
4.2.6	Money laundering	48
4.3	The report from the EU security agency (ENISA)	49
5	REGULATORY CHANGES.....	50
5.1	Coordination within the EU and changes in EU rules and regulations.....	50
5.1.1	Payment services.....	50
5.1.2	The Protection of Personal Data "package"	51
5.1.3	Networks and information security	51
5.1.4	Transmission of data between the EU/EEA and the USA – Privacy Shield	52
5.1.5	Insurance	52
5.1.6	Anti-money laundering measures	53

5.1.7	Taskforce on IT Risk Supervision	53
5.2	Changes in the Norwegian regulatory framework	53
5.2.1	The new Financial Institutions Act.....	53
5.2.2	Amendments to the ICT regulations.....	54
5.2.3	New regulations and guidelines for payment services.....	54
5.2.4	Amendments to the regulatory framework for insurance	55
5.2.5	Electronic signature	55
6	RISK AREAS	57
6.1	Financial infrastructure	57
6.2	The undertakings.....	59
6.3	Users	63
7	MONITORING BY FINANSTILSYNET	65
7.1	Monitoring of ITC risk and other contact with undertakings.....	65
7.2	Work with payment systems.....	65
7.3	Follow-up of incidents	65
7.4	Contingency preparedness.....	66
7.4	Contingency preparedness.....	66
7.5	Further development of supervisory tools.....	66
7.6	Monitoring of the threat picture associated with cybercrime.....	66
7.7	Consumer protection.....	66
8	GLOSSARY	68

1 Introduction

The Financial Supervisory Authority of Norway (Finanstilsynet) performs an annual risk and vulnerability (RAV) analysis of the financial sector's use of ICT and payment services. Through its supervisory functions, Finanstilsynet maintains a broad network of contacts with financial institutions, industry associations, service providers, standardisation bodies and national and international authorities. Based on these sources, the report provides an assessment of the potential impacts of identified risks on the financial sector in Norway.

The purpose of the report is to describe risks and vulnerability relating both to financial stability and individual undertakings and to individual consumers. It provides an up-to-date picture of the risks related to the financial sector's use of ICT and payment services, summarised in chapter 2 of the report.

Some risks and vulnerabilities are reported on every year, while others are not. In the report, Finanstilsynet highlights the risks considered to be the most important this year. Risks which were covered in earlier reports, but which are not mentioned in this year's report, have been deemed to be less relevant, but that does not mean that they no longer exist.

The core of this year's report is found in chapters 3 and 4. Chapter 3 provides an overview of findings and observations made through Finanstilsynet's activities in 2015. Chapter 3 also covers cybercrime and trends in the development of this type of crime. Technology trends considered to be of potential relevance to financial institutions' use of ICT are described. Chapter 4 reports on the financial institutions' own assessments based on questionnaires and interviews. A number of key service providers, including security systems providers, have also been interviewed and the annual reports of international security companies that focus particularly on the financial industry are cited.

Regulatory amendments that could entail substantial changes in financial institutions' system solutions are described in chapter 5.

Chapter 6 contains a summary of Finanstilsynet's overall assessment of the risk picture in 2015 based on findings, observations and trends. The assessments focus on the most important threats and vulnerabilities that could potentially be so detrimental to financial institutions' systems that they could jeopardise the goal of financial stability and well-functioning markets.

Chapter 7 describes the main areas to which Finanstilsynet will pay particular attention in the future.

A glossary explaining key terms and acronyms used in the report is attached.

2 Summary

In 2015 there were no serious ICT incidents that had consequences for financial stability. Compared with the previous year, there were fewer incidents with consequences for individual enterprises or consumers. However, there was a tendency towards an increase in the number of fraud attacks.

Technological developments have a major impact on the development of financial sector services. Deregulation opens the door for new operators and new solutions that challenge established business models.

2.1 Finanstilsynet's findings and observations

By following up on reported incidents and inspection findings and through other supervisory activities, Finanstilsynet obtains a good insight into financial institutions' use of ICT, payment systems and relevant areas of risk.

Payment systems

Finanstilsynet considers payment systems to have been generally robust and stable in 2015, but in certain areas there is nonetheless room for improvement. In several financial institutions, potential for improvement was observed in the fields of disaster recovery plans, operational risk management and access management.

Measures to ensure effective collaboration on shared services and infrastructure should be maintained as part of payment service governance.

Despite an increase in attacks on payment services in 2015, direct losses are still small. The low losses are largely attributable to preventive measures. There was little change in total online banking losses from 2014 to 2015. Losses in 2015 were largely incurred in connection with corporate online banking fraud.

Losses arising from payment card transactions where no extra security measures are required, such as a PIN code (Card-Not-Present transactions), continue to rise. The rise in these losses exceeds the increase in the volume of card payments, and amounted to 37 per cent from 2014 to 2015. This is almost double the increase from 2013 to 2014. Total payment card losses rose by NOK 25 million from 2014 to 2015, an increase of 15 per cent.

Banks

Banks have undergone major change processes in the ICT area in the past few years, but the changes have been implemented without significant consequences for operational stability.

However, Finanstilsynet sees a need for improvement in several areas. The risk of digital attacks is on the rise, and efforts to ensure ICT security should be further intensified. Finanstilsynet has noted from past inspections that ISPs¹ may be inadequately monitored. In Finanstilsynet's view, financial institutions can improve their system access management. At the same time, Finanstilsynet is aware that it may be difficult for the undertakings to procure the requisite security expertise.

Securities

Finanstilsynet considers the ICT systems in the Norwegian securities sector to be of generally good quality and high stability.

However, financial institutions must take more effective action to ensure that sensitive information from investment firms' corporate departments does not go astray. Finanstilsynet has noted cases where financial institutions have outsourced ICT systems with price-sensitive information without having sufficient control of the operating companies' users.

Agreements related to investment firms' outsourcing of ICT services showed that the firms' right to monitor and audit the supplier's activities under the agreements was deficient.

In 2015, several incidents were registered in which no sound recording was made of conversations with customers owing to a malfunctioning of the recording equipment.

Insurance

The insurance sector is currently undergoing numerous regulatory changes that entail significant changes in large-scale, complex ICT systems. Insurers must ensure the quality of, and compliance with, their ICT processes to make sure that they have adequate control of the changes made and that the quality of the systems is not impaired.

Many insurers still need to improve their risk assessments in order to obtain an accurate picture of the overall risk attached to the companies' use of ICT.

Accounting companies

In 2015, Finanstilsynet carried out a documentary inspection of accounting companies' use of ICT. The inspection showed that a number of companies need to put in place measures designed to mitigate ICT operational risk.

¹ Internet Service Provider

Outsourcing notifications

Financial institutions are required to notify Finanstilsynet of the outsourcing of ICT services. When processing outsourcing notifications, Finanstilsynet has found deficiencies in the risk assessments performed, the financial institution's independent assessments of the outsourcing agreement and compliance with applicable laws and regulations. This applies, for instance, to the ICT Regulations and the requirements of the Regulations on Risk Management and Internal Control stipulating that the inspected undertaking shall be entitled to inspect and control, including audit, activities carried out by the service provider under the agreement.

Use of cloud services will, in Finanstilsynet's assessment, fall within the scope of the rules governing traditional outsourcing.

Incidents

Financial institutions are required to report serious or critical events and irregularities in ICT activities. Fewer incidents were reported in 2015 than in 2014, and payment systems and customer services had higher availability in 2015 than in the previous year. The trend has reverted to the positive decline seen in 2011, which was interrupted in 2014. On the other hand, the volume of fraud attacks has increased, and in 2015 several financial institutions were the target of attacks with demands for ransom; however, no ransom was paid.

Cybercrime

Cybercrime is a growing problem and is changing the threat landscape for the financial industry. The ICT Regulations lay down clear requirements regarding financial institutions' governance of ICT security. It is important that the undertakings' executive management and Board of Directors set clearly defined requirements for and monitor undertakings' ICT security work. Intentional criminal acts may have significant consequences for individual undertakings. For example, an encryption virus caused undertakings to lose access to their tools and data for entire working days until the data were restored from backup. Financial stability may also be disturbed if such incidents affect coordinated solutions, shared operational service providers or other key operators.

2.2 Financial institutions' assessments

Financial institutions consider infrastructure disruptions, the complexity of ICT systems and supply chains, cybercrime and system penetration, as well as breaches of confidentiality, to be the most prominent threats.

Other areas of threat identified by financial institutions are a shortage of expertise, uncritical use of file sharing systems and inadequate management and control of the use of cloud services, the poor quality or lack of penetration testing, the scope of changes and the fact that ICT systems do not provide satisfactory support for decision-making, customer service or administrative procedures.

Undertakings also point to societal change, where payment systems can increasingly be used to move illicit funds, as a threat. Moreover, undertakings see a risk that they will be unable to produce systems with sufficiently high precision for identifying suspicious transactions.

2.3 Regulatory amendments

In 2015, there were a number of EU processes related to proposals for new, or amendments to existing, directives, regulations, technical standards and guidelines. These will have significance for Norwegian undertakings as and when they are incorporated into Norwegian legislation. At the national level, too, there were amendments to laws, regulations and guidelines. These regulatory amendments will necessitate changes in the financial institutions' systems in many areas.

The most pivotal regulatory amendment is the EU's new Payment Services Directive (PSD2), which allows new financial sector operators to offer payment services and gives them the right to access payment accounts. Other major regulatory changes are the EU General Data Protection Regulation, the EU Network and Information Security Directive, a new agreement on transmission of personal data between the EU/EEA and the USA, Norwegian Regulations on payment service systems, guidelines on the security of internet payments and Norwegian Regulations on the introduction of Norwegian regulations on the introduction of the EU Regulation on Interchange Fees.

2.4 Current areas of risk

Financial infrastructure

Finanstilsynet considers Norway's financial infrastructure to be robust. It was affected by fewer operational incidents and was more stable in 2015 than in the previous year. In some areas, such as disaster recovery plans and operational risk management, there is room for improvement.

Financial institutions

Finanstilsynet considers network fault, information leaks, cyber attacks, complex system portfolios and faults that arise in connection with changes to be the primary threats to and vulnerabilities in financial institutions' systems. Other threats to and vulnerabilities in the undertakings' systems are inadequate business continuity plans, concentration risk, inadequate testing possibilities and insufficient expertise and capacity.

Consumers

The financial industry is becoming increasingly digitised. This makes the consumer more vulnerable to failures in financial institutions' electronic services, and undertakings' solutions must therefore meet higher standards of robustness.

Increased digitisation can make it difficult for consumers to understand all the consequences of their digital actions. The (advantages of) simplicity and speed offered by small digital surfaces may be

attained at the expense of consumer security and rights. The consumer is increasingly exposed to fraud in connection with the use of digital solutions. Protecting data and preventing ID theft are still relevant challenges.

Consumers and consumer security and rights are key concerns in the work on regulatory amendments.

3 Finanstilsynet's findings and assessments

This chapter mainly presents findings and observations based on Finanstilsynet's supervisory activities, incident reports, notifications of new payment services and changes in existing services and new ICT outsourcing agreements and changes in existing agreements.

Trends that in the longer term are considered likely to be of significance for financial institutions' use of ICT, and that could entail changes in the risk and vulnerability situation for both the undertakings and consumers, are also covered.

A number of incidents in 2015 had consequences for both individual financial institutions and consumers. In Finanstilsynet's assessment, financial stability was not threatened in 2015.

3.1 Financial technology trends

Technological advances have a major impact on developments in the financial industry. Innovation and development in the fields of payment systems, lending, insurance and capital management are challenging established business models, and making it possible for new operators to enter the industry as participants or contributors.

The Norwegian financial industry early on adopted new technology in systems for both employees and the public at large. In order to remain a front-runner in the use of technology tools, it is important to be aware of the possibilities opened up by new financial technology solutions. This trend is spurred by a substantial increase in capital invested in financial technology, enabling the development of new solutions. Increased broadband access with higher capacity and the use of modern computers, smartphones and tablets have led to greater use of digital services.

The technology used and the new and/or improved financial industry services fall into two categories: new services provided by new operators and new services provided by operators that are well-established in the industry. The advent of new service providers is likely to promote a greater degree of development and creativity.

3.2 Payment systems

3.2.1 General comments regarding payment systems

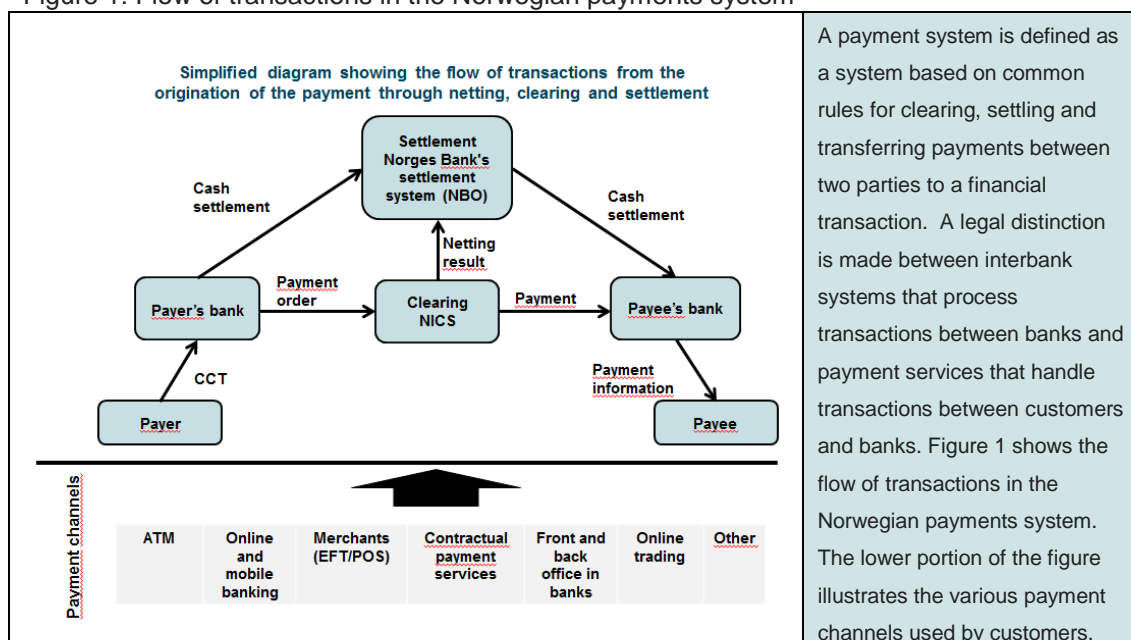
Financial stability means that the financial system is sufficiently robust to execute payments, channel funds and redistribute risk in a satisfactory manner. Effective, robust and stable payment systems are a fundamental prerequisite for financial stability and well-functioning markets.

In Norway, payment systems and payment services are governed by laws and regulations and through the financial industry's self-regulatory system which is administered by Finance Norway (FNO).

The Financial Contracts Act and the EU Payment Services Directive, which was recently revised, are designed to safeguard consumer interests and to provide the best possible protection for consumer security and rights. The Payment Services Directive is also intended to promote increased competition.

Relevant regulatory amendments relating to payment systems are described in 5.2.3.

Figure 1: Flow of transactions in the Norwegian payments system



Source: Finanstilsynet

3.2.2 Management of risk and vulnerability in payment systems

Finanstilsynet has found changes in outsourcing agreements where the financial institution has not carried out any prior assessment of the risk entailed by the changes. Finanstilsynet has also seen the introduction of payment services which initially did not include any risk mitigation measures, incidents reflecting poor testing quality and agreements that have not met regulatory requirements.

Ensuring that individual undertakings have an established framework for governance of the whole payment system that accords with the key role the system plays in a well-functioning economy is a management responsibility. The undertaking is responsible for the service in its entirety, including outsourced parts.

Incidents that occur in, or affect the payment infrastructure or payment services, can have a broad impact and quickly give rise to significant consequences. The most frequent causes of faults and irregularities in payment services are system changes and updates. Mediation of payments and the technologies used are constantly evolving, resulting in an ongoing need to modify existing payment services, in addition to developing new services. This contributes to a high rate of change and risk.

Risk management, quality assurance of development projects, effective end-to-end testing and the establishment of a sound security culture at every level are key aspects of financial institutions' development and change processes. Value chain-based risk and vulnerability assessments of payment services must also be carried out regularly to reduce vulnerability and risk to a defined, acceptable level.

It is important that undertakings conduct in-depth risk assessments by carrying out security and vulnerability analyses prior to the launch of new payment services, and then periodically. Undertakings must ensure that the service is protected by means of logical and physical security measures, and that data are adequately protected. The payment service must be monitored to maintain a sufficient level of security, and to detect and prevent unauthorised use of the service. Reference is made in this connection to the Regulations on Payment Service Systems (see 5.2.3), which govern this aspect.

3.2.3 Notifications regarding payment service systems

The Payment Systems Act requires that Finanstilsynet be notified without undue delay of the establishment and operation of payment services. The following are subject to notification:

- Introduction of a new payment service system
- A new version that materially affects other parties concerned who are part of the system
- A new version with a modified or new functionality that is of material importance for the payment service system.

In 2015, Finanstilsynet received nine notifications of new or modified payment service systems. Several of the notifications concerned mobile systems. The other notifications concerned other types of payment systems or payment card administration systems.

In Finanstilsynet's assessment, not all undertakings comply satisfactorily with the duty of notification. In light of the notifications received, some undertakings have been asked to provide supplementary information. Finanstilsynet has seen both launches of new systems and changes in existing systems without notification being sent. In such cases, the undertakings concerned are contacted and asked to submit the requisite notification.

3.2.4 Use of mobile phone functions and mobile payment solutions

Technological advances have a significant impact on the development of payment services and systems in the sense that financial institutions make use of new possibilities and new financial sector operators, also from outside Norway, establish businesses.

The rapid development of mobile systems continues unabated. Mobile devices and systems play an increasingly important role as a payment instrument, a digital wallet and a security enabler.

Mobile payment systems have primarily targeted person-to-person payments, which offer the greatest potential for simplification. In 2015, DNB launched its Vipps application² and Danske Bank its MobilePay application³ on the Norwegian market. mCASH, the Norwegian rights to which were acquired by the Sparebank 1 banks⁴ in the autumn of 2015, introduced its system for both person-to-person payments and person-to-business payments in 2014. Other financial sector operators are also developing systems for person-to-business payments, to both physical stores, associations and clubs and to online stores. For instance, Danske Bank has expanded its MobilePay application to include systems such as MobilePay Point of Sale⁵, and DNB has added systems for associations and clubs to its Vipps⁶ application. The Eika Banks are expected to launch their Eika Safe⁷ system in 2016.

So far, it has essentially only been possible to use the mobile systems with international payment cards. BankAxept, the national payment card in Norway, is currently developing new payment systems and is expected to launch the BankAxept contactless payment system (NCF technology) for payment cards, mobile devices and online payments in 2016⁸.

The Valyou⁹ payment application, based on contactless technology, was officially launched in the autumn of 2014. The service was discontinued as early as in the autumn of 2015 due to a lack of customers and the widespread availability of operational contactless payment terminals in stores.

Mobile device fingerprinting was adopted in 2015 as authentication for payment services in the Norwegian market. Fingerprints are used, for example, to open Danske Bank's MobilePay application and to log into DNB's mobile and online banking services¹⁰. The quality of the fingerprint sensors in mobile devices is a new area of vulnerability for payment services that must be subjected to a risk assessment and followed up by the payment service provider. In 2015, Skandiabanken launched its Quick Response (QR) code for logging into its online bank¹¹.

² <https://www.vipps.no>

³ <http://danskebank.no/nb-no/mobilepay/Pages/mobilepay-privat.aspx>

⁴ <https://www.bnbank.no/Omoss/Generell-informasjon/For-pressen/Pressemelding-03032014/>

⁵ <https://www.danskebank.no/nb-no/mobilepay/Pages/tilmelding-til-pos.aspx>

⁶ <https://www.vipps.no/bedrift/lag-forening.html>

⁷ <https://eika.no/om-oss/nyheter/2015/eika-safe>

⁸ <http://www.bankaxept.no/>

⁹ <http://www.digi.no/931241/naa-er-valyou-lansert>

¹⁰ <http://www.dinside.no/934551/logg-inn-i-nettbanken-med-fingeravtrykk>

¹¹ <https://skandiabanken.no/bruke/sikkerhet-og-innlogging2/logg-inn-med-qr-kode/>

New authentication systems are under development, with particular focus on the use of biometrics. MasterCard has launched its “selfie payments”¹², where authentication is carried out by means of image recognition or fingerprinting. Voice recognition¹³ systems have also been launched.

The purpose of mobile payment systems is to simplify electronic payment processes, but also to replace the use of cash. However, payment service providers have not reached agreement on any of the fast payment infrastructures that have already been developed¹⁴. In addition to developing payment applications, payment service providers have also developed their own infrastructure, which means that the payee cannot access the money without installing the same application as the payer. Due to the lack of standardisation of point-of-sale (POS) terminals, merchants (NorgesGruppen and Coop¹⁵) have joined forces to establish a single, shared infrastructure with one terminal system. Compared to the payment applications, this simplification appears to have limited effect so far. Because the different applications only function for some store chains, consumers may find mobile payment both confusing and inefficient. In many areas of use, moreover, the present card payment systems seem to be more efficient.

Lack of interoperability could result in lower efficiency and higher costs in payment services. If the costs become unreasonably high or the systems are not user-friendly, the need for regulatory measures will have to be assessed.

So far, major global mobile payment system providers have made little effort to enter the Norwegian market, but such services are expected to be established either directly or through collaborative constellations. In the case of other payment systems, a number of payment service providers have already established operations and more are expected to do so when the new Payment Service Directive (PSD2) (see 5.1.1) comes into force. The Directive allows more operators to provide payment services, and gives them the right to access payment accounts. This is expected to result in the entry of a large number of new operators with new solutions for all types of payment services, in addition to which existing service providers may expand their current systems to include new functionalities. These changes in the payment services sector could, especially at the establishment stage, create new risks and vulnerabilities that must be addressed.

As a consequence of PSD2, there is considerable activity in both the Norwegian and European financial sectors and in the service provider market to establish standards and technology for payment account access. The European Banking Authority (EBA) (see 5.1.1) has been tasked with drafting regulatory technical standards for strong authentication and secure communication in connection with such access.

¹² <http://money.cnn.com/2016/02/22/technology/mastercard-selfie-pay-fingerprint-payments/>

¹³ <http://www.pcquest.com/authshield-enhanced-online-payment-security-with-its-facial-and-voice-recognition-authentication-solution/>

¹⁴ <http://www.fno.no/aktuelt/nyheter/2014/12/betal-fra-konto-til-konto-med-mobil/>

¹⁵ <http://www.norgesgruppen.no/presse/nyhetsarkiv/aktuelt/onsker-a-gjore-mobilbetaling-tilgjengelig/>

Although technological advances make it possible to make mobile payment services safer to use, the threat landscape is expanding in step with the broader availability of mobile systems. Mobile phones are a major area of malware growth, and this trend is expected to continue as mobile phones are increasingly used for everyday activities.

Finanstilsynet presented its assessments of mobile-based payment systems in its Risk and Vulnerability Analysis for 2014¹⁶.

Finanstilsynet is aware that data on customers' use of mobile banking and payment services¹⁷ are reused for commercial purposes without the customers' knowledge. This may constitute a breach of the Norwegian Personal Data Act. Service providers are expected not to share customer data with third parties unless the customer is both aware of and has accepted such use, and the customer is assumed to have the right to use the service even if such acceptance is not granted. This issue is being followed up by the supervisory authorities.

3.2.5 Blocking use of payment cards for internet transactions

The EBA's final Guidelines on the Security of Internet Payments came into force on 1 August 2015. The guidelines prescribe, inter alia, that consumers must to a greater extent be able to set effective limits for use of payment cards. For instance, customers must be able to disable use of the card on the internet. Finanstilsynet has noted that not all payment card issuers have implemented the guidelines in their systems. Finanstilsynet will follow up on this issue in 2016.

3.2.6 Attacks on payment services

In 2015, a number of serious incidents affected access to payment services. Nonetheless, Finanstilsynet has noted a higher degree of accessibility to payment systems in the past year; see 3.9.2.

Several of the incidents affected BankID, resulting in simultaneous payment disruptions for a large number of undertakings. These incidents had a variety of causes, but none were critical for access to payment services. Several undertakings have established alternative log-in and electronic signature systems, thereby reducing the consequences of BankID service disruptions.

Although operational stability increased, the number of malicious attacks on payment services also rose. Finanstilsynet observed a number of phishing attacks targeting payment cards and online banking services.

The fraud schemes targeting payment services are largely based on phishing. Fraudulent enquiries and attempts to fish for information are now turning up in new, more credible versions, posing a security challenge for payment services. The fraudulent enquiries are camouflaged to appear to have been sent by parties known to the recipient. Both e-mail and SMS messages are used. Phishing is often part of

¹⁶ http://www.finanstilsynet.no/Global/Venstremeny/Rapport/2015/ROS_analyse_2014.pdf

¹⁷ <http://www.nrk.no/norge/dnb-sender-kundeinformasjon-til-facebook-1.12804837>

the scenario in payment card and online banking fraud, ransomware and APT and CEO fraud (see 3.10.1). Ransomware, APT and CEO fraud target all sectors, but payment services are particularly exposed because they are closely linked to the money sources.

In 2015, fraudsters adopted new approaches and on several occasions banks reported a higher level of threat due to fraud targeting corporate online banking. The scenario was based on “real-time phishing”. A company employee received a fraudulent SMS or e-mail with a link to a fake online bank. Clicking on the link took the user to a site that appeared to be identical to the bank’s corporate online bank. From then on the procedure was very similar to that used in Trojan attacks on online banks. The user was asked to provide his username and two one-time codes which the fraudsters immediately registered and used in the real corporate online bank. The fraudulent transactions were conducted with payees outside Norway. Despite extensive fraudulent activity of this type targeting Norwegian banks, online bank fraud losses were not particularly high in 2015. The banks’ monitoring procedures and collaboration in FinansCERT ensure that most of the fraudulent transactions are stopped before they are completed, or that the funds are returned by the payee bank.

Finanstilsynet is aware of the occurrence of several cases of CEO fraud¹⁸ in 2015. While this type of fraud does not target payment services directly, the services are used to transfer funds in connection with fraudulent activity. It is important that banks review their procedures, and where possible take action to limit the adverse consequences of this type of fraud.

In 2015, fraud was observed in connection with the use of payment applications (apps), where stolen ID information and card data were used to establish fake user accounts. In Finanstilsynet’s view, financial institutions have established effective procedures for monitoring the overall security of these services so as to minimise risk, even though there are deficiencies in control measures in connection with the establishment of user accounts, especially when stolen information is used.

Despite the proliferation of mobile payment systems and the global increase in infected mobile phones¹⁹, Finanstilsynet does not know of any incidents of attempted fraud using infected mobile phones in Norway.

Experience shows that criminal attacks on payment services are launched in waves. The activity is moved from one country to another depending on where fraudsters believe there is a potential gain.

In Finanstilsynet’s assessment, the financial institutions have effective contingency preparedness systems and have established good defences to stop attempted fraud attacks on payment services, and effective countermeasures reduce the extent of damage and the magnitude of customers’ fraud losses.

¹⁸ <http://www.aftenposten.no/okonomi/Okokrim-advarer-mot-CEO-svindel---norske-bedrifter-rammet-av-millionbedrageri-8382868.html>

¹⁹ <https://securityintelligence.com/mobile-malware-threats-in-2015-fraudsters-are-still-two-steps-ahead>

Finanstilsynet considers that the information provided by financial institutions to consumers on how to protect themselves against online and mobile-based fraud is steadily improving.

3.2.7 Overview of annual losses related to payment services

The tables below present figures for the last five years for losses due to credit card and online banking fraud in Norway. The figures have been obtained from Finance Norway (FNO) and the Norwegian Banks' Standardisation Office (BSK) in collaboration with Finanstilsynet.

3.2.7.1 Losses in Norway related to use of cards

In 2015 there was again a substantial increase in losses due to Card-Not-Present (CNP) fraud. With an increase of close to 37 per cent, losses have almost doubled in two years and have risen by 307 per cent in five years. Total losses related to other types of payment card fraud remained more or less unchanged.

Overall, there was a 15 per cent increase in payment card losses in 2015. In five years, losses have risen by 50 per cent.

Table 1: Payment card losses (figures in NOK 1 000)

Type of payment card fraud	2011	2012	2013	2014	2015
Fraudulent use of card information, Card-Not-Present (CNP) (online transactions etc.)	24 190	35 701	51 954	72 056	98 410
Stolen card information (incl. skimming), fraudulently used with counterfeit cards in Norway	468	2 308	762	524	2 670
Stolen card information (incl. skimming), fraudulently used with counterfeit cards outside Norway	57 340	55 869	51 534	51 685	48 447
Original cards lost or stolen, fraudulently used with PIN in Norway	32 224	28 128	21 274	21 266	18 875
Original cards lost or stolen, fraudulently used with PIN outside Norway	7 008	8 544	9 570	13 071	14 224
Original cards lost or stolen, fraudulently used without PIN	4 488	4 603	4 949	5 510	6 033
TOTAL	125 718	135 153	140 043	164 113	188 660

Source: Finanstilsynet

From 2013 to 2014, the total volume of card transactions in Norway rose by 7.6 per cent, while the volume of card payments for online purchases increased by 21 per cent (figures from Norges Bank 2014²⁰). Fraud increased by 37 per cent from 2014 to 2015 (from approx. NOK 72 million to approx. NOK 98 million). Over 0.14 per cent (1.4 per thousand) of online transactions were fraudulent. Of the total volume of payment card transactions in Norway, around 0.023 per cent were fraudulent²¹.

²⁰ Norges Bank does not publish figures for 2015 until May 2016. The comparisons are therefore based on Norges Bank's figures for 2014.

²¹ http://static.norges-bank.no/pages/103291/NB_memo_1_15.pdf?v=29062015145622&ft=.pdf

Table 2: Number of payment cards affected by fraud

	2011	2012	2013	2014	2015
Number of cards affected by fraud	16 784	20 332	22 531	38 541	44 900

Source: Finanstilsynet

Compared with 2014, the number of cards affected by fraud rose by 16.5 per cent in 2015. In the past five years, there has been an increase of 168 per cent. The increase in the number of fraudulently used cards in 2015 is lower than the increase in total payment card losses in 2015, which means that the average loss per fraudulently used card increased.

3.2.7.2 Payment card fraud and data theft

Card data theft has been a pervasive and profitable activity for several years, and this trend continues to grow. Operational sites where large quantities of card-related data²² are stored or transmitted are the most vulnerable.

CNP losses continue to rise, at both Norwegian and European level (see 3.2.7.5²³). These are primarily losses arising from fraudulent use of stolen card data in online stores that do not require 3-D Secure authentication. The failure of the e-merchant to require 3-D Secure authentication, instead only requiring use of the CVC code, poses a risk to consumers in payment services. Payment card data, if stolen, are easy to use in fraudulent transactions in online stores that do not require 3-D Secure authentication. Stolen card data can easily be sold on the “Dark Web”²⁴. Fraudulent use of stolen card data primarily takes place outside Norway.

To counteract this trend, the EBA drew up guidelines on the security of internet payments. Finanstilsynet has declared that these guidelines will form the basis for its oversight activities. The guidelines entered into force on 1 August 2015 (see 5.2.2), and target both issuers and acquirers of payment cards, but indirectly also online stores. The revised Payment Services Directive (PSD2) (see 5.1.1) also contains provisions designed to combat this negative trend.

Although the financial industry in Norway is implementing numerous measures and is in the vanguard of global efforts to reduce vulnerability, there is still room for improvement. Magnetic stripe readers are still in use, making it a simple matter for criminals to use stolen card data for fraudulent purposes.

Figures from Norges Bank show that the total value of online purchases in 2014 was NOK 69 billion. CNP losses totalling NOK 98 million account for 0.14 per cent, or 1.4 per thousand of NOK 69 billion. Card payments totalled NOK 807 billion in 2014. Payment card losses, which totalled NOK 188 660 million, accounted for 0.233 per cent of NOK 807 billion.

²² <http://newsroom.hyatt.com/news-releases?item=123453>

²³ https://www.ecb.europa.eu/pub/pdf/other/4th_card_fraud_report.en.pdf

²⁴ <https://no.wikipedia.org/wiki/Dypnettet>

3.2.7.3 Costs related to payment card fraud

Finanstilsynet has prepared an estimate of total costs related to stolen payment card data. The calculation is based on the sum of annual payment card losses and the estimated average administrative cost for the card issuer per fraudulently used card. A cost per card has also been estimated related to the costs incurred by the consumer in connection with stolen card data. (Administrative and consumer costs are kept constant for the period 2011–2015).

In addition to the costs presented in Table 3, there are further costs related to payment card fraud, including administrative costs incurred by card acquirers, merchants and the Norwegian Financial Services Complaints Board and costs in the form of lawyers' fees and court costs.

Table 3: Costs related to payment card fraud (amounts in NOK 1 000)

Costs related to payment card fraud	2011	2012	2013	2014	2015
Number of cards affected by fraud, see Table 2 (number)	16 784	20 332	22 531	38 541	44 900
Total direct losses, see Table 1	125 718	135 153	140 043	164 113	188 660
Administrative costs card issuer (NOK 2 250 per card)	37 764	45 747	50 695	86 717	101 025
Consumer costs, NOK 1 000 per card	16 784	20 332	22 531	38 541	44 900
Total estimated costs	180 266	201 232	213 269	289 371	334 585

Source: Finanstilsynet

The total costs incurred in connection with payment card fraud are therefore substantial. The percentage increase in card fraud costs exceeds the increase in the total volume of card transactions. Furthermore, significant amounts are spent on preventive measures and transaction and fraud monitoring to prevent the occurrence of payment card fraud.

3.2.7.4 Losses related to use of online banking

As reported in 3.9, online banking fraud attacks, particularly on corporate online banking, increased in 2015, but the losses are not large. However, they could have been far greater if the banks had not succeeded in stopping most of the fraudulent transactions before they were executed or had the funds returned by the payee bank. On the other hand, it might be reasonable to include the banks' investments in fraud prevention measures (monitoring and intelligence) when calculating the total costs.

Online banking fraud methods are constantly evolving. It is therefore more difficult to categorise types of online banking fraud than types of payment card fraud. Losses resulting from real-time phishing attacks (see 3.2.6) are presented on the line for "Phishing and false BankID merchants" in table 4.

Table 4: Losses related to the use of online banking (figures in NOK 1 000)

Type of online banking fraud	2011	2012	2013	2014	2015
Attacks using malicious software on customer's PC (Trojans)	664	5 064	1327	552	3055
Lost/stolen security device	3 321	3 367	1 285	6 655	963
Phishing and false BankID merchants		10		539	5815
Other/unknown		358	779	3474	2715
TOTAL	3 985	8 799	3 391	11 220	12 548

Source: Finanstilsynet

3.2.7.5 Losses in other European countries

Loss statistics are published at different times in different countries, and few countries publish loss figures as early as Norway. The comparisons below may therefore be between different years, but they nevertheless provide an indication of where Norway stands.

Payment card transaction losses are rising in Norway, as elsewhere in Europe. CNP losses are on the rise. The increase appears to be particularly high for Norway (see 3.2.7.1), but in Norway there is also a substantial increase in the use of payment cards for online transactions. Losses relating to online banking fraud vary more from one country to another. While these losses have increased in the UK and Norway, the same trend has not been seen in the Netherlands or Belgium. Online bank attacks have often been seen to move from country to country over a period of time. Loss statistics published by other countries that it is relevant to compare with Norway are presented below.

Payment cards

The Fourth Report on Card Fraud²⁵ issued in July 2015 by the European Central Bank (ECB) showed that the value of payment card fraud in European countries increased by 8 per cent from 2012 to 2013. CNP losses accounted for 66 per cent of the fraud losses, POS for 20 per cent and ATM for 14 per cent. CNP fraud was the only type of fraud that increased, but online transactions also accounted for a steadily growing percentage of the total use of payment cards.

Domestic transactions accounted for 92 per cent of the total number of card transactions, but only 49 per cent of fraudulent transactions. A total of 6 per cent of transactions in the Single European Payments Area (SEPA) were cross-border, but accounted for 29 per cent of fraudulent transactions. Around 2 per cent of transactions outside SEPA were cross-border, but accounted for 22 per cent of fraudulent transactions.

In the UK²⁶, payment card losses increased by 6 per cent from 2013 to 2014. CNP fraud (called remote purchase fraud in the UK) rose 10 per cent. CNP fraud is by far the biggest type of fraud in terms of

²⁵ https://www.ecb.europa.eu/pub/pdf/other/4th_card_fraud_report.en.pdf

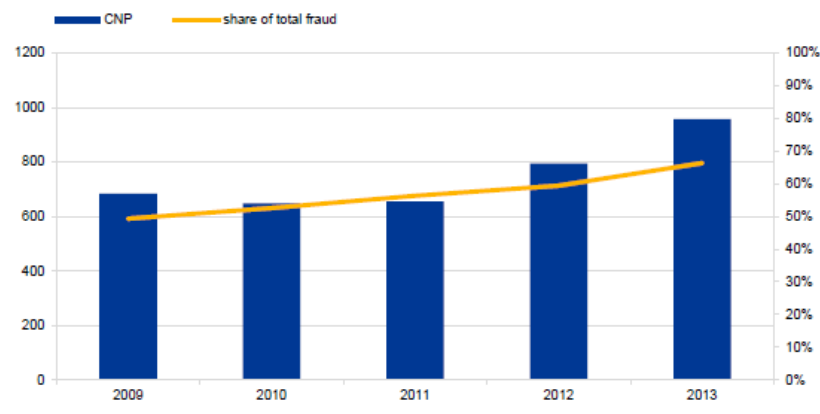
²⁶ <http://www.financialfraudaction.org.uk/Fraud-the-Facts-2015.asp>

both the value of fraud losses and the number of cards that are fraudulently used. CNP fraud in connection with transactions in online stores outside Norway increased the most (22 per cent).

Figure 2:

Evolution of the value of CNP fraud and its share of the total value of fraud¹²

(EUR millions; share of total card fraud)



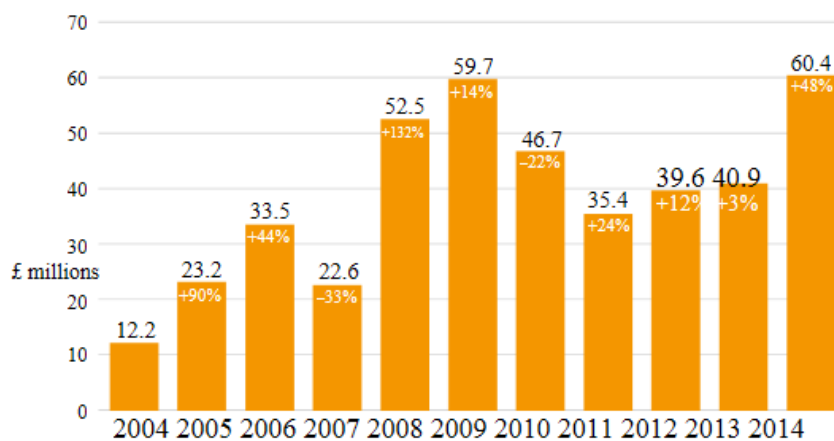
Source: ECB: Fourth report on card fraud

With fraud involving counterfeit payment cards, details from the original card's magnetic stripe are copied. These are then used to make counterfeit cards for use in countries that have not yet upgraded to Chip & PIN. The USA is the country where the most counterfeit cards from the UK are used, and counterfeit cards from the USA are the most frequently used counterfeit cards on UK websites.

Online banking

Figure 3:

Online banking fraud losses 2004–2014



Figures in white show percentage change on previous year's total

Source: Financial Fraud Action UK: Fraud The Facts 2015

There was a substantial increase in online banking fraud in the UK in 2014. The 48 per cent rise was attributable to a change in attack patterns, where the fraudster uses social manipulation and phishing through a variety of channels.

On the other hand, online fraud losses were low in Belgium²⁷ and the Netherlands²⁸, in both 2014 and 2015.

3.3 Banking

ICT deliveries are being spread across a larger number of service providers due to new cooperation agreements and amendments to existing outsourcing agreements. There is growing use of external service developers, often from low-cost countries. Cost savings are one of the main reasons for these changes, but the acquisition of expertise is also cited as a reason. Where security is concerned, however, several of the financial institutions lack expertise, which is a cause for concern in the long run in light of the anticipated increase in the threat of online attacks. Due to the extensive changes, a decline in the stability of operating services might normally have been expected, but that is not the case. The financial institutions have invested considerable resources in these changes, and have maintained control of processes.

Finanstilsynet has drawn the attention of the financial institutions to a number of areas where improvements should be made. The main findings are described in the chapters below.

3.3.1 Follow-up of internet service providers (ISP)

By virtue of its function as a means of transport for information exchange, the internet is a critical component of banks' product portfolio. Financial institutions' monitoring of providers of critical infrastructure is crucial for ensuring that the agreements established are relevant and that the agreed level of service is delivered.

In Finanstilsynet's experience, not all undertakings monitor the services delivered by ISPs as extensively as deliveries from other traditional service providers.

3.3.2 Access control

Reviewing the access of individual employees to systems, databases and file areas is important as a means of protection against unauthorised access to the undertakings' ICT infrastructure.

Finanstilsynet's findings in ICT inspections show that the lists used to review access rights are long and have a format and content that can make it difficult to determine which systems, databases and file areas each employee has access to. In Finanstilsynet's view, the quality of access lists should be improved to make it easier for the business manager to carry out effective checks. This also applies to access to applications with their own access management capabilities.

²⁷ <https://www.febelfin.be/en/stable-level-internet-banking-fraud-2015-rising-number-bank-card-phishing-cases>

²⁸ <http://www.nvb.nl/publicaties-standpunten/publicaties/4522/veiligheid-en-fraude.html>

3.3.3 Test environment

In conducting ICT inspections, Finanstilsynet has found that only a very few financial institutions have test environments that correspond to production environments. There is a particular lack of end-to-end test environments. This increases the risk that the testing will not adequately detect deficiencies in new or changed solutions. Ensuring that the testing carried out is based on specified criteria is also a challenge.

3.3.4 Online security

Efforts to ensure online security are being intensified in response to the increasing risk of digital attack, but the work is challenging due to the scarcity of specialised expertise and sufficient resources. Finanstilsynet considers it positive that banks appear to be making growing use of penetration testing.

Through ICT inspections, Finanstilsynet has found deficiencies in monitoring of security systems, log monitoring, processing of network equipment reports and security levels. As a result, unauthorised activity, both internal and external, may be hard to detect and it may consequently be difficult to put measures in place to prevent such activity.

Blackmail has become an increasingly common threat, also to banks. Finanstilsynet is aware that banks have received e-mails demanding ransom at about the same time as they are subjected to minor DDoS attacks. The e-mail contains a threat of a stronger DDoS attack if the ransom is not paid before the deadline expires. To Finanstilsynet's knowledge, no ransom has been paid in any of these instances, nor did the attackers carry out the attack as threatened. Finanstilsynet also received reports from banks that had been subjected to the encryption (see 3.10.2) of file areas, accompanied by demands for ransom for decryption (ransomware). As far as Finanstilsynet knows, no ransom was paid in any of these cases either. This type of attack is often costly for banks, especially due to lost work time due to lack of access to systems and data. Restoring ICT systems and data to normal operation is a comprehensive and expensive process.

3.3.5 Follow-up of internal ICT audit reports

Internal audits are an important part of financial institutions' control procedures. In Finanstilsynet's experience, undertakings' internal ICT audit reports are largely thorough and of high quality. In its inspections, however, Finanstilsynet has noted that, in a number of cases, the follow-up of measures proposed in the reports and the deadlines for implementation of the measures have not been documented, even if the activity has been carried out and completed.

3.3.6 Data quality – reporting to the Norwegian Banks' Guarantee Fund

In its supervision of compliance with the Regulations of 22 March 2013 No. 330 relating to computer software requirements and reporting to the Norwegian Banks' Guarantee Fund, Finanstilsynet has noted that the banks have largely established reporting systems in compliance with the regulatory requirements. An accompanying letter based on the guidelines to the Regulations is often attached.

Finanstilsynet has asked the banks to devote a little more effort to the accompanying letter so as to provide better documentation for potential disbursements from the Norwegian Banks' Guarantee Fund.

The inspections revealed a number of deficiencies in the quality of the information provided, which could have had consequences in the event of a disbursement from the Norwegian Bank's Guarantee Fund. It is important to verify the Guarantee Fund's lists to ensure that the information provided to the Fund is complete, thereby ensuring that all customers and the correct data are included in the information extracted from the bank's systems.

3.4 Securities

Finanstilsynet's general impression of the ICT systems in the Norwegian securities sector is that the systems are of high quality and high stability. The challenge in the future will be to ensure that risk remains at an acceptable level given the technological changes that Finanstilsynet anticipates, combined with the steadily growing outsourcing of ICT systems in the sector.

3.4.1 Information leaks

Preventing information leaks from investment firms' corporate departments and banks' marketing departments is vital for the investment firms and their customers and for maintaining confidence in the Norwegian financial sector. The banks' and investment firms' ICT systems are a key source of this type of information leakage and must therefore be effectively protected against unauthorised access.

3.4.1.1 Inadequate outsourcing control

The outsourcing of ICT systems has expanded in the securities sector as well in the past few years. In light of the need to reduce operating costs and share the costs of specialised systems, combined with the increasingly rapid pace of systems development, a growing number of investment firms are outsourcing substantial parts of their systems portfolio. This trend makes new demands on the firms' executive management in terms of ensuring that the risk assessments carried out prior to making such decisions are of high quality. Under the Norwegian ICT Regulations, the firm's governance of outsourced systems must be no less effective than its governance of systems administered, developed and operated by the company itself.

The ICT Regulations' provision on outsourcing also points out that the firm must have an unlimited right to inspect, audit and supervise all elements of significance for delivery of the outsourced system. In the case of investment firms, Finanstilsynet has noted the outsourcing of ICT systems with price-sensitive data where the firm neither exercises control in respect of the operating companies' users, nor has secured the possibility, in its agreement with the service provider, to receive and verify information on which operations personnel have had access to the data. This issue could, for instance, have been resolved by ensuring that systems run on an outsourced platform use encryption technology managed by the firm itself, while the platform is operated by the service provider.

3.4.1.2 Failure to classify sensitive information

In its inspections, Finanstilsynet has observed that many investment firms have inadequate or poor guidelines and procedures for classifying sensitive information. As a result, the security of exchanges and storage of this type of information may be impaired. This is particularly important for departments that handle price-sensitive information, such as the corporate departments of investment firms.

3.4.1.3 Inadequate security in e-mail exchanges

Through its supervisory activities, Finanstilsynet has seen that investment firms often pay insufficient attention to security in connection with use of e-mails. Establishing user procedures and conducting information campaigns will not suffice to achieve an appropriate level of e-mail security. Firms must also have control of the way their e-mail servers are configured.

E-mail servers' encryption function is often set up in such a way that the server negotiates with the counterpart server on the level of encryption to be used during a transmission. If the counterpart server does not support encryption, an encrypted e-mail may nevertheless be sent unencrypted without the sender being aware of the fact or given the opportunity to stop the transmission (opportunistic encryption). In firms that regularly exchange sensitive information with a counterpart, communication can be secured by entering into agreements stipulating a level of classification for encryption. Firms may also configure e-mail servers so that they can only send and receive encrypted e-mails from specific counterparts (forced encryption). Most e-mail systems are designed to be able to verify the identity of the counterpart's e-mail server by forcing it to use certificates.

Finanstilsynet has also found low awareness of the risk associated with the fact that an e-mail, on its way from sender to recipient, may pass through several e-mail servers and network hubs (SMTP servers), where it can be read in unencrypted form. This is possible because it is the communication, not the e-mail itself, that is encrypted. This type of encryption only provides protection against line tapping.

If an e-mail transmission contains highly confidential information, messages and any attachments should be encrypted before they are sent.

3.4.1.4 Use of third-party systems for information exchange

To a large extent, investment firms lack guidelines for use of third-party systems employed to exchange sensitive information. Third-party systems may be project tools, cloud-based file systems or other similar solutions that the client prefers and that are often used without the investment firm performing relevant risk analyses or setting security requirements for the systems. An investment firm is a professional party in a business relationship and is responsible for ensuring the secure communication of sensitive information. Firms should have procedures for and descriptions of the ways in which such communication is to be handled. The procedures should be differentiated according to the type of information and their respective security requirements.

3.4.2 Monitoring of voice recording systems

The Norwegian Securities Trading Regulations lay down requirements concerning voice recordings in investment firms. In 2015, Finanstilsynet noted several incidents in which voice recordings were not made due to the technical failure of the recording equipment. Several of these incidents went on for a long time without the failure being discovered by the firm. This shows that the firms have had inadequate procedures for checking the recording operation and inadequate electronic monitoring of the recording systems. Finanstilsynet will now take a closer look at investment firms' checking of voice recording systems and their procedures for monitoring these systems.

3.4.3 Outsourced order systems

Several major fund and capital management companies and a number of brokerage companies are currently using systems provided by third-party companies to handle the flow of orders between investment managers and brokers. The market for this type of system is dominated by a small number of large foreign companies. What is common to all these systems is that they handle price-sensitive information, and that the tasks they now perform used to be carried out by the investment firms themselves. Finanstilsynet therefore considers this type of third-party solution to be an outsourcing of ICT systems.

Through its supervisory activities, Finanstilsynet has uncovered agreements between investment firms and providers of outsourced order systems that are inadequate in terms of ensuring that the firms are able to check and audit the service provider's activities under the agreements.

3.4.4 Suppliers' ability to deliver in critical situations

Tests of contingency preparedness solutions and incidents that have occurred have shown that contingency agreements with infrastructure providers on the advance storage of equipment are no guarantee that a firm will have access to equipment as agreed in a critical situation. Many investment firms have chosen the same product from the same supplier and signed agreements on contingency storage of extra components with the same supplier. Finanstilsynet considers it a risk that suppliers have a smaller quantity of each component in an on-site storage facility than the total quantity to be supplied under the agreement between the supplier and its customers, as they consider it unlikely that all the components will need to be replaced at all the firms simultaneously. In situations where several firms experience problems with their components at the same time (e.g. in connection with a power grid failure), suppliers could have difficulties meeting their obligations. If so, the investment firm would not be able to deliver the expected operational security. Investment firms must therefore include this as a factor in risk assessments of their own ICT infrastructure.

3.4.5 Risk assessments and system ownership

In connection with several inspections, Finanstilsynet noted that the investment firms' management has shown little interest in the firms' ICT activities. Finanstilsynet has observed cases where the ICT department is stated to be the formal system owner of the firm's core systems without there being any guidelines for such ownership, nor any documentation that decisions are made in consultation with the rest of the firm's management. As a result, risk analyses of the firms' ICT systems lack a holistic and

business dimension, in addition to which the firm's management lacks the full picture of the firm's ICT risk.

The lack of involvement on the part of the investment firms' management in the outsourcing of the firms' ICT activities has resulted in contracts that do not regulate access to the firms' data. This may increase the risk of information leaks. One example is a firm that outsourced the operation of systems with price-sensitive information. The information was made available to the supplier's operations personnel by means of user accesses. The service provider gave many of its employees administrator rights with access to the firm's sensitive data, while the investment firm itself had no possibility of monitoring which persons had access to these systems. No log was kept of access to sensitive data, besides which the service provider's administrators had the right to erase digital tracks. The investment firm thus had no way of knowing who might have accessed the sensitive data or how this information might have been used.

3.4.6 Ransomware attacks

Finanstilsynet has seen that in the course of 2015 investment firms experienced cases of phishing that resulted in CryptoLocker attacks (see 3.10.2). Firms have had their network disks encrypted and received demands that a ransom be paid in Bitcoin. This has caused operational disruptions lasting more than 24 hours due to inaccessible network disks. These incidents show that even with effective, proactive efforts to avoid CryptoLocker attacks, firms are nonetheless dependent on a reactive security approach in the form of systems for security backup, well-functioning procedures and tested preparedness plans.

3.5 Insurance

Some insurers are part of a larger bank or insurance group, while others are independent entities. Several companies collaborate closely with banks and use the banks' distribution and sales networks. The size of the companies and the products they offer vary. The differences are reflected in the companies' use of ICT, the organisation of their ICT activities and their ICT risk picture.

The companies largely outsource their ICT activities, which appears to be a growing trend. The companies are innovative in their use of new technology in their systems. Like other financial institutions, insurers are targets for external data attacks, a threat that demands constant attention and adequate resources (see 3.10).

Inspections have revealed areas of risk on which greater attention should be focused; see the information below.

3.5.1 Risk related to complex insurance systems

As Finanstilsynet has reported in previous risk and vulnerability analyses, the insurance industry generally has numerous large-scale, complex systems involving a great deal of business logic, laborious actuarial calculations and interfaces with many other systems. Faults and deficiencies in the

systems may have consequences for the companies' financial statements and customers' premiums and compensation.

As stated in 5.2.4, the insurance sector is subject to a multitude of regulatory amendments, necessitating major changes in ICT systems. The companies' expertise with regard to the various systems, the quality of the ICT processes used to carry out the changes and compliance with these are crucial to ensuring control of the changes and that the quality of the systems is not impaired by the changes.

A number of companies buy specialised systems from external suppliers, in which case the supplier carries out the system changes. Finanstilsynet assumes that the companies, in accordance with the requirements regarding outsourcing in the Regulations on Risk Management and Internal Control and the ICT Regulations, have sufficient system expertise and take active part in and assume responsibility for the changes that are made.

3.5.2 Failure to comply with the ICT Regulations' requirements regarding incident reporting

Under section 9 "Problem and change management" of the ICT Regulations, financial institutions must report to Finanstilsynet any incidents that lead to a material reduction in functionality as a result of a breach of confidentiality, integrity or availability of ICT systems and/or data. Of the 148 incidents reported in 2015, 14 were from insurers. This is an increase from the previous year. Finanstilsynet's Incidents Seminar 2014 targeted insurers in particular, and this may have had some effect.

Under the ICT Regulations, reporting to Finanstilsynet must normally cover incidents which the undertakings themselves classify as serious or critical. However, the Regulations state that reporting may also cover other irregularities if they expose vulnerabilities in applications, architecture, infrastructure or defence mechanisms. Generally speaking, this is a point of which not all undertakings are aware. Finanstilsynet does not rule out the possibility that there may have been irregularities resulting from vulnerabilities in insurers' applications that should have been reported to Finanstilsynet.

3.5.3 Inadequate risk assessments

Many insurers still need to carry out better, more holistic risk assessments that show the overall risk related to the company's use of ICT. Inadequate, fragmented risk assessments make it difficult to manage the company's ICT risks and ensure that they remain within specified limits and that the companies are achieving their goals and strategies.

3.6 Accounting firms

In 2015, Finanstilsynet conducted a document-based inspection of accounting firms. The purpose of this thematic inspection was to identify ICT risk in authorised accounting firms, raise awareness of ICT risk in the accounting sector and improve compliance with the Regulations on Risk Management and Internal Control and generally accepted accounting practice.

Accounting firms make extensive use of hardware and software technology in their activities. If these tools fail, it can have serious consequences for their clients. ICT risk must be handled in accordance with the Risk Management Regulations. The responses received in the thematic inspection show that not all accounting firms operate in compliance with the Regulations.

It is important that accounting firms do not perceive the Risk Management Regulations to be a "formal requirement", because in that case the Regulations would not have the desired effect. Only if a genuine assessment is made, based on the actual situation in the individual accounting firm, will the Regulations be an effective tool for the Board of Directors and general manager in fulfilling their responsibilities under the Act on Authorisation of External Accountants, company legislation and other relevant legislation. Compliance with the Regulations will contribute to ensuring sound risk management and internal control of all of the accounting firm's activities, including ICT operations, whether or not they are outsourced. The results of the thematic inspection indicate that a number of accounting firms must make more thorough assessments of the need to take steps to reduce the risk related to the ICT systems used in their activities. Measures necessary to fulfil the statutory requirement of "generally accepted accounting practice" (the GRFS standard) must be carried out.

The thematic inspection also gives reason to believe that the agreements entered into between accounting firms and providers of ICT systems used by the firms in their activities do not adequately assure the accounting firms of the rights necessary to enable them to fulfil their obligations under the law, including their responsibility for risk management and internal control.

3.7 Joint efforts by the financial industry

Banks, other key financial sector operators and Finance Norway collaborate on security, the development of shared infrastructure, services and common standards. They exchange and discuss the results of incidents, monitoring, analyses and statistics and decide on the action to be taken.

In 2015, the financial industry decided to concentrate its efforts to optimise payment services in a new, strengthened infrastructure company – Bits²⁹. The company, which became operational on 1 April 2016, comprises the Norwegian Banks' Standardisation Office (BSK) and Finance Norway's specialised payment services unit.

The financial industry's scope for self-regulation is changing due to amendments to laws and regulations, not least to changes being introduced by the EU. This will compel the financial industry to include new payment service operators in its collaboration (see 5.1.1).

BSK has worked to modernise the banks' online transaction exchange system Baltus, thereby providing a flexible, secure infrastructure for the routing and transport of transaction-related financial

²⁹ <https://www.fno.no/aktuelt/nyheter/2016/03/bits-i-drift-fra-1.-april/>

enquiries between banks linked to the shared Norwegian infrastructure. The system came into use in 2015. The plan is for all banks to begin using the new infrastructure in the first half of 2016.

Work on making the transition to ISO 20022 is continuing. This process will entail major changes in the Norwegian payment infrastructure in the next few years. It is important that this work takes place in a coordinated and controlled manner, in the interests of both security and stability.

The financial industry has worked to improve identity control by distributing security tokens to be used with BankID, both through Posten's secure personal delivery service (PUM) and in the banks' own procedures. These measures are expected to be introduced in the course of 2016.

FinansCERT, the Norwegian financial sector cybercrime unit, was established as a private-sector computer emergency response team (CERT) and is an important instrument in the financial sector's efforts to counter digital threats and computer security incidents. In addition to acting as a coordinating link between the various financial institutions in this work, FinansCERT has actively sought to establish relations and cooperation agreements with other key data security operators, both national and global. To optimise the effectiveness of efforts to combat digital threats and incidents in the financial sector, it is essential that public-private sector cooperation is as flexible and efficient as possible.

Since BankAxept was established in 2014, the company has focused on building up the organisation and on modernising the Norwegian payment card system to enable contactless payment and new digital services.

3.8 Changes and outsourcing

3.8.1 Changes in the service provider market

When service providers are sold or undergo changes of ownership, it is important that established procedures and collaborative processes are adapted to and adopted by new partners. It is primarily the task of the financial institutions to ensure that this is done. This also applies if a service provider acquires a new sub-contractor.

The sale of **Evry**³⁰ was completed in 2014, and in 2015 Evry entered into an outsourcing agreement with IBM for the operation of its mainframe. The operations centre, Greenfield Data Center, is located in Fet, Akershus County.

Nets spun off its Norwegian business in 2015, which became a branch of the Nets group in Denmark, but will maintain its operations in Norway. Nets Norge Infrastruktur AS, which operates the banks' clearing system NICS, is still a separate Norwegian company.

³⁰ Described in the RAV Report for 2014.

Sandnes Sparebank became part of Eika Alliansen in 2015 and moved its ICT operations to the Eika Banks' operations centre at Eika Alliansen and SDC in October 2015.

DNB chose HCL as its new partner for decentralised platform operations in 2013. In 2015, DNB moved its server park (not mainframe) to the Green Mountain Data Centre 1 on Rennesøy in Rogaland County, and is in the process of establishing a back-up site for its mainframe there, as well as a back-up site for its server park at the Green Mountain Data Centre 2 at Rjukan in Telemark County.

DNB has entered into development and maintenance agreements with Infosys and Tata Consultancy Services (TCS) for parts of its systems portfolio.

Nordea has re-insourced all the operations previously provided by Nordic Processor, except for mainframe core operations (HW/OS), which from now on will be provided to Nordea by IBM and HP, respectively. This means that Nordic Processor will be wound up.

Large parts of its server park (mid-range) and associated systems have already been moved from IBM/NP's data halls in Solna and Kista to Nordea's own data halls in Denmark.

Nordea has also begun work on a project to renew its core systems. It has chosen systems from Temenos, which are being implemented in collaboration with Accenture.

3.8.2 Outsourcing notifications

In 2015, Finanstilsynet received over 100 notifications regarding outsourcing under section 4c of the Financial Supervision Act.

In view of the financial institutions' differing assessments of what requires notification and significant variations in the notifications received, Finanstilsynet sees a potential need to specify in greater detail when the duty of notification arises and how the notification should be formulated.

In previous annual RAV analyses, Finanstilsynet has pointed out that it deems the use of cloud services to be covered by the rules regarding traditional outsourcing. In 2015, Finanstilsynet received notifications from undertakings wishing to make use of systems supplied by major global cloud service providers. The Norwegian financial industry, in particular banks, has outsourced ICT services for several decades, and to a large extent the services have been shared by several undertakings. In principle, these are the same type of services that are today called cloud services. Improved technology has made it easier for service providers to offer this type of delivery model and thus offer infrastructure, platforms and software as a bundle or separately. If desired, they can be supplied by a service provider's data centres in different geographical places.

In assessing the outsourcing notifications, Finanstilsynet attaches importance to whether the undertaking has carried out a risk analysis and an independent assessment of the outsourcing arrangement. In its processing of outsourcing notifications, Finanstilsynet has seen deficiencies in the

risk analyses performed, the undertaking's independent assessments of the outsourcing and its compliance with applicable laws and regulations. Among other things, Finanstilsynet has followed up on notifications in cases where the agreements do not take sufficient account of regulatory requirements, such as the requirements in the ICT Regulations or the Regulations on Risk Management and Internal Control to the effect that undertakings under supervision must be given the right to inspect, including audit, the service provider's activities covered by the agreement.

3.9 Incidents reported in 2015

Pursuant to the Regulations on the use of information and communication technology (the ICT Regulations), financial institutions are required to report serious incidents in their ICT systems. Finanstilsynet monitors undertakings to ensure that they analyse the incidents, that the root of the problem is found and that possible preventive measures are identified. In the event of particularly serious incidents, Finanstilsynet also requires a plan for implementing the preventive measures. As a general rule, incidents and preventive measures will be monitored through supervisory inspections.

3.9.1 Incident statistics

The statistics below are based on reports from the undertakings. Fewer operating incidents and higher availability of technology-dependent financial services were reported in 2015 than in previous years. However, fraudulent attacks on financial institutions increased. Although they had little impact on overall availability, the attacks were a serious inconvenience to the affected customers and undertakings.

Figure 4: Number of reported incidents in the period 2013–2015

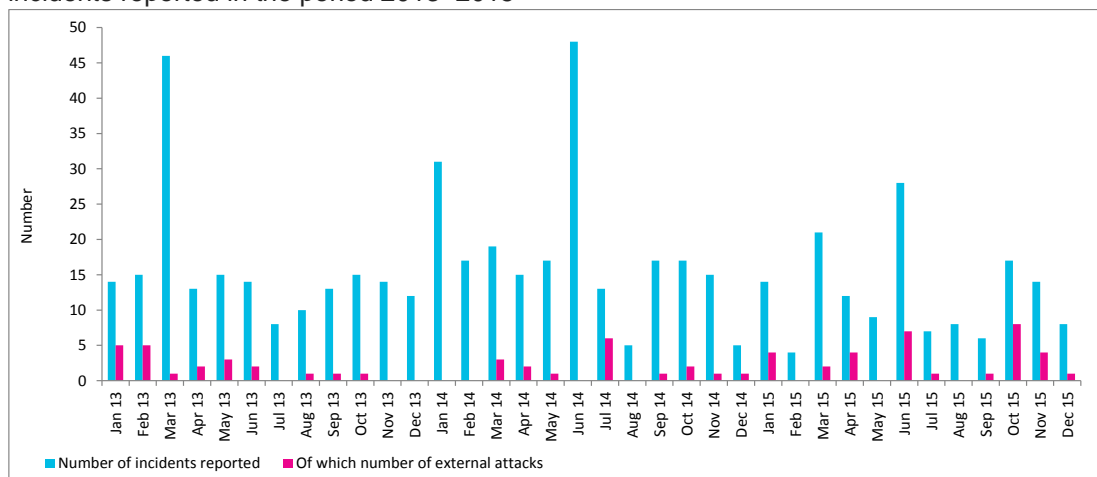


Source: Finanstilsynet

The causes of the operating incidents can be roughly broken down into faults and failures after changes, inadequate capacity planning, and failure to monitor parameters such as expiry dates, fill

ratios and threshold values. There is still potential for improvement, both in the procedures themselves and in using them as they are intended to be used.

Figure 5: Number of reported external attacks (malicious attacks) and total number of incidents reported in the period 2013–2015



Source: Finanstilsynet

Incidents that impacted BankID in May and June, and hence many financial institutions at the same time, were the most serious operating incidents in 2015. The incidents affected banks and payment services in particular. There were several incidents with different causes, but Finanstilsynet did not consider any of them critical to the availability of financial services.

Several network incidents that affected mobile services, including BankID, were reported. The consequences of faults in the mobile network are growing, as an increasing number of services are based on the availability of network infrastructure for mobile services.

Global changes in the internet affected Norwegian payment services and BankID in June, 2015. The network for parts of the Norwegian payment infrastructure was unstable as a result of a change made by a telecoms supplier in Malaysia. The cause was a routing table error. The supplier in question did not have sufficient control of which addresses belonged to which customers.

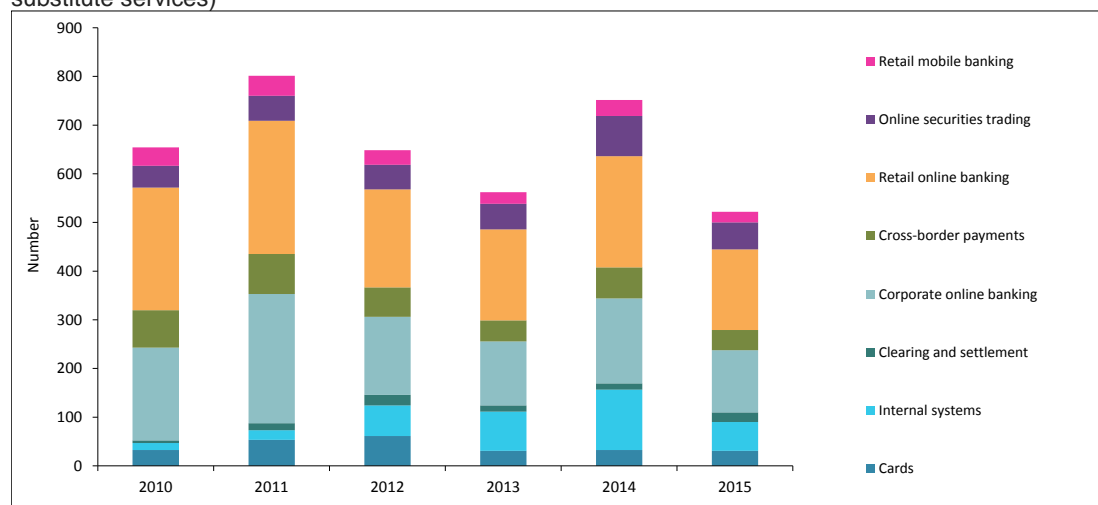
There was an increase in fraud targeting internet banking services in 2015, particularly corporate online banking, where transactions are large; see 3.2.6. Banks, insurers and investment firms reported attacks employing ransomware in 2015; see 3.10.2.

The majority of incident reports from insurers companies concerned application faults after changes. Operating problems were the second most common. The majority of incidents in the investment area were associated with operating problems, a number of them relating to failure to record telephone calls.

3.9.2 Analysis of incidents as a measure of availability

For each incident that has impacted availability, Finanstilsynet considers the duration of the disruption, the number of undertakings affected, the estimated number of customers affected and whether there are substitute services customers can use. This gives Finanstilsynet an index of the unavailability of the payment system and customer-facing solutions each year, and makes it possible to follow developments over time.

Figure 6: Incidents weighted according to impact (weighting: users affected, duration, time of incident, substitute services)



Source: Finanstilsynet³¹

Figure 6 shows that the availability of the payment system and customer-facing solutions to customers was greater in 2015 than in 2014, despite the fact that a number of undertakings changed their operating site and supplier in 2015, which entails a certain risk of downtime during the transition. The undertakings are now distributed among more operations service providers than previously. All else being equal, this means less risk of many undertakings being unavailable at the same time.

3.10 Observations of digital crime (cybercrime)

Cybercrime targets both undertakings and private customers. Undertakings are hit by DDoS and APT attacks, the computers of private customers are infected with malicious code. Phishing is an increasingly central aspect of cybercrime, targeting both undertakings and end-users. An important part of the fraudster's value chain involves gaining the victim's trust. In order to access really large sums, phishing is given a professional touch in the form of targeted approaches from a party claiming to be a named acquaintance or colleague of the victim. Phishing channels include the telephone, e-

³¹ I den grafiske fremstillingen er utligneligheten for aksjehandel på Internett rekalkulert for alle år i figuren, fordi foretakene rapporterer at de har gode erstatningstjenester for tilfellet at aksjehandel på Internett er nede. Erstatningstjenestene består av at foretakene på kort tid bemanner opp, slik at de kan ta imot og utføre ordrer manuelt.

mail, SMSs or phone calls with predefined response options (interactive voice response – IVR). The methods can be used alone or in combination with others.

3.10.1 CEO fraud

CEO fraud is the name given to attacks where an employee, often one with financial responsibility, is contacted by phone and/or e-mail by a party who is ostensibly the CEO, but in reality is a fraudster. The employee is asked to conduct specific monetary transactions. For market-related reasons, confidentiality is requested surrounding the transactions, which makes it easier for the fraud to succeed. The attacks target undertakings of different types.

Very large sums are often transferred in CEO fraud. As with internet banking fraud, mule accounts are needed to receive the fraudulent transactions. As a rule, the transactions are made to another country, preferably one in which it is difficult to trace them. CEO fraud affects all types of undertakings, and banks are directly impacted when a bank employee is the victim. Banks also have close encounters with fraud when the bank's corporate customers are affected, because the large fraudulent transactions take place through the bank. Successful CEO fraud has inflicted major losses on enterprises that are swindled. There is no reason to believe that CEO fraud will decline in the immediate future. The number of attacks, particularly those targeting bank customers, will probably increase in the years ahead.

A number of European countries have been subjected to cases of CEO fraud³², and these attacks appear to be on the increase. Fraud scenarios that arise in other parts of Europe often reach Norway after a while.

3.10.2 Ransomware

Ransomware is the term given to a type of malware that infects systems, and results in encrypted hard disks. Ransom money is then demanded to restore access. The point of entry is often false e-mails (phishing) with a link to the malware.

Norwegian banks, insurers and investment firms were all subjected to ransomware attacks in 2015, as were enterprises in other sectors. Finanstilsynet has observed that the attacks had the greatest consequences for small enterprises, while the defence mechanisms of major financial institutions were more effective in limiting damage.

CryptoLockers are an example of ransomware. Both the malware itself and the preceding phishing may be difficult to detect and reject with the aid of antivirus software and e-mail filters because sender, texts and links are constantly changed. The texts used in the e-mail to cause users to upload encryption macros have also become more credible, and therefore pass more easily through the defences the undertakings build up through procedures, training and awareness-building campaigns. The incidents show that no matter how much work is devoted to proactive measures to avoid CryptoLocker attacks, undertakings will still be dependent on the reactive security that is built up in the form of safety backup systems, functioning procedures and tested contingency preparedness.

³² <http://www.investopedia.com/terms/c/corporate-fraud.asp>

3.10.3 The Dyre Trojan

The Dyre virus (also called Dyre/Dyreza) is a banking Trojan designed to steal log-on information from its victims by forwarding all communications to and from the internet bank to the criminals' servers. This enables them to change what the user sees in the browser and at the same time to steal money from the bank account. The virus can also redirect users to dangerous and insecure websites where their computer becomes infected with other net threats that can be used for criminal acts.

This type of attack is called MITM (man-in-the-middle) and is where SSL protection of internet banking is circumvented. The Dyre Trojan is also capable of downloading and starting supplementary modules that give the criminal greater control of the infected PC. The Dyre virus is mainly spread by means of undesired e-mails (spam campaigns) and infects the PC by means of either attachments or links that the user is tricked into clicking on.

In 2015, Norwegian internet banking customers were subjected to Dyre attacks specially designed for a particular bank.

3.10.4 Targeted police actions successful

Dyre wrought havoc in many European countries in 2015. The persons behind the Trojan were arrested in a coordinated police action in Moscow in November ³³ 2015. Since then, no further Dyre attacks have been reported to date, in Norway or any other country. The same trend was seen in 2012, when the special cybercrime police unit in the UK struck at an organised ring who were responsible for an extensive botnet. The number of false websites that were identified as being a source of phishing was reduced to a tenth within a month³⁴.

3.11 Blockchain

A blockchain is a digital ledger of data transactions containing ownership rights or other types of agreement. With distributed blockchains, the ledger is directly managed and controlled by participants in the transaction or rights-holders, without the involvement of a central authority. There is great interest in employing blockchain technology in the financial sector.

This technology makes it possible to transfer ownership of assets in a matter of seconds, without a central counterparty and at minimal cost. The transactions are stored in a distributed ledger of blocks that contain all the transactions. The transactions are digitally signed, and network participants must approve them. There are also centralised blockchains, where a key player is responsible for approving transactions.

Today blockchains are mainly used in connection with cryptocurrencies. The advantage is low transaction costs and the possibility of realising immediate payments in a practical manner. The

³³ <http://www.reuters.com/article/us-cybercrime-russia-dyre-exclusive-idUSKCN0VE2QS>

³⁴ http://www.finanstilsynet.no/Global/Venstremeny/Rapport/2014/ROS-analyse_2013.pdf 7.5.2

objections are that the cryptocurrency is unregulated, which has led to wide and unpredictable exchange rate fluctuations. As a currency of this nature has no central control authority, it cannot be used as a monetary policy instrument.

Blockchains are designed to link owners to objects, for example properties. Blockchain transactions function in the same way as a digitally signed document. The owner of the private key owns the object described in the document. The documents are chained, and form a register of owners.

A number of initiatives have been launched to define platforms that can be used to establish systems for use in the financial industry. The platforms consist of rules, formats and protocols for entering into various binding agreements. The agreements are registered in a blockchain. Examples of initiatives: Ethereum (open), R3CEV ³⁵(several financial institutions involved)

The participants, for example the members of R3CEV, envisage digital transactions linked to physical assets. In this case, the document will differ from an ownership register by including a definition of the actual asset. This will require a trusted third party and a market-maker. It will also require fixed formats. The market for syndicated loans is a possible example. Today this is a global market with a volume of billions of dollars, in which transactions very largely take place by means of fax, e-mail and spreadsheet. These can be transferred to smart contracts in fixed formats in which the rules and conditions are programmed in, and which are then distributed among the participants in the syndicate by means of a distributed ledger. Similar solutions are conceivable in trade finance and the capital market. The present complicated processes will be greatly simplified, which may reduce the risk of error. Processes are faster, which means less operational and counterparty risk, and are consequently less costly (lower risk premium). The transaction ledger is distributed and less vulnerable to single point of failure as a result of attacks or operating error.

Common to all the aforementioned business areas is that parties to contracts currently use a great deal of resources on synchronising in the course of the transaction, instead of having one consistent picture at all times. At present they send information back and forth in efforts to harmonise, and costly post-processing is necessary to correct errors and differences. Distributed ledgers could remedy these problems.

Today international payments are a complex interaction between banks, central counterparties, liquidity banks and settlement systems on both payer and payee side. The participants believe these payments lend themselves to blockchain technology. Ripple, Stellar and Coinbase are examples of companies that are working on blockchain solutions in the area of payment services.

Finanstilsynet is of the view that the risk and security associated with blockchain have not been adequately clarified.

³⁵ <http://forklog.net/r3cev-tests-blockchain-for-banking-institutions/>

4 Operators' assessment of risk factors

This chapter considers the principal threats brought up the undertakings themselves in interviews and in their responses to Finanstilsynet's questionnaire. It also discusses major threats emerging from interviews with key security system operators and the most serious threats according to the assessments of some international security companies.

4.1 Interviews

In 2015, Finanstilsynet interviewed a variety of financial institutions in its study of ICT risk. Finanstilsynet also had discussions with other operators, including some central operators in the field of security and surveillance systems in Norway. The principal threat areas Finanstilsynet noted in these talks are discussed below. In some cases, control measures that were mentioned are described.

Certain threat types can cause severe adverse effects to an undertaking if they strike. Some threats can cause significant damage and inconvenience to consumers and thereby also negatively affect the reputation of the undertaking involved.

4.1.1 Societal changes affect security

The money-laundering rules require that banks and payment services have secure identification for their customers, and that transactions are monitored to ensure that they are not involved in financing terror, or are a direct part of such activities or money laundering. As a result of increasing demands for rapid mediation of payments, this monitoring is becoming part of the actual payment chain, and exerts great pressure on the participants to make changes.

The risk of terrorism and increased tension in conflict areas increase the risk of banks being used to finance terror actions. The undertakings maintain that the sharp increase in cross-border migration presents security challenges in connection with the establishment of new customers. Refugees without identification documents present particular challenges to the customer controls required by the money-laundering rules and regulations, and may increase the risk of attempts being made to transfer illegal assets through the payment systems.

4.1.2 Infrastructure disruptions

In 2015, banks noted increased instability in their infrastructure. This applies to services from both telecommunications and key suppliers. For the telephone operators, this applies in particular to mobile services and the SMS service which is used both for telephone banking and for some mobile telephony

applications offered by banks. Cases of failure of defences against cybercrime have been recorded by individual internet service providers (ISPs). However, the banks find that the DDoS security of the ISPs is sound.

Some banks express concern that the operating quality of BankID services is declining.

As dependence on electronic services increases, instability and disruptions result in poorer quality in the service offered to users, and confidence in services may be weakened.

4.1.3 Shortage of expertise

Several undertakings regard the mainframe expertise situation as challenging. A large proportion of employees with expertise in this area are approaching retirement, and there is an almost complete absence of mainframe training. The amount of outsourcing done by financial institutions is increasing, with the result that expertise in their own systems is being lost. Some undertakings compensate for this by increasing their use of consultants, but this, too, means that the expertise remains outside the undertakings. The result may be that undertakings end up with inadequate technical support for their purchasers, and in consequence deficiencies in their definition of technical delivery requirements. Some undertakings therefore express a need to upgrade the expertise of their purchasers in this area. The smallest operators are the biggest losers in this situation.

If offshoring becomes too extensive, this may threaten national expertise on the systems used in the financial sector with potential consequences for the ability to handle critical situations.

Most financial institutions have attempted to build up their expertise in the field of security. There is a shortage of training places, or applicants for these places, however. The candidates also need practical experience in the field before they can be regarded as qualified security experts. Several undertakings singled out the shortage of expertise in the area of security as a challenge.

The need for expertise on ICT security is also pointed out in several places in the Lysne Committee's report.³⁶

4.1.4 Risks associated with personnel

The threat associated with damage caused by an undertaking's own employees was mentioned in general terms by some undertakings. Outsourcing generally and offshoring in particular entail transfers, terminations and new personnel. Restructuring, cutbacks and disposals may result in a weakening of loyalty to the client.³⁷ Personnel replacements lead to "friction costs" in the form of training, relation-building and coordination/harmonisation. This may increase the probability of undesirable incidents.

³⁶ Committee on Digital Vulnerability in Society – [NOU 2015:13 Digital sårbarhet – sikkert samfunn \[Digital vulnerability – secure society\]](#)

³⁷ <http://e24.no/jobb/en-av-fire-norske-bedrifter-har-utro-ansatte/23592656>

4.1.5 Undertakings' supply chain complexity

New technological opportunities are constantly being offered by various suppliers. When some operators make use of these opportunities, it attracts attention in the market, and undertakings feel under pressure to quickly offer similar functionality. At the same time, new regulatory requirements are introduced, particularly through EU directives and regulations. The undertakings experience this as increasing demands for change. New functionality to counter this pressure tends to be met by a combination of outsourcing and use of consultants. The solutions lead to long value chains, particularly for internet and mobile banking. Both the fast rate of change and the ever more demanding follow-up present undertakings with challenges.

The changes also have consequences that extend beyond the software itself. Both infrastructure and internal business processes are affected by these changes, and providing sufficient capacity in the project area for ICT adaptations is also a challenge.

In the area of payments, undertakings mention the risk of a lower security level when more operators are authorised to provide payment services as a result of the new Directive on Payment Services (PSD2), and requirements regarding approval of more authentication mechanisms. The undertakings stress that the delivery pattern in this area may become complicated, despite the fact that the intention is to simplify matters for users.

Changes in production environments make it increasingly difficult to maintain good test environments. Undertakings express a need for better coordination of testing and production environments.

The steadily increasing complexity of transaction chains increases the risk of error, as does a large number of changes. This may result in a growing number of incidents.

4.1.6 The undertakings' views concerning cybercrime

Operators report that in a global perspective there is little malware activity in Norway (and the Nordic countries generally) compared with some other countries. Norway continues to be one of the least infected countries.

The Norwegian National Security Authority (NSM) monitors targeted attacks in Norway, and reports increasing threats. The fact that the impact of DDoS attacks has lessened is attributable to undertakings having sound protective mechanisms against such attacks.

Undertakings must be quick to upgrade and plug security holes. When criminals learn where the weaknesses are, it does not take long before a virus is developed to attack computers in which the weakness has not been repaired. Some undertakings have procedures for countering this.

Undertakings report that cyber attacks are becoming increasingly sophisticated and combine several of the traditional methods of attack. Circumvention of security, and the use of web addresses that are virtually the same as those of the undertakings, are methods that are employed. The attackers acquire

false certificates to enable them to use secure communication (https). An "industry" that issues criminal certificates is emerging in this area.

Some operators are interested in better interaction among the CERT operators and better cooperation between the different sectors in this area.

The cybercrime threat was high in 2015, and it is important that undertakings focus on stopping this threat. This requires increased surveillance of service deliveries, in addition to which clients must focus on security. The undertakings that have come furthest have defences at various levels: in relation to customers, channels and key applications. It is not a question of whether an undertaking will be attacked, but of being ready to resist when the attacks come. So far, the largest financial institutions have suffered the most attacks.

Current types of attack

- APT, for example CARBANAK, which steals data from Norwegian banks
- In the future, small and medium-sized enterprises (SMEs) are expected to be important targets for APT attacks, because they are assumed to have less comprehensive security measures. Small undertakings must also ensure that their local networks are well secured, even if the majority of their systems are outsourced to and secured by external service providers.
- Theft via mobile platforms. In 2016, more attacks are expected on mobile platforms, for example in the form of SMSs that dupes the user into downloading a false mobile banking app
- Distributed denial of service attacks (DDoS)
- Theft via electronic self-service channels
- Real-time phishing. Corporate clients are affected in more than 95 per cent of cases. One bank reports that attempts were made to swindle 188 customers, but the criminals only succeeded in gaining access to the customer's account in five cases
- The Dyre Trojan. Undertakings experienced attacks by the Dyre Trojan in 2015. The security community has been monitoring Dyre for a long time, and in mid-September there were indications of preparations to attack selected targets. Recovering data after these attacks entails a great deal of work. (See also 3.10.3)

The attacks listed below appear to be those that have hit Norwegian financial institutions most. (See explanation in the glossary in Chapter 8).

- Dyre
- ReTeFe (DNS changer)
- Tinbal
- Vawtrak
- Gozi-ISFB
- MITM/MITB (inject mode)
- Dridex + ammyy
- RAT-based "manual" fraud

Raising employee awareness

Many undertakings stress that they put a great deal of effort into building employee awareness, and providing training in what can happen if an e-mail recipient is careless and opens attachments or complies with requests or instructions from these e-mails. The undertakings point out that such awareness building and training play an increasingly important role in resisting digital attacks.

4.1.7 Breach of confidentiality

The undertakings consider that the threat of breach of confidentiality is on the rise. At the same time, customers increasingly have access to their own data. Availability through new channels adds to the threat picture. Attempted frauds are proliferating, and good protective systems must be established.

Many undertakings give priority to rapid product launch in the market, which may take place at the expense of security. Good launch procedures for new services, and good access control, are essential.

Data protection

Many undertakings are concerned with classifying and protecting data. Undertakings have seen a need to review 'unstructured data, i.e. data that are not stored in databases, and which can be less effectively protected against unauthorised access. These may be presentations, Microsoft Office documents, e-mail documents etc. Company-internal information may be concerned as well as information concerning other enterprises, such as customers, suppliers and business connections.

Issuing of BankID/security token

Some banks report that they have stopped delivering BankID security tokens through the post. The reason is that BankID is an identity instrument, which can be used for fraud if it goes astray.

4.1.8 Use of cloud and file-sharing services

Undertakings have shown an interest in using cloud services in some areas. Some are waiting for a clarification of the Safe Harbour question (see 5.1.4), but planning for the day when "suitable services" are gradually adapted and moved to cloud services. The undertakings want a clarification of the rules, so that equitable competitive terms are maintained.

As Finanstilsynet sees it, cloud services constitute outsourcing (see 3.8.2.), and must be in line with the undertaking's outsourcing strategy and with legislation and rules. Cloud services are marketed in many ways. Procurement expertise is necessary in order to know what one is purchasing, since most suppliers vary in the manner in which they formulate their offers of services. Undertakings must ensure that they are in control of the individual unit's use of cloud services, such that this use is consistent with the undertaking's outsourcing strategy.

Various types of file-sharing are also in use. Some undertakings are concerned about uncritical use of file-sharing services that are offered on the internet. File-sharing services are readily available, and meet the user's needs "then and there". Some of the services have had security weaknesses. Data on employees, the undertaking itself and business connections may go astray. Knowledge about

employees and undertakings may be misused by attackers for targeted attacks (spear phishing). There appears to be inadequate control of these services. It is said that:

- An undertaking's IT function is only aware of a small portion of the cloud services that are used
- there is a great deal of uploading to and use of cloud services with a high risk profile
- it is not unusual for an undertaking to use many different file-sharing services

4.1.9 Penetration testing

The threat of financial institutions' systems being hacked is increasing. Undertakings and their suppliers build up defences against penetration, but it is a complex area requiring a high level of expertise. Penetration defences must be tested to ensure that they function satisfactorily.

Some undertakings have performed penetration tests, often with the aid of external consultants. Others are planning to perform these tests in collaboration with other undertakings that have a similar infrastructure and use the same service supplier for their core systems.

4.1.10 Internet faults have a global impact

Undertakings report increased awareness of the fact that vulnerabilities far beyond Norway's borders may affect Norway. One example, mentioned in 3.9.1, is a weakness in Border Gateway Protocol³⁸ (BGP defines who owns IP addresses and is used by ISPs to route traffic).

4.1.11 Other risks pointed out by institutions

Spare parts

Some institutions found in 2015 that their suppliers did not have sufficient spare parts to meet their needs; see also 3.4.4. In one case, power outages and subsequent return of power inflicted damage on a number of network components. In this situation, it proved difficult to get sufficient replacement components delivered within a reasonable period of time. If several important undertakings within the same financial sector experience this problem simultaneously, it may have serious consequences for deliveries of financial services in Norway.

Physical access

A number of undertakings report that unauthorised parties have had physical access to technical infrastructure. This tends to be the case in buildings with several tenants. Not all tenants have the same access control requirements, and unauthorised persons may penetrate far into premises before there is a reaction.

Logical access controls

Failure of logical access controls is constantly perceived to be a risk. The operation and development of systems is a complex interaction between an undertaking's own employees and suppliers, both

³⁸ <http://www.washingtonpost.com/sf/business/2015/05/31/net-of-insecurity-part-2/>

domestic and offshore. Approving and following up persons, roles and accesses is demanding work. Some undertakings find that there is a need for improvements in this area.

4.2 Questionnaire

In December 2015, Finanstilsynet conducted a questionnaire survey of 22 undertakings. In the questionnaire, Finanstilsynet asked the undertakings to rate themselves with respect to their vulnerability to potential threats. The results are shown in tables 5–10 below. Green expresses low vulnerability for the undertaking, yellow medium vulnerability and red high vulnerability. No colour indicates that the undertaking did not reply.

The undertakings were also asked to rate their vulnerabilities going forward, i.e. as increasing, stable or decreasing. The trend that emerges in the column on the far right in the tables below is an expression of the average of the assessments given, where the interval -0.2 to +0.2 is indicated by a horizontal arrow and implies a stable trend. Arrows pointing up indicate that vulnerability is considered to be increasing (the interval +0.2 to +1), and arrows that point down indicate that vulnerability is regarded as decreasing (the interval -0.2 to -1).

4.2.1 Support for strategic decisions

Table 5: Support for strategic decisions

	Vulnerability	The undertakings' response	Trend 2014	Trend 2015
1	The ability of systems to retrieve and compile relevant information from internal and external sources for decision-making purposes		↘	→
2	Decision-support and reporting systems retrieve relevant information from our production systems and compile and synchronise the information into a picture of the undertaking's risk for the purpose of control and reporting to authorities		↘	→
3	The systems automatically provide an overall risk picture, so that if, for example, a cornerstone enterprise goes bankrupt, 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		↘	→
4	Our systems provide a good picture of customers' needs and ability to service debt		↘	→
5	The quality of data in our systems and registers		↘	↘
6	Integration and synchronisation of systems		↘	→
7	When new IT systems are to be developed, we take into account the needs and systems of all relevant departments. We do this to avoid the challenges associated with "silo solutions", such as extensive software maintenance, complicated operations and challenges associated with data synchronisation		↘	→
8	Complexity of IT systems		→	→
9	Extent of and faults and deficiencies in systems		→	→
Green: low vulnerability Yellow: medium vulnerability Red: high vulnerability				

Source: Finanstilsynet

The table shows the risk that ICT will not function satisfactorily as support for strategic decisions, customer services or case processing. One example is that ICT systems do not give sufficient warning of, for example, financial problems affecting a cornerstone enterprise or a whole industry. Undertakings therefore do not receive information from the ICT systems that enables them to take the necessary steps.

In this area, six of the threats have changed from declining in 2014 to stable in 2015.

4.2.2 Operational irregularities

Table 6: Operational irregularities

	Vulnerability	The undertakings' response	Trend 2014	Trend 2015
1	Organisation, procedures, job description, reporting and controls		↘	↘
2	Agreements with our suppliers give us the right to scrutinise all aspects of the delivery		→	→
3	The test systems are "production-like", i.e. test data, applications, software, control systems (SW) and hardware are the same for testing as for production		↘	→
4	We make changes in the infrastructure ("non-functional" changes) during periods with little traffic, and can quickly reverse the changes and roll back if necessary		→	→
5	Our ability to detect all weaknesses		↘	→
6	Checks to ensure that all hardware and software are included in IDS/IDP, firewalls and antivirus and other measures for ensuring stable operations		→	→
7	Logs and our ability to react to the contents of the logs		→	↘
8	"Ticking bombs", i.e. components that are gradually wearing out, or assets that gradually reach levels requiring intervention without our noticing it, such as memory leakage, worn out electronic components, an energy supply that is running down (batteries etc.)		↘	↘
9	Our ability to detect irregularities in data traffic (abnormal load, abnormal ports / protocols, irregular response times) in the operating pattern and take action before damage occurs		↘	→
10	Our protection against data attacks (advanced persistence threat, Trojans, ransomware, DDoS)		→	→
11	The quality of our business continuity and disaster recovery systems		↘	→
12	Procedures for cooperation with suppliers		→	→
13	The pressure to deliver we are exposed to in the market		→	↗
14	Access to expertise, including the expertise to stipulate requirements for suppliers and to monitor deliveries		↘	→
15	Amount of change (new supplier, new core systems)		→	→
16	New regulatory requirements that make it necessary to change our systems		→	↗
17	Our knowledge of where data transmission lines go and line redundancy		→	→
18	Control of access to systems, physical control of access to premises and segregation of duties		→	→

Green: low vulnerability Yellow: medium vulnerability Red: high vulnerability

Source: Finanstilsynet

Hacking is a persistent threat, as is the amount of changes in systems and suppliers. More undertakings than last year consider that testing systems could be better. This may be related to increased pressure to deliver (13), the scope of changes (15) and changes due to new regulatory requirements (16).

4.2.3 Data are not adequately protected

Table 7: Data are not adequately protected

	Vulnerability	The undertakings' response	Trend 2014	Trend 2015
1	Our guidelines for classification and protection of information		→	→
2	The quality of our access controls		→	→
3	Our logging systems and our ability to react to log contents		→	→
4	Possible penetration of our systems		→	→
5	Protection of data on portable equipment (remote deletion of mobile data etc.)		→	→
6	On termination of data storage agreements, the supplier must document that data have been completely deleted.		→	→
7	Unstructured data (i.e. data that users themselves evaluate the need to protect) such as e-mails, presentations, text documents, are reviewed regularly with a view to protection or alternatively deletion..		→	→

Green: low vulnerability Yellow: medium vulnerability Red: high vulnerability.

Source: Finanstilsynet

Access controls continue to represent a challenge. Outsourcing, offshoring and temporary, contracted expertise create challenges.

System penetration is regarded as a threat. There was an increase in ransomware in 2015; see 3.10.2.

4.2.4 ID theft

Table 8: ID theft

	Vulnerability	The undertakings' response	Trend 2014	Trend 2015
1	Our protection against malware that infects a user in the undertaking and misuses the rights of the infected user		→	→
2	Controls on the issue and use of log-on IDs and passwords to customers and employees (BankID, employee ID, system users, admin users)		→	→
3	Controls that prevent skimming and card-not-present fraud		→	↗

Green: low vulnerability Yellow: medium vulnerability Red: high vulnerability





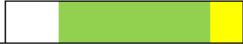
Source: Finanstilsynet

Malware and misuse of rights in connection with ID theft are still regarded as a considerable risk.

In 2015, the threat of CNP fraud was considered to be increasing.

4.2.5 Misuse of access to IT systems

Table 9: Misuse of access to IT systems




	Vulnerability	The undertakings' response	Trend 2014	Trend 2015
1	Access control		→	→
2	Our policy on segregation of duties		→	→
3	Logging		→	→
4	Analysis of suspicious transactions such as retroactive value dating, movements in internal accounts, transfers from customer to employee and back		→	→
5	Monitoring of employees' own-account trading		→	→
Green: low vulnerability Yellow: medium vulnerability Red: high vulnerability				

Source: Finanstilsynet

The threat picture is unchanged from previous years.

4.2.6 Money laundering

Table 10: Money laundering

	Vulnerability	The undertakings' response	Trend 2014	Trend 2015
1	Market surveillance		→	→
2	The ability of the IT systems to compile information about customers, customer relations and customer behaviour (KYC – Know Your Customer)		→	→
3	Electronic surveillance of transactions – precision in flagging suspicious transactions		→	→
Green: low vulnerability Yellow: medium vulnerability Red: high vulnerability				

Source: Finanstilsynet

Several undertakings consider it a challenge to develop systems that flag suspicious transactions with high precision. A substantial number report active work to improve compilation, flagging, analysis and reporting in this area.

Overall, tables 5-10 show that eleven vulnerabilities have changed from declining in 2014 to stable in 2015. This may indicate that threats have either levelled off or become more real or acute in 2015 than in 2014, or alternatively that the undertaking does not consider that it has adequate protection against the threats. It is also worth noting that three vulnerabilities have gone from being stable to regarded as increasing. All in all, undertakings consider that risk increased from 2014 to 2015.

4.3 The report from the EU security agency (ENISA)

The European Union Network and Information Security Agency (ENISA) is the EU countries' resource centre for network and ICT security. ENISA is used in connection with ICT security and is referred to by the EU financial supervisory bodies, EBA, ESMA and EIOPA. ENISA publishes an annual report³⁹ with a summary of the previous year's incidents and of changes in the ICT security threat landscape for the financial industry in Europe.

In its 2015 report, ENISA points out that the battle against digital vulnerability continues, and that public authorities and their suppliers have become more effective through:

- more coordinated/organised measures to halt cyber attacks
- greater expertise and knowledge of cybercrime, increased budgets and more cross-border cooperation
- exercises, more intelligence and sharing of information among nations
- increased focus on research and development to produce systems that provide protection against cybercrime

On the other hand, criminal forces are still demonstrating that they have abundant resources through:

- ever better applications for criminal acts, which are offered as services over the internet
- improved means of detecting and exploiting weaknesses in existing systems
- a high degree of success in developing various lucrative ransomware services
- expanding the range of crime to include all entities connected to the internet
- attacks that are not registered by the usual defence systems.

ENISA maintains that 2015 can be described as the "ransomware year", in view of the wide distribution ransomware has now achieved; see 3.10.2. Special attention is paid to a variant called the CTB locker (Curve-Tor-Bitcoin).

Part of ENISA's report shows developments in different ICT risk areas based on reports from various sources. In brief, the following risk areas have:

– increased in extent:

- Malware
- Cyber attacks
- Web application/injection attacks
- Denial of service (DDoS)
- Insider threats
- Information leakages
- Ransomware
- Cyber espionage

– decreased in extent:

- Spam
- Phishing
- Use of botnets

³⁹ The ENISA Threat Landscape 2015 Published on ENISA's website.

5 Regulatory changes

In 2015 there were once again a number of EU processes associated with proposals for new, or amendments to existing directives, regulations, technical standards and guidelines which will have a bearing on Norwegian conditions as and when they are incorporated into Norwegian legislation. There were also amendments to laws, regulations and guidelines at national level.

In some areas, the changes may entail a need for extensive changes in undertakings' system design. Changes in the system portfolio are generally a significant source of error.

5.1 Coordination within the EU and changes in EU rules and regulations

5.1.1 Payment services

Guidelines on the security of internet payments were adopted with effect from 1 August 2015. Finanstilsynet has endorsed the guidelines (see 5.2.3).

The work of revising the new Payment Systems Directive (PSD2)⁴⁰ was completed in 2015. The directive enters into force on 13 January 2018, and is intended to promote innovation by creating greater competition between existing and new operators. Its scope has been broadened to include all currencies and one-leg transactions within the EU. The directive authorises new operators to act as payment service providers and gives the right of access to payment accounts to both existing and new operators. Authorisation is required for payment initiation services (PIS) and account information suppliers (AIS) are required to register. The new payment service operators are required to have insurance. The directive stipulates high security requirements for all electronic payments and all payment service suppliers, including strong authentication and secure communication. Undertakings must meet requirements with regard to incident reporting, performance of risk analyses and control of risk in the payment service. The provisions of the directive are intended to strengthen cooperation on supervision of cross-border activities and result in improved consumer protection. The directive also regulates the right to charge user fees. The Ministry of Finance has announced that the Ministry of Justice and Finanstilsynet will be assigned to prepare proposals for incorporating PSD2 into Norwegian law⁴¹.

⁴⁰ http://ec.europa.eu/finance/payments/framework/index_en.htm

⁴¹ <https://www.regjeringen.no/contentassets/034971cd8bc54244b025fab9af15c45e/betalingstjenestedirektiv.pdf>

The EBA has been made responsible for drawing up proposals for more detailed guidelines covering several areas governed by PSD2. These were outlined in the 2014 Risk and Vulnerability analysis. The most demanding work is associated with preparing regulatory technical standards for strong authorisation, including exemption rules, and secure communication. The rules are designed to ensure safe and secure payment services, even when several participants are involved in the payment execution value chain.

In 2015, the EU drew up a Green Book on retail financial services⁴², with a view to achieving better products, more choice and greater opportunities for users and enterprises. The European Commission circulated the document for comment in December 2015.

The EU has initiated a process to revise the E-Money Directive. The first partial reports are expected to be available in the winter/spring of 2016. One of the purposes of the revision is to achieve consistency with the adopted PSD2.

5.1.2 The Protection of Personal Data "package"

The EU has adopted a new regulation⁴³ on the protection of personal data. It is expected to enter formally into force in the first quarter of 2018. The proposal strengthens the rights of the person the data concern through:

- requirements that the person in question must give clear consent to the processing of personal data
- readier access to checking one's own personal data
- the right to have information corrected, deleted, and "the right to be forgotten"
- the right to raise objections, including to having the information used for profiling
- The right to move one's own personal data from one provider of services to another.

The personal data protection regulation contains rules about inherent privacy (privacy by design, privacy by default), data protection officers and internal control.

5.1.3 Networks and information security

In the work on the proposed Network and Information Security Directive (NIS Directive), where there have been extensive and demanding discussions in the EU on several of the areas, political agreement on the draft directive was reached in December 2015⁴⁴. The financial sector is one of several that will be covered and affected, even though a number of the directive's provisions are incorporated in PSD2. This subject has previously been discussed in Finanstilsynet's RAV reports for 2013 and 2014.

⁴² http://ec.europa.eu/finance/consultations/2015/retail-financial-services/index_en.htm

⁴³ <http://data.consilium.europa.eu/doc/document/ST-5455-2016-INIT/en/pdf>

⁴⁴ [Draft directive](#)

5.1.4 Transmission of data between the EU/EEA and the USA – Privacy Shield

The European Court of Justice has previously ruled invalid an agreement on data transmission between the EU and the USA (the Safe Harbour agreement). A new agreement has since been negotiated. The agreement, which will be called Privacy Shield, will apply to all enterprises that provide services in the EU.

The main points of the new agreement are:

- New requirements regarding enterprises' handling of personal data
- rules for access by US authorities
- the Ombudsman arrangement
- a new appeal mechanism
- rules for ordinary appeal processing

All undertakings that wish to take part in the arrangement must show how they intend to observe the principles of the agreement. Annual inspections will be introduced of enterprises that take part in the Privacy Shield arrangement.

The new agreement contains rules for US authorities' possibility of access to the personal data of European citizens. The US Department of Trade is to deliver annual reports showing how the agreement is being complied with. An Ombudsman associated with the US Department of Foreign Affairs is to be created. The role of the Ombudsman will be to protect the rights of appellants.

An independent arbitration scheme will be established, with members from Europe and the USA. Undertakings that handle personal data on the basis of the new agreement will be obliged to process appeals within a given time limit, and follow-up of appeals is guaranteed by the US Trade Department. The appeal arrangement is to be evaluated annually.

Before a final decision is taken concerning content and implementation, a committee consisting of representatives of the member countries is to be consulted, and the Article 29 group (the EU working party on personal data protection) is to make a statement. The Article 29 Working Party aims to have a statement ready in the second quarter of 2016. At the same time, the US authorities are carrying out the necessary preparations for introducing the new regulatory framework, including the establishment of the new Ombudsman mechanism.

5.1.5 Insurance

The new European regulatory framework for financial stability in insurers, Solvency II⁴⁵, entered into force on 1 January 2016. Internal and external reporting requirements are more stringent, and rigorous requirements are set for data and data quality, which will mean substantial changes in ICT systems.

⁴⁵ http://www.finanstilsynet.no/no/Artikkelarkiv/Aktuelt/2014/4_kvartal/Finanstilsynets-forskriftsforslag-for-gjennomforing-av-Solvens-II/.

5.1.6 Anti-money laundering measures

In 2015, the EU adopted the fourth money-laundering directive on the basis of the 2012 recommendations of the Financial Action Task Force (FATF)⁴⁶. The new directive and the comments in FATF's 2014 evaluation report for Norway⁴⁷ form the basis for the work that has been initiated on new legislation regarding action against money laundering and terror financing in Norway. The Committee is to complete its report in 2016.

The Norwegian money-laundering regulations require banks to have systems for electronic monitoring of transactions and to ensure that specified types of suspicious transactions are not carried out prior to scrutiny. The complexity of the controls is increasing steadily, and the possibility that they may challenge operational stability cannot be excluded.

5.1.7 Taskforce on IT Risk Supervision

The EBA's Taskforce on IT Risk Supervision (TFIT)⁴⁸ was established in 2015. The TFIT's responsibilities and objectives are to provide advisory services and support to national supervisory authorities and EBA staff, to help ensure that the EBA's work programme relates to supervisory practices in ICT risk inspection, and to develop a unified and effective framework for assessing ICT risk. This is done through exchange of information on approaches to and practices in supervision, identification of relevant supervisory cooperation, and the drawing up of guidelines. The TFIT will also adopt a position on issues associated with the implementation of international standards, best practice and other recommendations.

5.2 Changes in the Norwegian regulatory framework

5.2.1 The new Financial Institutions Act

A new Act on Financial Institutions and Financial Groups (the Financial Institutions Act), entered into force on 1 January 2016. The new Financial Institutions Act replaces the Savings Banks Act, the Commercial Banks Act, the previous Financial Institutions Act and the Bank Guarantee Act and parts of the Act on Insurance Activity. The new Act contains rules relating to licensing, organisational rules, general business rules, rules concerning guarantee schemes and capital inadequacy and sanctions for banks, insurers and other financial institutions.

Financial institutions that were already operating when the new Act entered into force had had a time limit of one year to fulfil some of the requirements, while the remaining parts of the Act had to be complied with by 1 January 2016.

The Ministry of Finance circulated draft regulations to the new Financial Institutions Act for comment, with a deadline of 1 April 2016.

⁴⁶ http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf

⁴⁷ <http://www.fatf-gafi.org/countries/n-r/norway/documents/mer-norway-2014.html>

⁴⁸ [https://www.eba.europa.eu/documents/10180/758113/EBA+BS+2015+180rev1+\(Final+Minutes+BoS+28-29+April+2015\).pdf](https://www.eba.europa.eu/documents/10180/758113/EBA+BS+2015+180rev1+(Final+Minutes+BoS+28-29+April+2015).pdf)

5.2.2 Amendments to the ICT regulations

The ICT regulations⁴⁹ were amended on two essential points on 17 December 2015. Section 2, fourth subsection contains requirements to the effect that outsourcing agreements and amendments to such agreements must be dealt with by the Board of Directors of the undertaking. Section 10 Requirement of continuity plan has been repealed and the substantive contents incorporated in section 8 Operations, as continuity plans are becoming increasingly established as part of the undertakings' ordinary operating systems. Amendments have also been made to section 9, third subsection, to the effect that collection companies and pension funds are no longer exempt from the requirement to report incidents. Some minor additional adjustments have been made in the regulations.

5.2.3 New regulations and guidelines for payment services

The Regulations on payment service systems entered into force on 1 January 2016⁵⁰. The regulations stipulate a requirement that undertakings perform risk and vulnerability analyses as part of the basis for decision-making before a new payment service is launched and in the event of incidents or changes that have a bearing on the security level. The regulations also contain a number of security requirements.

The Guidelines on the security of internet payments⁵¹, prepared by the European Banking Authority (EBA)⁵² in collaboration with SecuRePay, took effect on 1 August 2015. Finanstilsynet will make these the basis for its inspections. The guidelines, which were drawn up on the basis of the existing Payment Services Directive (PSD1), are reflected in Norway in the Regulations on payment service systems.

The purpose of the guidelines is to define common minimum requirements for the security of the online payments listed below, irrespective of which technological solution is used for access to the service:

- execution of online card payments, including payments with virtual cards and registration of card payment data for use in ePurse solutions
- execution of online credit transfers
- registering and changing of electronic orders for direct debiting
- online transfer of electronic money between two e-money accounts

The guidelines define strong client authentication, and establish that strong client authentication is the general rule for online payments. The guidelines require end-to-end security.

⁴⁹ <https://lovdata.no/dokument/SF/forskrift/2003-05-21-630>

⁵⁰ <https://lovdata.no/dokument/SF/forskrift/17/12/2015-1731>

⁵¹ http://www.finanstilsynet.no/Global/Temasider/IT-tilsyn/Retningslinjer%20for%20sikkerhet%20i%20internettbetalinger_korr-AEJ-21-09.pdf

⁵² <https://www.eba.europa.eu/regulation-and-policy/consumer-protection-and-financial-innovation/guidelines-on-the-security-of-internet-payments>

In 2015, Finanstilsynet held information meetings for the financial industry to provide information about the contents of the guidelines.

A proposal to incorporate the EU Regulation on interbank fees⁵³ into Norwegian law was circulated for comment in December 2015. It includes requirements regarding the following: caps on interchange fees for consumer cards; separation of card schemes from the processing of card payments; co-branding of cards and consumer's right to determine choice of card brand. Control of the use of a co-branded card will be prohibited, thereby rendering illegal the current priority rule, where the BankAxept brand receives priority ahead of other combined cards. It is proposed that the Regulations relating to interchange fees in card schemes enter into force on 1 July 2016.

5.2.4 Amendments to the regulatory framework for insurance

Over a period of years, major changes have been made in the regulatory framework governing insurance, including the occupational pension scheme and the Solvency II regulations. Amendments are still being made to the regulatory framework for pension schemes, and substantial ICT work is required to adapt to them. The Solvency II regime applies to both life and non-life insurance. The regulatory requirements pertaining to model-based projections and more stringent reporting requirements entail extensive ICT work, and good data quality is a prerequisite. Solvency II reporting differs from the current financial accounting standards, IRFS, and poses a challenge for companies. Interfaces and harmonisation of the various systems are essential.

5.2.5 Electronic signature

Up until 1 March 2016, the Ministry of Trade and Fisheries circulated for comment a proposal⁵⁴ to implement Regulation (EU) No 910/214 of the European Parliament and of the Council on electronic identification and trust services for electronics transactions in the internal market and to repeal Directive 1999/93/EC. The consultation document proposes a new Act to implement the Regulation, and that Act no. 81 of 15 June 2001 relating to electronic signatures be repealed. The EU Regulation strengthens and extends the rules relating to electronic signature, regulates eID and also covers other types of electronic trust services. The Regulation consists of two parts, and contains rules that pave the way for:

- mutual acceptance of electronic identification systems (eID). This means that private persons and enterprises must be able to use their eID, issued either by the public sector or under the purview of a government authority, to gain access to electronic services from the public sector in other countries that offer logging on with eID.

⁵³

https://www.regjeringen.no/contentassets/fbc25cd42f8d44c781924e597fed3da0/horingsnotat_des2015.pdf

⁵⁴ <https://www.regjeringen.no/no/dokumenter/gjennomforing-av-eus-forordning-om-elektronisk-identifisering-eid-og-tillitstjenester-for-elektroniske-transaksjoner-i-det-indre-marked---horing/id2464892/>

- Mutual acceptance of electronic signature and other trust services – chapters III and IV. The Regulation strengthens the current rules on electronic signature and introduces rules for several types of electronic trust services, including electronic seals and time stamps, electronic registered delivery series and certificate services for website authentication.

6 Risk areas

Finanstilsynet's primary objective is to contribute to financial stability and smoothly functioning markets. Financial services cannot be delivered without well-functioning ICT systems. New digital solutions increase efficiency and lower costs. However, the trend also implies increased vulnerability.

If payments and some other financial services are unavailable, after a short period important societal functions will no longer function satisfactorily. After a longer period, important societal functions may come to a halt. Markets will no longer function as they should.

6.1 Financial infrastructure

The Norwegian financial system is coordinated, and shared systems and operations service providers are used extensively in the financial industry. The result is an efficient, smoothly functioning system. However, it means that both intentional incidents, such as ICT-targeted attacks, and unintentional incidents that affect coordinated systems or operations service providers used by many undertakings may have major consequences. Incidents that affect individual undertakings may also have undesirable collateral consequences for other financial system participants. In addition to causing systemic damage and economic problems, these incidents may have societal consequences and impact financial stability.

Several undertakings changed from a shared supplier to individual suppliers in 2015. This may reduce vulnerability, because it is less likely that several of the operations centres will be hit simultaneously.

Financial services are becoming available through an increasing number of service channels. If one channel is unavailable, customers can in some cases use another.

By means of supervisory activities and the work of the Contingency Committee for Financial Infrastructure, which includes reviewing incidents in financial institutions and financial market infrastructures (FMIs), Finanstilsynet obtains a good, broad picture of the state of the Norwegian financial infrastructure.

The financial infrastructure was more stable in 2015 than in 2014, and it was affected by fewer operational incidents. The regularity of clearing and settlement systems and communication with the Society for Worldwide Interbank Financial Telecommunication (SWIFT) and the international settlement system Continuous Linked Settlement (CLS) was also good. Consequently Finanstilsynet considers that the Norwegian financial infrastructure is sound and stable, but that there is room for improvement in some areas. This applies to both individual infrastructure undertakings in the financial

sector and to some other undertakings, in areas such as contingency planning, operational risk control and access control.

The IMF's assessment of financial stability in Norway

The International Monetary Fund (IMF) conducted a Financial Sector Assessment Program (FSAP) of Norway in 2014/2015. The purpose of the programme is to assess weaknesses and strengths in the financial systems of member countries of systemic importance, and to propose measures to promote stability and security. The financial infrastructure in Norway was discussed in the main report (Financial System Stability Assessment) and in a technical report (Technical note – Oversight and Supervision of Financial Market Infrastructure, and Selected Issues in the Payment Systems).

The main report describes Norway's financial market infrastructures (FMI) as modern and stable, and concludes that the supervisory and surveillance functions of the FMIs appear to be effective. However, the IMF also indicates that there is potential for strengthening cooperation at government level in order to address the risk some FMIs have with respect to dependence on critical suppliers. In the view of the IMF, one risk-reducing measure may be for Norges Bank to obtain assistance from Finanstilsynet's technical and operational experts to draw up requirements for suppliers of critical infrastructure.

Outsourcing of systemically critical payment systems has improved their efficiency, but also increased the potential risk. The IMF points out that improvements can be made by strengthening risk control and the administration of NICS. Another measure would be to improve the contingency preparedness plans of NBO and NICS. Figure 1 above provides an overview of the flow of transactions in the Norwegian payment system.

The IMF's "Technical Notes" point to more concrete measures for reducing operational risk for the FMI undertakings that form the core components of Norway's financial infrastructure. The following points summarise the IMF's recommendations for action in this area:

- Strengthen control and monitoring of Norges Bank's outsourcing of operations for NBO and NICS.
- Expand the present cooperative agreements between Norges Bank and Finanstilsynet to include crisis management of FMIs, and expand the role of the Contingency Committee for Financial Infrastructure (BFI) in financial infrastructure crises.
- Contribute to greater visibility by publishing the FMI undertakings' own evaluations of CPMI/IOSCO analyses.
- Establish clear objectives for the time required by FMIs to restore ICT service.
- Analyse the risk associated with FMIs' use of multiple operating sites.
- Analyse the possibilities of reducing FMIs' dependence on critical service providers (CSPs)
- Develop cooperation with regulatory authorities in the home countries of central counterparty clearing houses (CCPs) that operate in Norway.
- Increase transparency surrounding Finanstilsynet's supervisory practice, for example in the RAV analysis and on Finanstilsynet's website.

Cooperation on supervision and surveillance of financial infrastructure in Norway.

A robust financial infrastructure is crucial to financial stability. In its work of supervising ICT, Finanstilsynet will focus particular attention on areas of vulnerability that may result in serious failure or major disruptions in the financial infrastructure and constitute a threat to financial stability.

Areas to which weight is attached in inspections are the undertaking's ICT governance and security work, including undertakings' measures to counteract cybercrime, the robustness of their operations and emergency planning systems and their management of change and control of access rights.

Finanstilsynet and Norges Bank developed their cooperation on supervision and surveillance of Norway's financial infrastructure over a period of years. It includes regular meetings and cooperation on risk assessment and joint inspections.

Finanstilsynet's and Norges Bank's responsibilities for supervision and monitoring of Norway's financial infrastructure overlap. Finanstilsynet is responsible for supervising the VPS register function and securities settlement, while Norges Bank is responsible for monitoring the same functions. Finanstilsynet is responsible for supervising Norwegian banks and their payment systems. Norges Bank is responsible for supervising interbank systems in Norway. Interbank/settlement systems that are offered by banks are generally part of the banks' ordinary systems as far as operations are concerned. Observations and feedback from Finanstilsynet's ICT supervision of these banks will thus provide important information of benefit to Norges Bank in its oversight of the interbank systems.

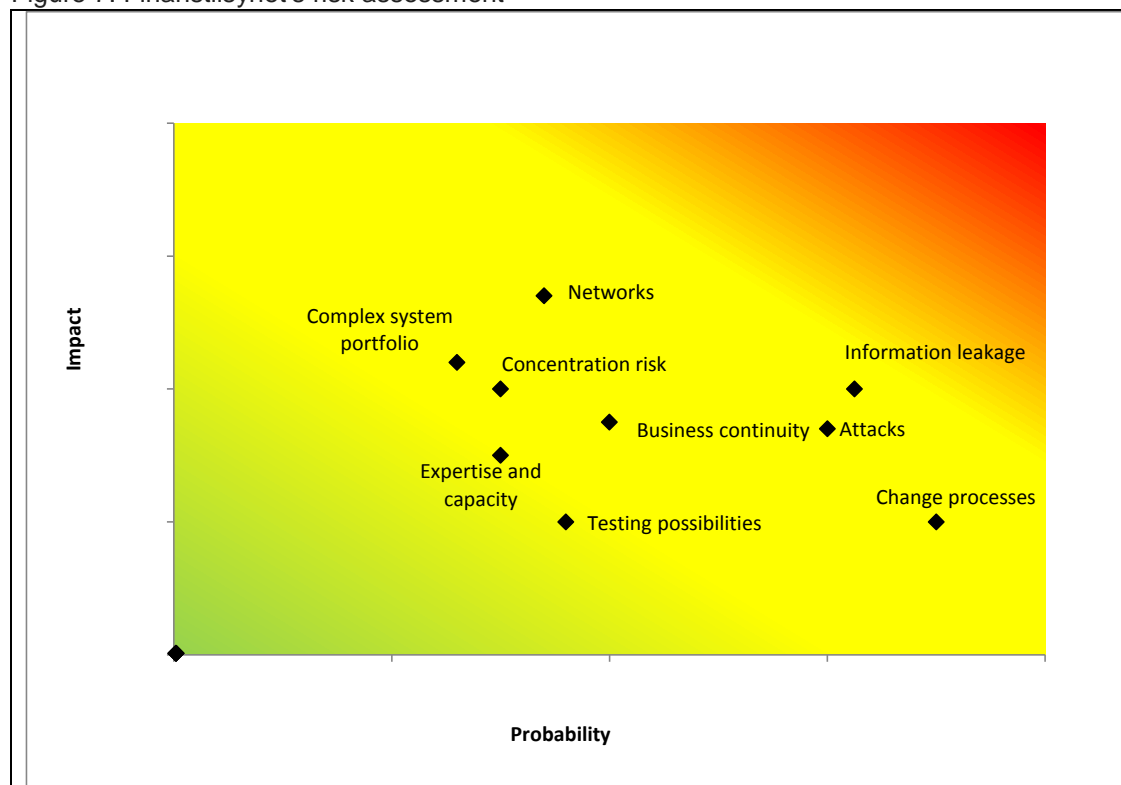
Finanstilsynet can attend the supervisory and surveillance meetings that Norges Bank has with FMIs in the capacity of observer, and Norges Bank can take part as observer at Finanstilsynet's inspections of banks and data centres of importance to financial infrastructure.

6.2 The undertakings

The figure below shows Finanstilsynet's assessment of the most central threats to and vulnerabilities of the undertakings' systems. In the figure, the various risk areas are classified according to the probability of a negative incident occurring (low, medium, high) and the consequences if the incident occurs (low, medium, high).

Finanstilsynet considers network faults, information leakages, cybercrime, complex system portfolios and faults associated with changes to be the most critical threats to and vulnerabilities of the undertakings' systems. Other threats to and vulnerabilities of the undertakings' systems are inadequate business continuity solutions, concentration risk, inadequate testing possibilities and inadequate expertise and capacity.

Figure 7: Finanstilsynet's risk assessment



Source: Finanstilsynet

Networks

Networks include local networks in the undertakings, networks between the undertakings' offices and subsidiaries, and connections to the internet (via ISPs). They also include the networks among the various collaborating parties in the industry. The networks are complex and require specialised expertise, not least on firewalls and defences against the internet. In many cases, faults are due to physical incidents such as ruptured cables, power outages, construction work or natural events.

Network faults may be difficult to locate if technical components or software fail, and repairs may also take a long time in the case of physical incidents. Some networks are crucial to the infrastructure.

Information leakages

Each year Finanstilsynet receives reports on undesirable exposure of information. Finanstilsynet's inspections have revealed inadequate access control. System classification has been found to be inadequate, with the result that information is not adequately protected. Undertakings also have incomplete logs of parties who have had access, with the result that the extent of leakages is difficult to determine. New participants, who are expected to represent a more deregulated market, may also want to use information that becomes available to them in a different way from in the past.

The consequences of leakages of personal data may be high for those concerned. For undertakings, such leakages imply risk to their reputations and the financial consequences, particularly in cases of leakage of sensitive information, may be considerable.

Attacks

The frequency and diversity of network attacks is on the increase. However, undertakings have built up solid defences, which reduce the probability of the attacks causing major damage.

In 2015 there were several cases where hackers made data inaccessible to the undertakings, and demanded a ransom. Finanstilsynet does not know of cases where ransom money was paid. Finanstilsynet is aware that the situation has caused quite substantial costs for restoring data from backups and lost time due to lack of access to systems and data.

Complex system portfolios

Operation of multi-layer architecture with systems and applications on different technical platforms that have to interact is challenging. The different layers of the architecture often have different operators. The daily running cycle of major financial institutions consists of a large number of individual tasks which are interdependent and have to be synchronised with external deliveries from other undertakings and partners. When changes are made, including purely technical changes, some dependencies may not be taken into account. Dependencies between systems are not always adequately documented. Agreements and procedures on cooperation among the various operators in the event of faults are not always good enough.

Operating error of this type may be difficult to locate. There may be a need for re-runs and corrections, and it may mean unavailability of services that may have consequences for both undertaking and customers.

Change processes

Change is one of the most frequent causes of system faults, and the pace of change is high.

Most faults following changes are rapidly revealed, and undertakings are able to reverse them before they have serious consequences. However, over the years Finanstilsynet has seen examples of changes in networks and data storage that have caused lengthy downtime for services.

More details about change processes

A number of major financial enterprises changed their ICT suppliers in 2015. There were some undesirable incidents in connection with the transitions, but thanks to good planning and testing by undertakings, the transitions to new suppliers were successful on the whole.

New methods of executing financial services were introduced in 2015. Finger prints and QR codes are being used by some to authenticate customers, and apps are being used for payment. Undertakings report strong competition in the market for new payment methods.

New methods of executing financial services may be the start of large-scale restructuring of this market. Banks and suppliers of payment services may have to change substantially as a result of further automation in credit and payment systems. The new Payment Systems Directive (PSD2) lays down premises for the entry of new types of operators into the market for payment services and account information.

Concentration risk

The banks' use multiple operating sites for their core systems. Nordea and DNB operate their own systems, the systems of the Eika banks and some small banks are operated by SDC, and those of the other savings banks are operated by Evry. Branches of foreign banks in Norway also have different systems, mostly operated by their parent bank. Payment system infrastructure is largely concentrated in Nets, but international cards and some other systems are also handled by Evry.

The insurance sector and the securities industry also tend to have operations located in different places.

Business continuity

Financial institutions have business continuity solutions that are based substantially on earlier disaster recovery systems. In many undertakings, the transition to business continuity systems is not automatic. Manual intervention is required, and in some cases coordination involving several operators before business continuity systems can be implemented. Finanstilsynet's inspections have revealed inadequate requirements regarding the critical availability of systems.

Smoothly functioning business-continuity solutions have been established for payment card infrastructure.

Expertise and capacity

The number of employees who have insight into the systems is small, partly as a result of outsourcing. Expertise on an ageing system portfolio may also be difficult to maintain because employees with this expertise are approaching retirement age, and there is little new recruitment to traditional mainframe technology.

There is a shortage of expertise in network technology and defence against cybercrime.

Testing possibilities

It is difficult to set up test environments that simulate production, and to achieve full end-to-end testing in a complex infrastructure. Finanstilsynet's inspections have also revealed that testing plans and procedures may be inadequate.

Experience shows that faults due to inadequate testing are relatively simple to detect, and can be rapidly corrected or reversed without serious consequences.

6.3 Users

BankID is the primary solution used by the public to access important services in and outside the financial sector. BankID is operated at a common operating site for all service providers that use BankID. There were several disruption situations in 2015. The impact on the financial sector was dampened thanks to new, alternative solutions for access to services. Consideration should be given to establishing more alternative solutions and operating sites.

From 1 August 2015, the EBA Guidelines on the security of internet payments apply. The guidelines stipulate that strong authentication is the rule. There are more stringent requirements regarding alerts and communication with customers. Customers must be able to set restrictions on the use of cards, for example so that a card cannot be used for internet trading.

ID theft remains a challenge. There are a large number of passports astray at any given time. Passports may be the port of entry for stealing an identity and escalating privileges. National, signed blacklists could remedy this.

More and more purchase agreements are entered into online. Very frequently, the customer is presented with a comprehensive agreement text at the moment of paying. In such a situation the agreement text may be difficult to absorb. There is reason to believe that in many cases, conditions etc. are not sufficiently well understood by customers before a purchase takes place.

The information left by the customer directly (personal data) and indirectly (purchases, and searches carried out on the internet) is sold and re-used in targeted advertising. Customers must be able to control the use of their personal data. Awareness on this point appears to be low, among both collectors and providers of data.

Customers' access to accounts and transactions is becoming steadily simpler. Customers can monitor accounts and movements and react in case of suspicion, thereby reducing risk.

Undertakings alert customers by SMS of transactions, blocked accounts, suspected misuse etc. to a greater extent than previously. Customers can also place restrictions on the area of use of cards, which gives customers greater control and a greater possibility of controlling risk.

The manner in which financial services are carried out is changing very rapidly. There is a risk of older customers not being able to "keep up", and having to pay high charges for financial services.

The Consumer Ombudsman is regularly contacted by parents who have received bills for large amounts after their children have used the phone for games. The games may be free, but the user is often required to pay in order to obtain advantages. In both App Store and Google Play, users risk spending many thousands of kroner with just a few keystrokes.

Some payment systems are designed such that when you get to the electronic cashier you are offered the opportunity to "pay instalments at your own pace". In recent years there has been an increase in the number of offers for payment by instalment when customers shop online.

Instalment agreements may be costly for the individual user, and it is important that the rules be followed, so that customers receive the information they need to enable them to evaluate the offer. Agreements that are presented on a small surface (mobile phone) and in a "pressurised" purchasing situation, are not appropriate in this connection. Credit agreements must be signed, either by means of an approved electronic signature such as Bank ID, or by means of pen and paper. There are examples of financial institutions entering into agreements with users without the user having signed in a valid manner.

False PC helpers were active in 2015. These false helpers ring and claim to be Microsoft employees who want to help the user with a problem. They often maintain that there is a virus or fault on the computer, and that the solution is to install software that the fraudsters recommend. The consumer has to pay for this by supplying a credit card number and code. If users supply payment information to fraudsters, they may at worst end up having to cover a loss of up to NOK 12 000 from their own pocket, following a decision by the Norwegian Financial Services Complaints Board, as the Board was of the view that the user in question had been grossly negligent.

Other callers ask the user to give them remote access to the PC. The fraudster is given full access to the computer, without the user realising it. Cases are known where consumers who have given fraudsters remote access have had both their credit cards and their banks accounts emptied.

7 Monitoring by Finanstilsynet

7.1 Monitoring of ITC risk and other contact with undertakings

Monitoring of undertakings' ITC risk primarily takes the form of on-site inspections. In 2016, as in 2015, Finanstilsynet will be focusing on those supervisory units and their suppliers that have the greatest influence on financial stability and smoothly functioning markets.

Special attention will be paid to outsourcing of key ICT systems that are critical for emergency planning. In particular, Finanstilsynet will monitor financial institutions that make major ICT changes, including outsourcing, and which thereby increase operational risk in the transition periods.

Finanstilsynet will continue to monitor the undertakings' contingency preparedness and crisis management systems. Inspections will also be used to monitor operating stability and structural changes in the suppliers to the entities subject to supervision. Compliance with rules and regulations, including reporting of new or changed outsourcing of ICT, and compliance with the provisions of the ICT Regulations on outsourcing will be closely monitored. Access controls, telephone logging and money laundering are other areas to which attention will be paid.

Risk assessments will be scrutinised, particularly when new technology is introduced that creates the possibility of new security risks.

7.2 Work with payment systems

Verification of compliance with the legislation is an important responsibility, and development of legislation is essential in such a dynamic area.

Major changes in payment systems, either through the development of new systems or in the form of outsourcing, will be monitored by Finanstilsynet if they may imply greater operational risk.

Compliance by the financial services industry with guidelines for secure internet payments will be monitored through self-evaluation, spot testing and penetration testing of internet-based solutions.

Collaboration with Norges Bank will continue.

7.3 Follow-up of incidents

The volume of serious incidents showed a positive trend in 2015. In 2016, Finanstilsynet will continue to closely monitor developments in serious incidents, and place emphasis on finding the cause(s) and taking steps to prevent recurrence.

7.4 Contingency preparedness

The work of the Contingency Committee for Financial Infrastructure (BFI) will continue, with monitoring of the stability of the payment infrastructure, incident scenarios and assessment of whether responsibilities in crisis situations are sufficiently clear. Two exercises are being planned for 2016.

Finanstilsynet will also participate in relevant contingency preparedness work initiated by other sectors concerning the payments infrastructure and payment services and undertakings' use of ICT.

7.4 Contingency preparedness

The work of the Contingency Committee for Financial Infrastructure (BFI) will continue, with monitoring of the stability of the payment infrastructure, incident scenarios and assessment of whether responsibilities in crisis situations are sufficiently clear. Two exercises are being planned for 2016.

Finanstilsynet will also participate in relevant contingency preparedness work initiated by other sectors concerning the payments infrastructure and payment services and undertakings' use of ICT.

7.5 Further development of supervisory tools

International best practice such as COBIT, ITIL and ISO forms the basis for the self-evaluation methods used by Finanstilsynet in its oversight of ICT and payment systems. It is essential that supervisory tools are best practice and the supervisory modules will be gradually updated in accordance with COBIT 5.

In the work of developing supervisory tools and methods, Finanstilsynet cooperates closely with the supervisory bodies of other countries and with the EU, including the EBA's Taskforce on IT Risk Supervision (TFIT).

7.6 Monitoring of the threat picture associated with cybercrime

Finanstilsynet will continue its close monitoring of developments in cybercrime and focus particular attention on undertakings' contingency measures against the growing threat scenario and their incident management. The increased threat level calls for more effort and increased cooperation among operators, and Finanstilsynet will seek to contribute.

7.7 Consumer protection

Finanstilsynet will place emphasis on undertakings taking customer security seriously and protecting customer data against sharing without consent or falling illegally into the possession of third parties. Stable payment services and access to their own money are also important to customers. The undertakings must also have services for users who are challenged by the use of new technology.

The security associated with new payment services will be monitored so as to minimise the risk of customer relationships or services being established in the names of others or by means of stolen identities. Undertakings' routines for managing and helping to rectify such situations, should they arise, will also be monitored.

8 Glossary

<u>Term/abbreviation</u>	<u>Meaning</u>
3-D Secure	3-D Secure is an XML-based protocol used in internet payments. It provides an extra layer of security to card transactions by authenticating the user in relation to the card issuer, irrespective of the payee. In connection with use of Visa, which developed the protocol, it is called Verified by Visa
AIS <i>Advanced Persistent Threat (APT)</i>	Account Information Supplier Persistent attacks on systems aimed at acquiring confidential information. Normally consists of an exploratory phase in which many methods are used, an implementation phase which proceeds as covertly as possible, often with low intensity, and frequently a final phase to cover tracks
App	Application, for tablet or mobile phone
AML	Anti-Money Laundering
Baltus	Banks' On-line Transaction Exchange System, which is the network used by banks to check the balance of accounts in each other's account systems
BASH	Standard command processor on many GNU/Linux systems (freeware)
BFI	Contingency Committee for Financial Infrastructure Committee to coordinate action in the event of financial sector crises. Chaired by Finanstilsynet
Botnet	A term compiled from the words 'robot' and 'network'. A network of programmes on various servers linked together via the internet. The programmes work together on a given task
CARBANK	An APT virus that steals information from Norwegian banks
CTB-locker	Curve-Tor-Bitcoin. A ransomware that demands payment of a ransom in Bitcoin
CEO fraud	A fraudster purports to be the chief executive officer of a company. Also called "Fake President Fraud" or "Business Email Compromise"
CEO attack	Online attack using CEO fraud
CERT	Computer Emergency Response Team. Team of experts who deal with cyber security breaches
Cloud computing	Remote network-based services. Distributed computing over a network. Possibility of running software on a large number of networked servers. Cloud computing may be both private and public sector, or a combination of the two. The term is used differently by different service providers; the services are often delivered via the internet

CNP	Card Not Present. Fraud with the aid of stolen card data, mainly in connection with online transactions
CPMI/IOSCO	Committee on Payments and Market Infrastructures/International Organisation of Securities Commissions
CVC code	Card verification code. The last three digits on the reverse of most credit cards
DNS	Domain Name System
DDoS attack,	Distributed Denial of Service attack. An internet attack that overloads a server by directing a huge amount of traffic at the server, usually by means of a botnet. The purpose is to prevent normal access by ordinary users
Dyre	Malware; see http://www.symantec.com/connect/blogs/dyre-emerges-main-financial-trojan-threat
Dridex + ammyy	Malware in the form of macros in Microsoft Office programs. Looks “innocent”, but is dangerous. http://blog.trendmicro.com/trendlabs-security-intelligence/banking-trojan-dridex-uses-macros-for-infection/
EBA	European Banking Authority
ECB	European Central Bank
EIOPA	European Insurance and Occupational Pensions Authority
ENISA	European Union Agency for Network and Information Security
ESMA	European Securities and Markets Authority
FATCA	Foreign Account Tax Compliance Act
FATF	Financial Action Task Force
FinansCERT	Norwegian financial sector cybercrime unit
FMI	Financial Market Infrastructure – consists of key market operators
FS-ISAC	Financial Services – Information Sharing and Analysis Centre. A European initiative consisting primarily of participants from CERTs, banking organisations and police authorities. In Norway, a collaboration between NSM, BSK and Finanstilsynet. At present an informal collaboration between individual countries and defined authorities, supported by ENISA. The USA has established an authority covering the same area. Exchanges of information, some of it confidential, on vulnerabilities, attacks and measures associated with the use of the electronic payment systems.
Gozi ISFB	Malware; see https://storify.com/bbddst/instructions-to-completely-remove-gozi-trojan-hors
GRFS standard	Standard for good accounting practices
ISACA	Information Systems Audit and Control Association, an independent, non-profit organisation. Works on developing and promoting the use of globally accepted, industry-leading knowledge and practice for information systems. ISACA has now changed its profile to an IT governance organisation
ISO 20022	ISO 20022 is the ISO financial services messaging standard. It contains descriptions of the messages and business processes and their maintenance.
IRFS	International Financial Reporting Standards (Currently applicable financial accounting standards)

ISP	Internet Service Provider – providing services such as internet access and domain names
Malware	Common term for software with “hostile intentions”, such as viruses, Trojans, ransomware, etc.
Man-in-the-middle attack	An attack where the attacker secretly relays communication between two parties who believe they are communicating directly with each other
MIF Regulation	Regulation on multilaterally-fixed interchange fees for card-based payment transactions
MITM/MITB (inject mode)	Malware; see https://en.wikipedia.org/wiki/Man-in-the-middle_attack
NBO	Norges Bank’s Settlement System
NICS	Norwegian Interbank Clearing System
NIS Directive	EU directive designed to secure a high common level of network and information security in the EU
NFC	Near Field Communication. Used in some payment cards and mobile telephones (the card or mobile phone is held near the payment terminal)
NTP	Network Time Protocol. Used to synchronise the clocks in networked computers.
Offshoring	Procuring services from outside the country. Sometimes used to refer to procurement outside the Nordic/Baltic regions
One-leg transaction	Transaction where one payment service provider is headquartered in a EU/EEA country, while the other payment service provider is headquartered outside the EU/EEA
Outsourcing	Procuring services from outside one’s own institution
Passporting guidelines	A payment service provider or e-money provider in an EEA country can freely establish itself in another EEA country provided that neither the home country’s nor the host country’s authorities have material objections. The process when such an institution, with a licence in one EEA country, wishes to establish itself in another EEA country, is called passporting. Briefly, passporting means communicating from the home country to the host country that an institution wishes to operate in the host country in the form of a branch or agent. Passporting guidelines are instructions for how to do this
PIS	Payment Initiation Supplier
Phishing	Impersonating another, and in this guise seeking information from a person. This is an attempt to exploit the person’s trust in the original sender
PKI	Public-key infrastructure. Consists of hardware, software, procedures, guidelines and personnel necessary to create, manage, distribute, use, store and revoke digital certificates
Privacy Shield	Agreement between the EU and USA on the secure transmission of personal data between the parties. Not yet in force
PSD2	New payment services directive from the EU (so far at draft stage).
Public cloud	Cloud service offered to “all” users

QR code	Quick Response code is a mosaic code for commercial and personal use. It can store a vast number of alphanumeric characters, enabling it to be read extremely quickly. It is therefore highly suitable for optical reading of data such as an address
Ransomware	A type of malware that restricts access to infected ICT systems and demands a ransom
RAT-based manual fraud	http://www.trusteer.com/glossary/remote-access-trojan-rat
Recovery points	Previous versions of data files that can be accessed and restored in the event of data loss or corruption
ReTeFe	Malware (DNS changer). See https://www.symantec.com/security_response/writeup.jsp?docid=2014-072516-1220-99
SMTP servers	Simple Mail Transfer Protocol servers. Used for sending and receiving external emails
SSM	Single Supervision Mechanism. The ECB's oversight of systemically important banks
SSL	Secure Sockets Layer. An old encryption method, now replaced by TLS
SecuRe Pay	European Forum on the Security of Retail Payments, an ECB forum
Strong authentication	Authentication employing several methods, e.g. pin code + password
TFIT	Taskforce on IT Risk Supervision, an EBA working group
TFPS	Taskforce on Payment Services, an EBA working group
TLS	Transport Layer Security. A protocol used between e-mail servers to encrypt messages and deliver them safely and prevent eavesdropping and "counterfeiting"
TPP / Third Party Providers	Term from the PSD2 Directive. These are service providers that provide payment services and that do not normally hold the payer's or the payee's accounts
Trojans	Viruses that pretend to be ordinary programs, but that contain malware
Vawtrak	Malware, see: http://now.avg.com/wp-content/uploads/2015/03/avg_technologies_vawtrak_banking_trojan_report.pdf

FINANSTILSYNET

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

Tel. +47 22 93 98 00
Fax +47 22 63 02 26
post@finanstilsynet.no
finanstilsynet.no