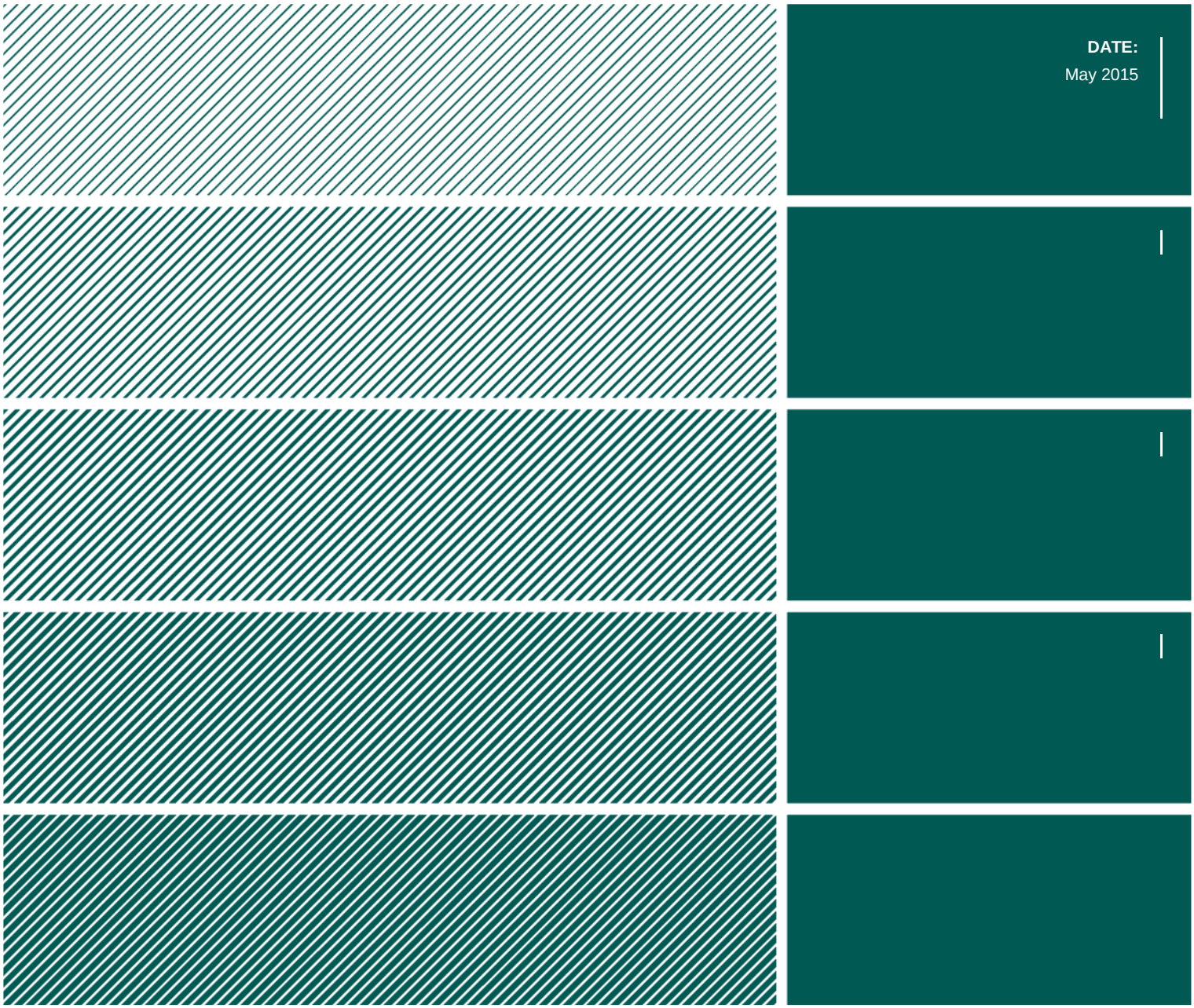
FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Report

Risk and Vulnerability Analysis 2014

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



DATE:
May 2015

Contents

1 Introduction 6

2 Summary 6

2.1 Finanstilsynet's findings 6
2.2 Observations from interviews and surveys 8
2.3 General trends 8
2.4 Current areas of risk identified in the 2014 analyses 9
2.5 Further follow-up by Finanstilsynet 9

3 Finanstilsynet's findings 10

3.1 Incidents reported in 2014 10
3.1.1 Operational incidents that affected many banks 11
3.1.2 Operational incidents that affected individual banks 11
3.1.3 Incidents involving a breach of confidentiality 12
3.1.4 Few malicious attacks 12
3.1.5 Little reporting from financial institutions other than banks 12
3.1.6 Analysis of incidents as a measure of availability 13
3.2 Payment systems and developments 14
3.2.1 General comments regarding payment systems 14
3.2.2 Management of and risk and vulnerability in payment systems 15
3.2.3 Findings and observations 16
3.2.4 Notification of payment service systems 16
3.2.5 Mobile payment systems 17
3.2.6 Attacks on payment systems 18
3.2.7 Overview of annual losses related to payment services 19
3.3 Securities 23
3.3.1 Securities firms' use of cloud-based services 24
3.3.2 Administration of users with access to sensitive corporate information in IT systems 25
3.3.3 Concentration risk in network infrastructure 25
3.3.4 Risk in connection with changes in key infrastructure components for securities trading 25
3.4 Banks 25
3.4.1 Changes related to operational service providers 25
3.4.2 Disaster recovery preparedness 26
3.4.3 Outsourcing agreements 26
3.4.4 Regulations on computer system requirements and reporting to the Norwegian Banks' Guarantee Fund 27
3.4.5 Access control 27
3.4.6 Classification of information 27
3.5 Insurance 28
3.5.1 General comments 28
3.5.2 Complex insurance systems 28
3.5.3 Control of changes 28
3.5.4 Outsourced ICT activities 29
3.5.5 Risk management 29
3.5.6 Testing of contingency preparedness systems 30

3.5.7 External data attacks 30
3.6 Findings in other institutions 30
3.7 Prioritisation of electricity and telecommunications for critical financial infrastructure 30
3.8 Consumers 31
3.8.1 Inadequate ID check on delivery of BankID 31
3.8.2 Online transaction fraud 31
3.8.3 Online stores and information security 31
3.8.4 Cards and PIN codes 32
4 Other observations 33
4.1 Financial institutions' risk assessment 33
4.1.1 Interviews 33
4.1.2 Questionnaire 36
4.2 Risk areas identified by security companies and internet service providers (ISP) 38
4.2.1 Interviews 38
4.2.2 Reports from security organisations 41
5 General trends 43
5.1 Cybercrime (digital crime) 43
5.2 Changes in the service provider market, organisation and ownership and outsourcing situation 44
5.3 Developments in payment services 45
5.4 Changes in the Norwegian regulatory framework 47
5.4.1 Regulation of outsourcing 47
5.4.2 Amendments to and new regulations 47
5.4.3 Amendments to the regulatory framework for insurance 47
5.4.4 Changes in rules for securities 48
5.5 Coordination and changes in EU rules and regulations 48
5.5.1 Networks and information security 48
5.5.2 Payment services 48
5.5.3 Regulation on electronic identification and trust services 49
5.5.4 Banks 50
5.5.5 Securities 50
5.5.6 Insurance 51
5.5.7 Anti-money laundering measures 51
5.6 Joint efforts by the financial industry 51
5.7 Virtual currencies 52
5.8 Cash and electronic systems 53
6 Risk areas 55
6.1 Overview 55
6.2 National financial stability 57
6.3 Financial institutions 57
6.4 Consumers 57
7 Monitoring by Finanstilsynet 59
7.1 IT-inspections risk and other contact with institutions 59
7.2 Work with payment systems 59
7.3 Follow-up of incidents 59

7.4 Contingency preparedness 60
7.5 Further development of supervisory tools 60
7.6 Follow-up of the threat picture associated with digital crime 60

8 Glossary 61

1 Introduction

The Financial Supervisory Authority of Norway (Finanstilsynet) performs an annual risk and vulnerability analysis (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 report describes risks and vulnerability relating both to financial stability and individual institutions and to individual consumers.

The core of this year's report lies in chapters 3, 4 and 5. Chapter 3 provides an overview of findings and observations made through Finanstilsynet's activities in 2014. Chapter 4 reports on the financial institutions' own assessments based on a questionnaire and interviews. In addition, some key security systems providers have been interviewed and the annual reports of global security companies have been reviewed. Chapter 5 describes developments and trends in or of relevance to the financial sector and its use of ICT.

The purpose of the annual RAV report is to provide an updated picture of the risks related to the financial sector's use of ICT and payment services. Some risks and vulnerabilities are the focus of attention year after year. However, the discussion of risks and vulnerabilities in the report is not exhaustive, and must not be interpreted as an indication that risks not mentioned are not considered by Finanstilsynet to be of importance to financial institutions. Chapter 6 contains a summary of Finanstilsynet's assessment of the risk picture in 2014. The approach adopted in this year's report is to provide a factual assessment of risks combined with an assessment of development trends related to the threats, vulnerabilities and security measures discussed.

Chapter 7 describes the areas on which Finanstilsynet intends to focus particular attention, and at the end of the report there is a glossary explaining key terms and concepts.

2 Summary

2.1 Finanstilsynet's findings

Institutions are required to report to Finanstilsynet any significant faults and failures that occur in the operation of ICT systems. Through the follow-up of reported incidents, findings from inspections and other forms of industry supervision, Finanstilsynet gains a good insight into institutions' use of ICT, payment systems and relevant areas of risk.

A few more incidents were reported in 2014 than in 2013, and the favourable declining trend seen in the past few years was interrupted halfway through the year. In the course of 2014 there were some serious incidents relating to breaches of integrity and confidentiality. Few malicious attacks were reported.

Observations show that there is potential for improvement in institutions' monitoring and control of access to applications and data.

Payment systems

Financial stability is dependent on well-functioning, available payment services and systems. Breakdowns in these services and systems, whether in the form of planned malicious incidents or as unplanned incidents, can pose a threat to stability and quality.

Finanstilsynet considers payment services to be generally stable and of satisfactory quality, although 2014 saw a rise in the number of serious incidents and in payment system unavailability, which returned to the 2011 level. Although the incidents per se did not jeopardise financial stability, there were a number of incidents which, had they been allowed to develop, could have impacted on financial stability.

Although attacks on payment services do occur, direct losses are still small. The low losses can largely be ascribed to measures taken by individual institutions and the financial sector. These crucial efforts to put in place preventive measures must continue. It is therefore important to give priority to governance, and to continue to take steps to ensure collaboration on common solutions and infrastructure.

The percentage of losses arising from payment card transactions where no PIN code is required (Card-Not-Present transactions) is rising significantly, and has close to tripled in the past three years. However, the losses are small in a global context.

Banks

Observations showed weaknesses in institutions' operating systems in the form of inadequacies in solutions established to ensure business continuity. These particularly affect payment services. Potential for improvement has also been seen in connection with disaster recovery systems.

Inspections of compliance with regulations laying down requirements for computer systems and reporting to the Norwegian Banks' Guarantee Fund, found that not all banks had established systems for reporting in accordance with the requirements. The quality of the data submitted varied substantially.

Securities

The overall picture in the securities sector in Norway is one of both high stability and high quality. This is underscored by the fact that there were few incidents in 2014, although some were serious as they resulted in breaches of confidentiality.

Ensuring acceptable risk in legacy systems can pose a challenge. The core systems of the Norwegian Central Securities Depository (VPS) are one of the most critical components of securities trading in Norway. To ensure continued high stability and high quality, a major project is currently being carried out to replace these systems with new, more modern solutions.

Insurance

Both stability and quality are high in the insurance sector. However, a number of incidents occurred in 2014, which were serious since they resulted in breaches of confidentiality.

Certain insurance companies were seen to have potential for improvement with regard to testing of contingency preparedness systems and to fail to involve themselves sufficiently in service providers' contingency preparedness and disaster recovery testing.

Consumers

Finanstilsynet notes that new developments in digital crime, or cybercrime, are increasing the vulnerability of consumers. It is therefore important that service providers produce secure, safe solutions that are easy to use and understand, establish high-quality processes when services are outsourced (e.g. in connection with the delivery of security tokens), and adopt a proactive approach in providing information on services and ways in which consumers should protect themselves against cybercrime.

2.2 Observations from interviews and surveys

Interviews and surveys conducted in financial institutions show that the most prominent threats appear to be targeted attacks by intruders to gain access to ICT infrastructure and applications.

Other areas of threat that present significant risk are the increase in ICT- and cybercrime, security loopholes in software that can be exploited by criminals, heavy dependency on the internet, employees' use of social media and information that falls into the wrong hands.

The complexity of ICT systems also poses a high risk to data quality and operational stability, and can hamper new product development.

2.3 General trends

Technological developments and efforts to ensure financial stability in the financial sector generate a need for changes in services, infrastructure and regulatory frameworks in every part of the sector. Seen as a whole, these changes represent an increased risk. New technology can introduce new, unknown vulnerabilities and create greater risk. In the payment services sector, in particular, major changes are taking place in the battle for the online and mobile payment service market, and there is a risk that security systems are not being given sufficient emphasis in the competition for market shares.

The rise in ICT- and internet-based crime and the heightened threat picture that accompanies this increase for institutions and consumers alike, have led to a significantly stronger focus on IT security, nationally, globally and on the part of the authorities. New financial sector participants who are not subject to Norwegian law and who operate in a borderless internet, create challenges for customers, Norwegian financial institutions and authorities. Intentional incidents can also have ramifications for financial stability. Attacks are increasingly targeted and sophisticated, and the financial sector may be exposed to attacks of the same nature as those suffered by other industries, such as the telecommunications sector.

Changes have taken place in the ownership structure of key providers of services to the financial sector and in the institutions' choice of service providers. These changes may bring improvements, but they can also create new vulnerabilities. In general, changes lead to higher operational risk when interaction constellations are altered. It is important that institutions

have control of their changes and risks, since the aggregate effect of the changes could pose a significant risk to the Norwegian financial infrastructure.

In several places in the report, it is pointed out that technological developments, when used in the right way, can help to reduce the vulnerability of national payment systems.

2.4 Current areas of risk identified in the 2014 analyses

Current areas of risk have been assessed on the basis of the security goals integrity, confidentiality and availability and the importance of IT services functioning satisfactorily as support for business operations.

In Finanstilsynet's assessment, the risk related to integrity is high and increasing, the risk related to confidentiality is moderate and stable, the risk related to availability is moderate and increasing and the risk related to IT services functioning satisfactorily as support for business operations is moderate and stable.

Financial institutions were under attack in 2014. The effect of the attacks was mitigated by measures implemented by the institutions. Digital attacks on the financial sector could pose a threat to markets and financial stability.

As in previous years, changes in systems and operating environments appear to be the most frequent cause of error or the risk driver in institutions, which must continue to focus special attention on this area.

It is difficult for consumers to deal competently with threats and vulnerabilities in financial services, and the financial industry has a major responsibility for ensuring that sufficient security is incorporated into their systems.

2.5 Further follow-up by Finanstilsynet

Finanstilsynet will continue to give priority to maintaining a close dialogue with important financial sector participants, in order to ensure that they understand the level of risk and in order to understand the challenges faced by the institutions. Emphasis will be placed on gaining insight into the institutions' contingency preparedness solutions, outsourcing, access management and efforts to ensure IT security. This will primarily be achieved through IT inspections.

Finanstilsynet will attach importance to following up on incidents, monitoring the threat of crime and keeping abreast of the development of payment services. Finanstilsynet serves as the secretariat and chair of the Financial Infrastructure Crisis Preparedness Committee (BFI), and will continue its work in this capacity.

3 Finanstilsynet's findings

This chapter presents findings and observations based on IT inspections carried out, incident reports received and notifications of new payment services and changes in existing services. It also describes the follow-up of IT projects, outsourcing agreements and participation in national and international working groups and organisations in 2014. The topics of payment systems, securities, banking and insurance are addressed in sub-chapters.

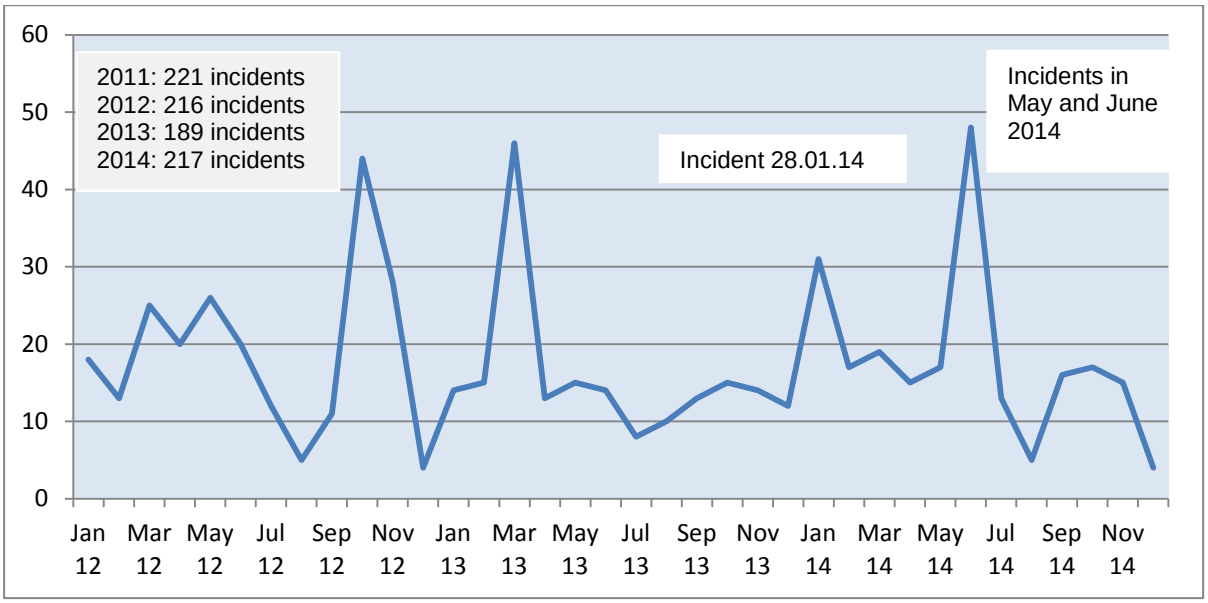
3.1 Incidents reported in 2014

Institutions must report to Finanstilsynet any faults or failures entailing a significant reduction in functionality due to a breach of confidentiality (data protection), integrity (protection against unauthorised changes) or availability of ICT systems and/or data. Reporting must normally cover incidents classified by the institution itself as "extremely serious" or "critical", but may also cover other faults or failures if they reveal special vulnerabilities in applications, architecture, infrastructure or defences.

The number of incidents reported in 2014 was approximately equivalent to the level in previous years. With the exception of one serious operational incident that affected numerous banks in January, the positive trend from 2013 continued in the first half of 2014 with fewer operational incidents than in preceding years. In May and June, several operational incidents occurred with an interval of a few days, affecting many banks. In the course of the year, there were a number of serious incidents involving loss of integrity and confidentiality. There were few reports of malicious attacks.

In 2014, Finanstilsynet established a procedure for notifying the Ministry of Finance of particularly serious incidents, or incidents liable to receive extensive media coverage. The Ministry of Finance was notified of nine incidents in 2014.

Figure 1: Number of incidents reported in the period 2012–2014



Source: Finanstilsynet

3.1.1 Operational incidents that affected many banks

The operating environment is particularly vulnerable in two areas where fault situations have far-reaching consequences: networks and central systems. Networks are especially exposed, as was demonstrated by incidents in 2013 and 2014. On those occasions, a number of banks were hit simultaneously by one and the same incident in the network. Further network separation may be one way of ensuring that business continuity systems function as intended.

3.1.2 Operational incidents that affected individual banks

A number of serious incidents affected individual institutions in 2014. A power outage in a data hall caused down time and delays in the traffic pattern for several days which had consequences for services for the general public. An operational incident on 17 February rendered this bank's public services more or less unavailable on that day. In October another incident affected VISA card customers. The same transactions were debited two days in a row. In the scheduled reversal the following night, the transactions were erroneously debited a third time.

There were also serious individual incidents in connection with the transfer of systems and/or operations to a new service provider, some of which had significant consequences for customers, such as lack of access to online banking in order to make payments.

Incidents in 2014 also revealed weaknesses in the design of business continuity and disaster recovery systems. It is important to ensure that the threshold for initiating the disaster recovery system is not so high that it is not a real option.

In 2014, Finanstilsynet followed up a total of nine serious incidents particularly closely.

3.1.3 Incidents involving a breach of confidentiality

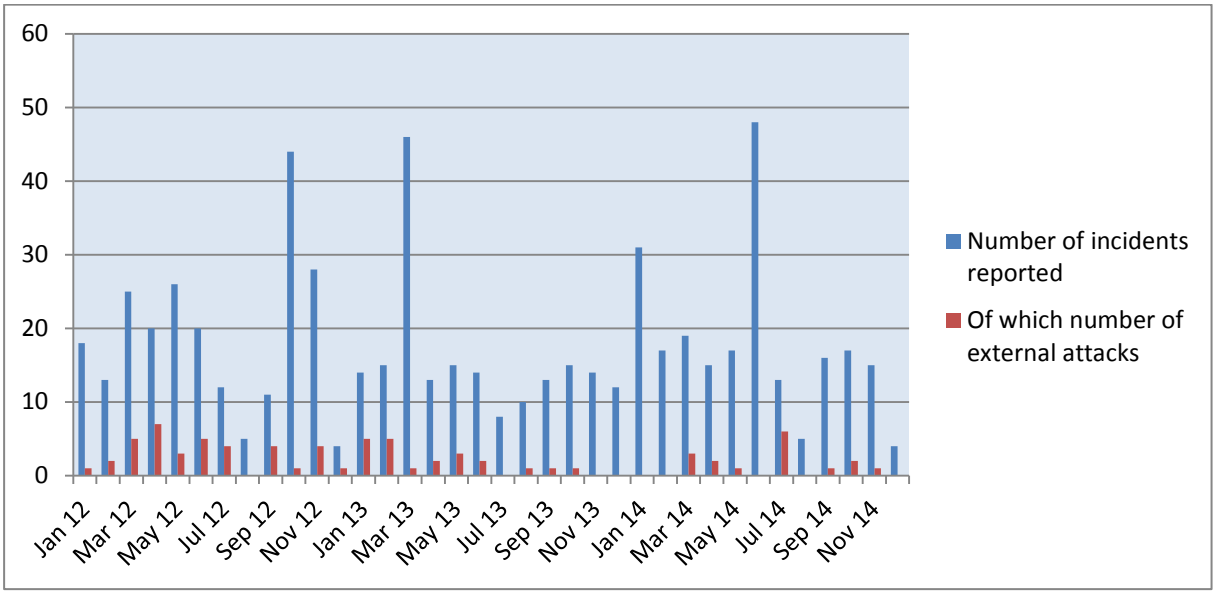
A substantial number of incidents each year involve breach of confidentiality. After changes are made in online banking systems, session management is a recurrent problem. In certain circumstances, customers have been able to access another customer's account. It can take a long time for the bank to become aware of the problem, and it is difficult to determine how many and which customers have been exposed. There is a risk that the exposed customer data may be used in attempts to commit fraud. Finanstilsynet has called for better testing of session management applications.

Confidentiality breaches are the usual reason for notification by securities firms and insurance companies.

3.1.4 Few malicious attacks

Finanstilsynet received few reports of malicious attacks in 2014. The DDoS attack on 8 July attracted the greatest attention. The attack affected a number of Norwegian banks and other types of enterprise, but was dealt with effectively and rapidly quashed. A somewhat larger number of DDoS attacks were also reported in 2014, and there were still some phishing attacks in which the swindler purported to be a bank. Insider attempts to acquire information were observed, which could be a warning that Advanced Persistent Threat (APT) attacks are being planned.

Figure 2: The number of reported external attacks (malicious attacks) in relation to the total number of incidents reported in the period 2012–2014



Source: Finanstilsynet

3.1.5 Little reporting from financial institutions other than banks

Finanstilsynet considers the level of incident reporting to be relatively satisfactory, both for Norwegian banks and for foreign banks with a branch in Norway. An indicator that this is the case is incidents affecting many banks simultaneously. In 2014, Finanstilsynet received around 20 reports from various banks and bank groups concerning the same incident

experienced by a shared service provider. Even though the original incident was the same, the banks were affected differently.

In 2014, 197 out of 217 reports were from banks. The remaining 20 were divided between the securities sector (11 reports) and the insurance sector (9 reports). This may be an indication of underreporting by the other types of financial institutions, and at the incidents seminar in 2014 Finanstilsynet emphasised the importance of insurance companies reporting incidents.

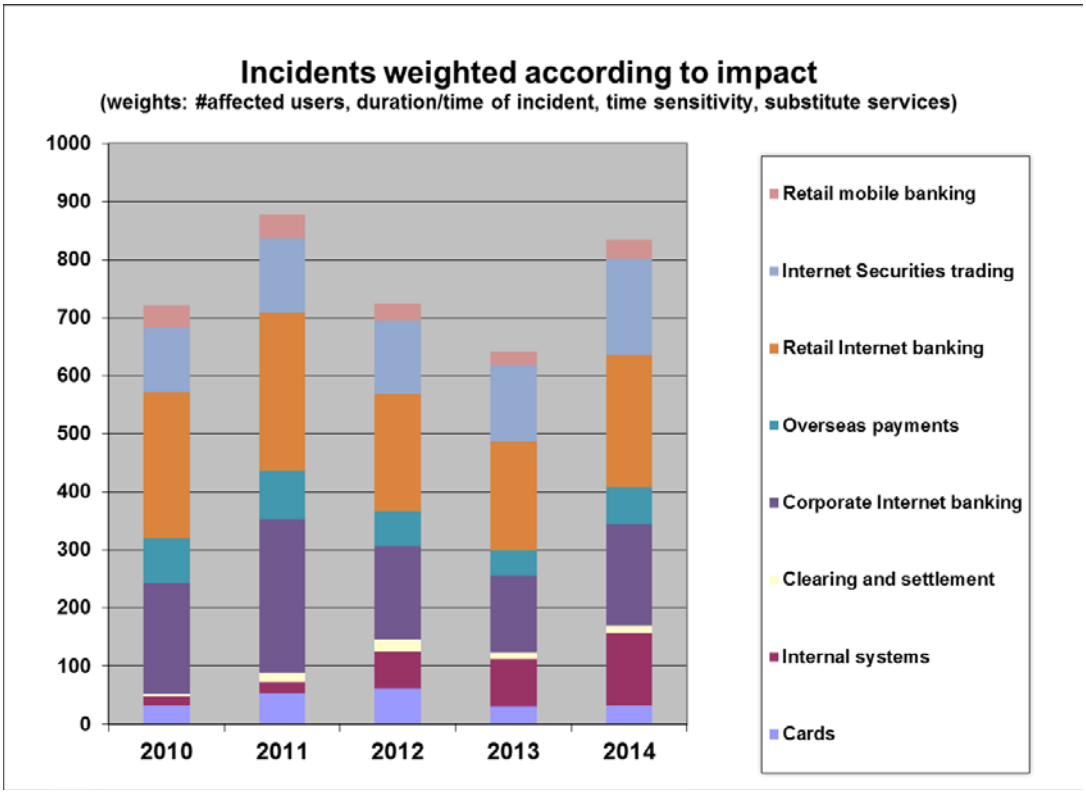
For the time being, debt collection agencies are not required to report incidents.

3.1.6 Analysis of incidents as a measure of availability

For each incident that has affected availability, Finanstilsynet has assessed the duration of the interruption, the number of institutions affected, the estimated number of customers affected and whether there are replacement services that the customer can use. In this way, Finanstilsynet has obtained a year-by-year index of the payment system's unavailability, and can thereby follow the trend over time.

Figure 4 shows that the payment system was more unavailable to the public in 2014 than in 2013. Up until June 2014, it was less unavailable than in the corresponding period in 2013, but due to incidents during the rest of 2014 this positive trend dating back to 2012 was reversed.

Figure 3: Incidents weighted according to impact



Source: Finanstilsynet

3.2 Payment systems and developments

3.2.1 General comments regarding payment systems

Effective, robust and stable payment systems are essential for financial stability and well-functioning markets. In Norway, payment systems 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 were established as key defences to safeguard consumer interests and to provide the best possible protection for consumer security and rights.

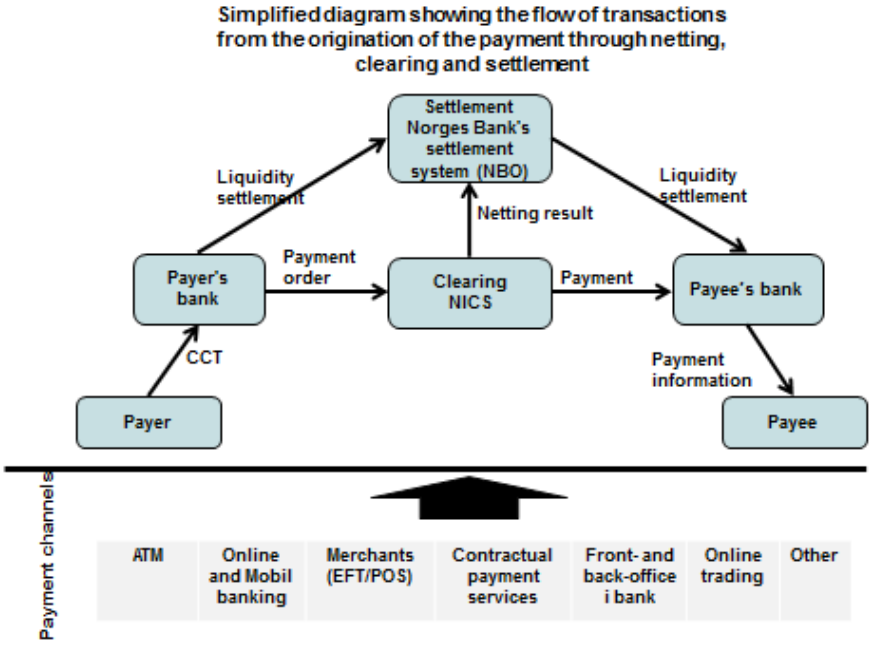
Laws and regulations are increasingly being aligned with regulatory developments in the EU, and to some extent this poses a challenge to established, well-functioning national systems such as the priority rule, where several card systems are grouped in the same physical payment card (such as BankAxept and VISA) and the traditional value chains between bank and consumer.

A payment system is defined as a system based on common rules for clearing, settling and transferring payments between two parties to a financial transaction. A legal distinction is made between interbank systems that process transactions between banks and payment services that handle transactions between customers and banks. Figure 5 shows the flow of transactions in the Norwegian payments system. The lower portion of the figure illustrates the various payment channels used by customers.

As authorised by the Norges Bank Act and the Payment Systems Act, Norges Bank and Finanstilsynet together perform important functions in the area of payment systems, collaborating and sharing responsibilities[1] so as to achieve optimal interaction in this area.

[1] http://www.finanstilsynet.no/Global/Venstremeny/Om_tilsynet/Samarbeid/Betalingssystemloven_samarbeid_og_ansvarsdeling_Finanstilsynet_og_Norges_Bank.pdf

Figure 4: Flow of transactions in the Norwegian payment system



Source: Finanstilsynet

3.2.2 Management of and risk and vulnerability in payment systems

To have financial stability, the financial system must be robust enough to provide financing, carry out payments and spread risk in a satisfactory manner. Consequently, payment systems are a cornerstone of financial stability.

Finanstilsynet noted a reduction in the availability of payment services in 2014. It also observed that in certain contexts the robustness of the payment systems is not consistent with the pivotal role that they play, whether it is a question of the payment services of individual institutions, services used by several institutions or central shared infrastructure. Incidents that occur in, or affect the payment infrastructure, have a broad impact and quickly give rise to significant consequences.

Mediation of payments is constantly evolving, and in addition to developing new services, there is an ongoing need to modify existing payment services, resulting in a rapid rate of change. The changes are made in applications, technology and communication systems alike, and are generated by a multitude of change drivers. Changes are a frequent cause of faults and failures in payment systems, and thus entail considerable risk. It is therefore essential that risk assessment and management, in addition to effective end-to-end testing processes and the establishment of a sound security culture at all levels, are a central part of institutions' development and change processes.

It is a management responsibility to ensure that individual institutions have an established framework for the governance of the entire payment system, which accords with the key role the system plays in a well-functioning economy, and with established procedures for important functions. Controls must therefore be put in place to ensure compliance with rules and regulations and with the quality standards adopted by the institution. Value chain-based

risk and vulnerability assessments must be carried out regularly, not least when developing new services and systems, in order to reduce vulnerability and risk to a defined, acceptable level, ensure effective measures to prevent criminal attacks and avoid serious incidents. This includes the establishment of an operational, contingency preparedness and security system that meets the institution's documented requirements for the payment service and regular exercises to ensure that effective action can be taken when incidents occur.

All the participants in the value chain have an independent responsibility for governance of their own operations, those of ICT service providers and not least those of (any) subcontractors. Although large parts of the electronic infrastructure used by payment systems are outsourced to ICT service providers, it is the payment service provider who bears the responsibility – a responsibility that cannot be outsourced. Payment systems will therefore always present challenges in terms of risk and vulnerability that necessitate awareness with regard to security and monitoring and implementation of measures where necessary.

3.2.3 Findings and observations

As described under reported incidents, a number of serious incidents affected the payment system in 2014. The incidents have numerous underlying causes, and no striking similarities can be seen apart from changes.

Some institutions have experienced weaknesses in their operational systems designed to ensure continuity in payment services. Potential for improvement has also been observed in connection with disaster recovery systems.

In 2014 there were some network incidents, a type of incident that hits payment services particularly hard. They usually result in simultaneous failures in several banking and payment services such as online banking, card authorisations, ATMs and cash register functions at branches and in in-store postal and banking outlets. The impact of these network incidents clearly illustrates the vulnerability of the network infrastructure.

Inspections carried out by Finanstilsynet identified deficiencies in some institutions' payment service contracts. Among other things, it was found that some contracts do not satisfy the requirements of the provisions in the ICT regulations regarding outsourcing, a matter that Finanstilsynet has followed up closely.

3.2.4 Notification of payment service systems

The Payment Systems Act requires that Finanstilsynet be notified without undue delay of the establishment and operation of payment services.

In 2014, Finanstilsynet received 13 notifications, the majority of which concerned mobile payment systems. Nine of the notifications concerned new systems, while four concerned new versions of existing systems. Based on the notifications received, some institutions have been followed up particularly closely and asked to provide supplementary information or to amend their contracts with subcontractors.

3.2.5 Mobile payment systems

The preceding paragraph shows that most of the notifications in 2014 concerned mobile systems.

Mobile payment systems are developing rapidly, both nationally and globally. At the national level, systems such as the mCASH[2] payment application and the NFC mobile payment application Valyou[3] were officially launched in 2014. Eika Gruppen is currently developing its contactless mobile payment system[4]. At the global level, Apple has launched its Apple Pay[5] (so far only in the USA), and Snapchat its Snapcash[6] payment system. Visa Europa launched its pan-European digital wallet V.me[7] in the late autumn of 2013.

In Denmark, Danske Bank's MobilePayapp now has close to two million users, while a number of other Danish banks have collaborated on the Swipe mobile banking service. In Sweden, Swish is the predominant mobile payment service with around two million users.

All of these mobile payment services are designed to increase the speed of and simplify electronic payments, and replace cash.

Finanstilsynet has made the following assessments[8] of mobile payment systems, which also include NFC:

- Increased use of electronic payments means that the user leaves more electronic traces, posing a challenge in terms of personal data protection.
- Mobile wallets mean that even more details of the "user's life" can now all be found in one place, as a result of which the user could face considerable practical problems if his or her mobile telephone goes astray or is lost in some other way.
- Having a larger number of sensitive operations in mobile telephones requires that the user knows how to protect the telephone and its use, and not all users are sufficiently aware of the importance of doing so.
- Mobile telephones are exposed to viruses and software deficiencies, and the user must update the telephone with virus protection and the latest version of software. This is not always done.
- Mobiles can be "jailbroken" by the user or other persons, causing the security of the mobile telephone to be compromised and rendering it vulnerable.
- The payment service provider must use well-known damage control techniques, such as spending limits, transaction limits and classified security levels.
- Providers of this type of payment system will either themselves or through business partners store large amounts of personal and payment-related data, placing heavy demands on service providers' security.

[2] https://www.bnbank.no/For-pressen/Pressemelding-03032014/
[3] http://www.digi.no/931241/naa-er-valyou-lansert
[4] http://www.cw.no/artikkel/it-bransjen/kontaktlos-betaling-fra-eika
[5] https://www.apple.com/no/pr/library/2014/09/09Apple-Announces-Apple-Pay.html
[6] http://techcrunch.com/2014/11/17/snapcash/
[7] http://www.visa.no/media/pdf/11068.pdf
[8] The assessments must not be regarded as exhaustive.

It may be argued that it is just as safe or safer to pay by mobile telephone as it is to swipe a card, provided that the security of the telephone has not been compromised (for instance, by jailbreaking) by the user or other persons:

- It may be safer to have payment data (card number, account number, expiry date, etc.) protected on a mobile telephone than to have such data clearly displayed, for instance on a bank card.
- Systems that provide for central storage of payment data so that the data are not stored in the telephone further reduce the vulnerability of the mobile payment system; on the other hand, they create a new risk in the form of concentration of data at the storage site. An example of this is "tokenisation", whereby payment data is converted into a "token" that functions as an alias, thus eliminating the need to either store payment data in the mobile telephone or transmit the data.
- Transactions can be protected by PIN authentication and/or a fingerprint scan.
- Payments will often be logged on the mobile telephone and can be reconciled with the bank.
- The traditional use of payment cards can make collecting and keeping paper receipts a challenge. The transaction log on the mobile phone may make it less necessary for the user to keep paper receipts.
- It may be possible to remotely erase the content of a mobile telephone, if it goes astray.
- Well-known damage control techniques can be applied, such as spending limits, transaction limits and classified security levels (low, moderate or high authentication).
- Mobile systems usually have several layers of security, including spending limits, and there is reason to believe that fraudulent use can be limited and further action taken before the damage becomes extensive.
- Mobile payment can eliminate the need to enter a PIN code in a crowded environment, such as on the bus.

3.2.6 Attacks on payment systems

In 2014, a number of DDoS attacks were seen to target banks' websites and online banking services, thereby also preventing access to payment services and security services, even though the payment or security service itself was not the primary target. The general trend is that such attacks are occurring more frequently, and with greater force.

In the course of 2014, institutions continued to see a number of phishing attacks, targeting payment cards in particular, in which fraudsters seek to appropriate data that can be used to gain access to consumers' assets. As a rule, phishing is carried out by e-mail, in which criminals pose as a genuine institution. In the same way, phishing is used to dupe consumers into visiting websites infected by malicious software. Attempts at phishing by sending text messages to mobile telephones have also been seen. Finanstilsynet considers it positive that some institutions[9] have established dedicated websites with information for consumers on what to do if they suspect that an e-mail is fraudulent, and how they can protect themselves. These websites also include a list of fraudulent e-mails sent in the institution's name of which the institution is aware.

[9] http://www.danskebank.no/nb-no/Privat/Nettbank-og-Mobil/nettbank/Sikkerhet/falsk-e-post/Pages/falsk-e-post.aspx

Although no losses resulting from Trojan attacks on online banking services and payment systems were reported in 2014, this does not mean that there is no activity. The international trend is that this type of attack is launched in waves, moving from one country to another. The attacks are now more targeted, and it must be assumed that Norway may again be affected and by more targeted attacks than before.

Despite the proliferation of mobile payment systems and a global increase in infected mobile telephones[10], Finanstilsynet does not know of any incidents of attempted fraud using mobile telephones in Norway.

In Finanstilsynet's experience, the financial institutions have effective preparedness systems, they have established good defences and they are taking effective steps to reduce both the extent of any damage and the magnitude of customer losses.

3.2.7 Overview of annual losses related to payment services

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

The tables also present loss data from a number of other countries to make it possible to compare trends. The trend in Norway in 2014 was similar to the trend in most other European countries. Losses arising from card-based payments for goods purchased on the internet are increasing, and losses arising from the use of online banking services are declining.

3.2.7.1 Losses in Norway related to use of cards

Card-Not-Present (CNP) fraud constitutes the largest category of loss. Losses are steadily increasing, and rose by around 39% in Norway in 2014. CNP losses have doubled in two years, and tripled in the past three years. Fraudulent use of lost or stolen original cards with PIN outside Norway increased by 37%. Other types of fraudulent use of payment cards remained more or less unchanged. All in all, there was a 17% increase in payment card losses.

[10] http://www.eetimes.com/document.asp?doc_id=1325677

Table 1: Loss related to use of payment cards (figures in NOK 1,000)

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

Source: Finanstilsynet

From 2012 to 2103, the volume of card payments for online purchases in Norway rose by 13% (figures from Norges Bank 2013[11]). Fraud increased by 39% from 2013 to 2014 (from approx. NOK 52 million to approx. NOK 72 million). Of the total volume of card payment transactions in Norway, around 0.026% were fraudulent. For online transactions using a card issued in Norway, over 0.1% (1 per thousand) were fraudulent.

Table 2: Number of payment cards affected by fraud

Type of payment card fraud	2011	2012	2013	2014
Number of cards affected by fraud	16,784	20,332	22,531	38,541

Source: Finanstilsynet

The number of cards affected by fraud rose by 71% in 2014. This increase exceeds the increase in losses, which means that the average loss per card declined.

3.2.7.2 Payment card fraud and data theft

Fraudulent payment card use is one of the highest technology risks faced by the financial industry. Payment card data theft has been a pervasive and profitable activity for cybercriminals for several years, and the trend continues to grow. Sites where large quantities of card-related data are stored or transmitted are the most vulnerable.

Card-Not-Present (CNP) losses are on the rise, both nationally and globally. These are primarily losses resulting 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

[11] Card fraud totalled around NOK 72 million. Figures from Norges Bank in 2013 show a volume of 59.7 billion online card payments, which means around 0.12%, or over 1 per thousand were fraudulent. http://static.norges-bank.no/pages/99263/NB_memo_1_14_2_no.pdf

payment services. Stolen payment card data can easily be used fraudulently in online stores that do not require 3-D Secure authentication.

CNP losses were one of the factors driving the establishment of guidelines issued by the European Banking Authority (EBA)[12] based on the recommendations of the European Forum on the Security of Retail Payments (SecuRe Pay), which are scheduled to come into effect as from 1 August 2015. The revised Payment Services Directive[13] (PSD2) establishes requirements for strong customer authentication, which will be included in the guidelines once the directive has been adopted.

At the global level, new, large-scale thefts of payment card data continually occur, such as at Home Depot and Staples[14]. The Verizon 2014 PCI Compliance Report[15] found a strong correlation between non-compliance with the Payment Card Industry Data Security Standard (PCI DSS)[16] and the likelihood of suffering a data breach. It is also feared that stolen data may be used for targeted phishing to acquire more sensitive data.

Although the industry in Norway is taking numerous actions and is far out in front in global efforts to reduce vulnerability, at national level it needs to monitor merchants more closely with regard to the security of internet payments, such as by requiring e-merchants to adopt 3-D Secure authentication. It is important that merchants storing large quantities of payment card data comply with internationally recognised security standards, such as PCI DSS.

The continued use of magnetic stripe cards in many places facilitates the fraudulent use of stolen card data by criminals. An interesting finding in the Netherlands noted a significant decline in skimming losses from 2012 to 2013 due to the establishment of geo-blocking where the magnetic stripe is deactivated for use outside Europe (see below).

3.2.7.3 Losses related to use of online banking

Online banking losses due to attacks using malicious software were extremely low in 2014. Conversely, there was a higher incidence of lost/stolen security devices which increased the overall volume of online banking fraud. Some of these were related to fraud in connection with the delivery of BankID security tokens through Posten Norge's Post in Shops delivery service; see further information in 3.8.1.

Table 3: Fraud losses related to use of online banking (figures in NOK 1,000)

Type of online banking fraud	2011	2012	2013	2014
Attacks using malicious software on customer's PC (Trojans)	664	5,064	1,327	552
Lost/stolen security device	3,321	3,367	1,321	6,655
TOTAL	**3,985**	**8,431**	**2,648**	**7,207**

Source: Finanstilsynet

[12] https://www.eba.europa.eu/regulation-and-policy/consumer-protection-and-financial-innovation/guidelines-on-the-security-of-internet-payments
[13] http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ecofin/146078.pdf
[14] http://www.tomsguide.com/us/home-depot-data-breach-theft,news-19577.html
http://techcrunch.com/2014/10/21/staples-becomes-the-latest-retailer-affected-by-a-payment-card-data-breach/
[15] http://www.verizonenterprise.com/pcireport/2014/
[16] https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

3.2.7.4 Losses in other European countries

Loss statistics from other countries are relevant for comparing fraud trends. However, only a limited number of European countries publish loss figures, and the date of publication differs. Few countries publish the previous year's loss figures as early as Norway. Loss statistics from other countries are reported below. Due to publication delays, these figures and figures for Norway for 2014 are not entirely comparable, but they nonetheless provide an indication of trends.

Payment cards

The Third Report on Card Fraud[17] issued in February 2014 by the European Central Bank (ECB) showed that after several years of declining losses, total payment card losses for the European countries increased by 14.8% from 2011 to 2012 and CNP fraud rose by 21.2%. All categories of loss increased, but at 60% the proportion of CNP losses was largest in terms of absolute value and CNP fraud was the category with the highest growth. Domestic transactions accounted for 93% of the total volume of card transactions, but only around 50% of fraudulent transactions. A total of 5% of transactions in the Single European Payments Area (SEPA) were cross-border, while 25% of fraudulent transactions were cross-border. Around 2% of the transactions were acquired from outside SEPA, but accounted for 25% of the fraudulent transactions. Fraudulent point-of-sale (POS) and ATM transactions using cards issued in SEPA countries occur almost exclusively in countries outside SEPA. Just as in Norway, the magnetic stripe is skimmed and used in countries where the magnetic stripe portion of the card can still be utilised.

In the UK[18], payment card losses rose 16% from 2012 to 2013 and CNP fraud by close to 22%. At the same time, the total volume of card-based payment transactions increased, which means that the fraud-related share of the total volume increased by only 0.003%.

In the Netherlands, payment card skimming was reduced by 76% from 2012 to 2013, due to geo-blocking whereby the magnetic stripe is deactivated for use outside Europe.[19]

Online banking

Losses due to Trojan attacks on online banking services in Norway and in several other European countries are generally low.

Denmark[20] has seen more or less the same trend in online banking attacks as Norway, with losses peaking in 2012, followed by lower activity and finally very low losses in 2014. Losses for the Netherlands[21] show a decline in online banking losses of 72% in 2013.

Fraud loss figures from Belgium[22] show a drop of 85% in the number of fraud cases in 2014. This is as strong a decline as was seen in the Netherlands, but took place a year later. The decline is ascribable to a combination of several factors, including increased consumer vigilance. A number of information campaigns have been conducted in Belgium to warn the general public against careless use of the internet and online banking services.

[17] http://www.ecb.europa.eu/pub/pdf/other/cardfraudreport201402en.pdf
[18] http://www.financialfraudaction.org.uk/Fraud-the-Facts-2014.asp
[19] http://www.nvb.nl/thema-s/veiligheid-fraude/166/fraude.html
[20] http://www.finansraadet.dk/tal--fakta/Pages/statistik-og-tal/netbankindbrud---statistik.aspx
[21] http://www.nvb.nl/thema-s/veiligheid-fraude/166/fraude.html
[22] https://www.febelfin.be/nl/fraudegevallen-internetbankieren-dalen-sterk

In the UK[23], online banking fraud losses increased by 4% from 2012 to 2013. The volume of losses through the use of online banking services (GBP 40.9 million) in 2013 was less than one-tenth of the volume of card fraud losses (GBP 450 million).

3.3 Securities

In the securities industry, far-reaching changes are taking place that entail risk and necessitate quality assurance. Here, too, old legacy systems can present a challenge, while replacing the systems may also entail a risk during the replacement process.

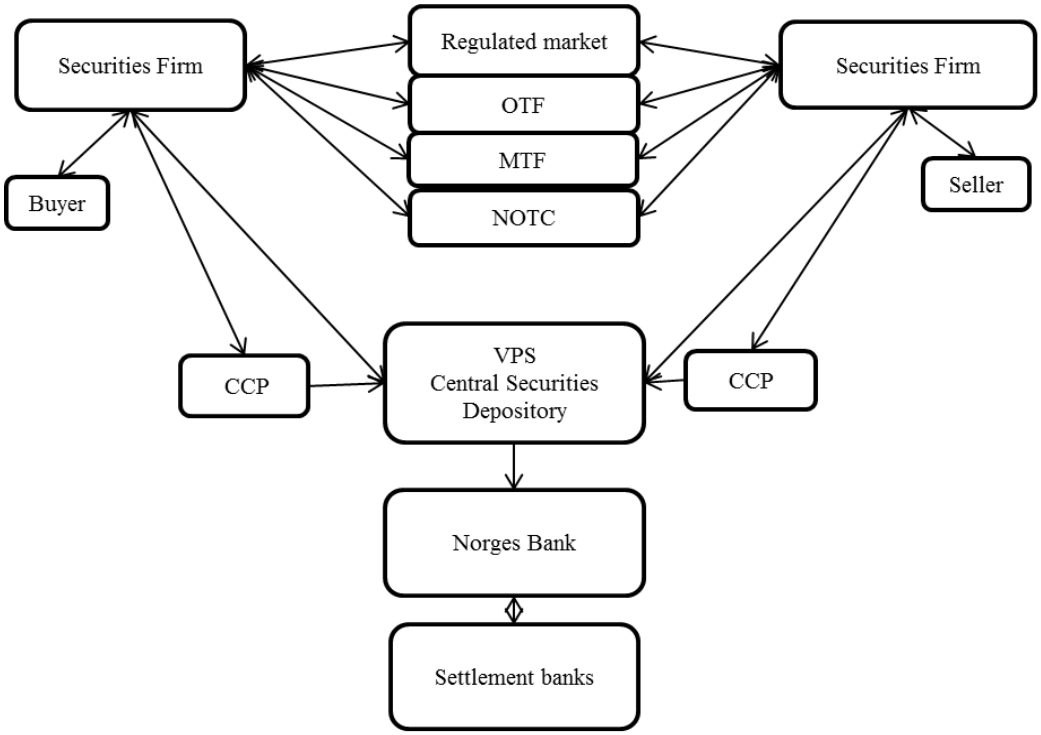
A wave of regulatory changes is sweeping across this sector that will affect infrastructure and operators in an increasingly borderless EU. New marketplaces for securities trading based on cross-border electronic trading are affecting the volume and revenues of existing marketplaces and creating a need for changes.

The overall picture in this sector in Norway is still one of high stability and high quality, but ensuring acceptable risk in the face of the changes anticipated in this sector going forward may pose a challenge.

Figure 8 shows the entities/players involved in securities transactions by type of security traded. The upper part of the figure shows the execution of the actual transaction, while the lower part illustrates the settlement process.

[23] http://www.financialfraudaction.org.uk/Fraud-the-Facts-2014.asp

Figure 8: Key roles and links in the securities sector



OTF: Organised Trading Facility
MTF: Multilateral Trading Facility
NOTC: Norwegian Securities Dealers Association's system for unlisted securities
CCP: Central Counterparty Clearing House

Source: Finanstilsynet

3.3.1 Securities firms' use of cloud-based services

In 2014, Finanstilsynet noted a growing trend towards outsourcing office applications among securities firms as well. By using available technology, firms can achieve economies of scale, and the need for employees with specialised IT expertise is limited to the purchasing function.

Applications and storage systems used by ICT service providers are generally administered by dedicated, professional staff. This may help to reduce the risk of operational disruptions and makes cloud technology an attractive option for securities firms.

Large companies like Google, Microsoft and Amazon offer standard contracts for cloud-based services. The purchase of cloud services is deemed to be an outsourcing contract, and firms must make sure that they retain management and control of services, thereby ensuring that they have control of their own ICT activities and that they are in compliance with the ICT Regulations. This applies to areas such as disaster recovery testing, annual risk assessment of services, change management and incident reporting.

The provision of standardised, reasonably priced ICT services can give rise to new challenges. The set-up of traditional systems for storage and application operation has, in the past, been resource-intensive. The staff members responsible for business operations in firms may be tempted to procure ICT services without going through their own IT department. As a

result, the systems may not be subjected to relevant risk assessments, and may not be aligned with the firm's strategy and systems architecture.

3.3.2 Administration of users with access to sensitive corporate information in IT systems

Securities firms process a great deal of sensitive information, and it is therefore important to protect information regarding corporate events and other price-sensitive information. Firms must ensure that the information is adequately protected during storage, during transport, in connection with print-outs and e-mails (encryption) and when stored on USB flash drives. Where access is concerned, it is the responsibility of the firms to ensure adequate control. This also applies to the use of outsourced file exchange systems and the distribution of sensitive information.

Cases of inadequate control have been observed, and in future Finanstilsynet will emphasise supervision of processes for managing access to sensitive information and related application access settings.

3.3.3 Concentration risk in network infrastructure

Securities market participants all use very much the same network infrastructure in relation to marketplaces and clearing houses. This infrastructure has so far proved to be both robust and cost-effective. Nonetheless, Finanstilsynet is concerned by the fact that this constitutes a concentration risk, with major potential consequences in the event of a fault situation, and therefore deems it important that this concentration risk be reflected in risk analyses and preventive measures in this area.

3.3.4 Risk in connection with changes in key infrastructure components for securities trading

The Norwegian Central Securities Depository (VPS) is currently replacing major components of its core systems. This is a large-scale project that will continue to entail substantial risk. Finanstilsynet considers the VPS's systems and data to be part of Norway's critical financial infrastructure. The VPS's core systems are among the most critical components in securities trading in Norway. Finanstilsynet is monitoring the project and expects the VPS to perform high quality risk assessments and to adopt best practices for project management and change management when introducing new systems.

3.4 Banks

3.4.1 Changes related to operational service providers

The trend in 2014 showed that a growing number of banks are changing service providers and systems in central areas of their ICT activities. They are breaking their ties with service providers that they have had for many years, and often choose several different providers. Institutions are playing a more passive role when it comes to IT development and day-to-day operations.

A number of major organisational changes have taken place in the past two years. In 2014, Finanstilsynet continued to monitor changes in the organisation of Nets, with particular emphasis on the agreement between Finance Norway (the banks) and Nets. In 2014, Nets was sold to Advent International and Bain Capital. Evry was also offered for sale.

In 2014, requirements relating to data hall equipment acquired new relevance due to new outsourcing partners, the construction of new data centres and operational incidents (see 5.2).

Changes in service provider agreements and operational systems can increase risk, especially during the change process. The institution is responsible for its own operations, which include the parts of their business functions that are outsourced, such as ICT (see section 12 of the ICT Regulations). It is therefore important that the institution's risk assessment also covers the outsourced functions in order to obtain an overview of the overall risk for the business areas.

3.4.2 Disaster recovery preparedness

Findings in 2014 indicate that it will take longer than assumed to restore ICT services in a disaster situation. Two factors have a particular impact in this respect: 1) inadequate coordination of institutions' own disaster recovery plan with the disaster recovery plan for the outsourced services, and 2) the insufficient scope of disaster recovery testing and inadequate documentation of test results by both the institution and the service provider. Finanstilsynet has also noted institutions' lack of plans for dealing with various situations, such as how to run their operations without ICT for a period of time, and how to inform their customers and employees.

When disaster recovery plans are drawn up, institutions should carry out impact analyses and risk assessments based on their business functions. The disaster recovery plan must identify critical infrastructure, necessary personnel and services on which its business functions are dependent to be able to operate as intended. Requirements must be documented for the various systems comprising the disaster recovery system, stipulating how long the business can operate without system support and how much data loss the institution can tolerate.

3.4.3 Outsourcing agreements

Each institution is responsible for its own operations, which includes the parts of the business functions that have been outsourced. Finanstilsynet wishes to point out that even if the service provider is certified, for instance under ISO/IEC 27001: 2005, this does not automatically constitute compliance with the provisions of Finanstilsynet's ICT Regulations. This applies in particular to governance of ICT operations. The institution's management and control of its own activities must ensure that applicable rules and regulations are observed and that agreements are upheld. This requires, in particular, that institutions have sufficient access to information on, and control of the provision of services to be able to verify compliance with the ICT Regulations. This applies, among other things, to factors such as disaster recovery testing, annual risk assessments of the service provided, change management and incident reporting.

Finanstilsynet considers insight into the provision of services to be essential for institutions' ability to assess risk and govern their own activities.

3.4.4 Regulations on computer system requirements and reporting to the Norwegian Banks' Guarantee Fund

The Regulations on computer system requirements and reporting to the Norwegian Banks' Guarantee Fund came into force on 1 July 2013. In 2014, Finanstilsynet and the Norwegian Banks' Guarantee Fund carried out inspections of four banks to assess the banks' compliance with the Regulations. The focus of the inspections was to investigate how quickly the banks, Finanstilsynet and the Guarantee Fund can prepare the information necessary to serve as the basis for paying out secured assets if the bank were to be placed under public administration. Not all the banks had established systems for reporting in accordance with the regulatory requirements. Moreover, the quality of the information provided varied substantially. This topic will be followed up in similar inspections in 2015. The banks have offered constructive comments and drawn attention to unclear points in the text of the Regulations. Finanstilsynet and the Norwegian Banks' Guarantee Fund have taken note of these comments and have decided to prepare a guide to the Regulations.

It is important that the institutions develop systems that meet the requirements of the Regulations, incorporate the reporting procedures into their contingency preparedness plans and ensure that the procedures are tested regularly.

3.4.5 Access control

Finanstilsynet has noted that in their processes and procedures banks have largely defined the tasks assigned to functions such as line managers, system owners and business owners. These tasks include the allocation and monitoring of access to systems. Line managers are often responsible for reviewing the access rights of individual employees, and it is normally required that this be done at least once a year. It is important that the information regarding accesses is of a quality and format that enables the person who is tasked with reviewing access rights, to meet the control requirements.

Most banks have a very extensive portfolio of applications. Each application has access rights that are based on the role of the individual user. It is therefore important that summaries be made showing the accesses of each user at application level, and that application accesses be subjected to the same examination as user identities, domains and file areas.

Finanstilsynet's findings show that reviews of individual employees' accesses have been deficient in several cases. This applies in particular to areas in which the individual application has its own access management capability.

3.4.6 Classification of information

In 2014, Finanstilsynet was informed that institutions classify their IT systems in order to ensure confidentiality, integrity and availability. Often the classification process is carried out by the individual system owner. Strictly confidential, confidential or for internal use are levels of categorisation used by the institutions to classify their IT systems. The categorisation is based on the need to protect use of the information and is linked to access control.

Finanstilsynet is aware that it is a challenge for institutions to manage and control the application of classification rules. This applies in particular to management of access to classified data and systems.

3.5 Insurance

3.5.1 General comments

Norwegian insurance companies vary substantially in terms of organisational structure, size and range of products. Some insurance companies are part of a larger Norwegian or foreign financial or insurance group, while others are free-standing, independent limited companies. Some life insurance companies collaborate closely with non-life insurance companies in areas such as ICT, and may appear to be one company even though they are technically separate limited companies. A number of companies work in close collaboration with banks and use the banks' distribution and sales networks. Some of the companies operating in the Norwegian market are Norwegian branches of foreign companies (Norwegian-registered foreign enterprises (NUF)). These companies are not directly subject to the supervision of Finanstilsynet.

The insurance companies that are members of Finance Norway use Finance Norway's shared systems. The differences between the insurance companies are reflected in the companies' ICT activities, challenges and risks. Nonetheless, they share a number of common features, which are described below.

3.5.2 Complex insurance systems

In general, insurance companies are enterprises with advanced ICT systems and services. As a rule, the companies, particularly traditional life insurance companies, have several different business-critical core systems, which are often large-scale and include many complicated actuarial tools and are difficult to manage. The systems often contain sensitive personal data. It is essential for the company that these systems are managed and used in a safe, satisfactory manner and that back-up systems, based on a business risk assessment, are established and tested regularly.

3.5.3 Control of changes

In the past decade, life insurance companies have been subject to major regulatory changes, including the introduction of compulsory occupational pensions, a new Insurance Act and a pension reform. There have also been a number of major changes with regard to pricing. Changes are continually being made; see 5.1.3. As a result of the new Insurance Act, non-life insurance companies have had to change their price tariffs. The changes have entailed a considerable amount of ICT work in the companies' core systems, which are complex and difficult to change.

Both life insurance and non-life insurance companies have long been engaged in preparing for the introduction of the Solvency II regulatory regime, which after numerous postponements is due to come into force on 1 January 2016. The new regime necessitates some quite extensive development of ICT systems. Among other things, modelling calculations and increased internal and external reporting requirements set high standards for data and data quality.

In addition to changes imposed by the authorities, insurance companies devote a great deal of effort to adapting their ICT activities to rapidly changing technological solutions, new

products and functions, and the automation and rationalisation of business processes.

Under section 9 of the ICT Regulations, financial institutions are required to report significant incidents to Finanstilsynet. Finanstilsynet has received few reports of incidents from insurance companies. A majority of the incidents concern breaches of confidentiality which are not directly related to system changes. This may be an indication that the companies have effective change controls. It may also be ascribable to a lack of understanding of which incidents are to be reported; see the information on incident reporting in 3.1.5.

Changes generally lead to increased operational risk, and it is important that the companies establish and utilise good change management processes, and that risks related to changes are controlled and managed.

3.5.4 Outsourced ICT activities

Almost all insurance companies have outsourced ICT activities, to varying degrees, and using a variety of systems. However, there are companies which, on the basis of a cost assessment and a stated desire to improve the management and control of their ICT activities, have decided to do all their ICT systems development and operational work themselves.

Under section 5 of the Regulations on risk management and internal control and section 12 of the ICT Regulations, the insurance company is responsible for risk management and internal control even when parts of the activities are outsourced. The company must have sufficient competence to manage the outsourcing agreement, which also includes being able to control the provision of services. The requirements apply irrespective of the size of the insurance company and who the service provider is.

Finanstilsynet has observed in inspections that some insurance companies are not fully compliant with the requirements in the Regulations when it comes to outsourcing. Non-compliance can result in an inadequate overview of, and control of, the company's ICT activities and risks.

3.5.5 Risk management

Risk assessments and risk management must be an integral part of the company's day-to-day work. These processes are important means of preventing losses and ensuring that the company is able to implement its strategies and achieve its goals, also in the field of ICT. This requirement is also set out in section 6 of the Regulations on risk management and internal control: "A review of material risks, based on defined goals and strategies, must be conducted for each area of activities at least once a year." Section 3 of the ICT Regulations also requires that risk assessments be conducted at least once a year or in the event of significant changes.

Finanstilsynet has found that the companies' documented risk analyses are generally fragmented and inadequate and do not cover all of the companies' ICT activities. Consequently, there is a risk that the risk analyses are not an effective means of managing the company's ICT risks within defined limits and do not contribute to ensuring that the company achieves its goals.

3.5.6 Testing of contingency preparedness systems

Institutions are required to have established business continuity and disaster recovery plans in the event of operational disruptions and loss of service. To ensure that the disaster recovery system functions as intended, business continuity and disaster recovery plans must be tested at least once a year.

In its inspections, Finanstilsynet has found potential for improvement in testing of business continuity and disaster recovery plans. Among other things, Finanstilsynet has observed that insurance companies do not take sufficient responsibility for, or become sufficiently involved in, service providers' testing of plans that affect the insurance company.

3.5.7 External data attacks

Insurance companies store personal information and often also medical and account information concerning their customers. This is information that may be of interest to intruders in many ways. In one example, the US insurance company Anthem Inc[24] was hacked in February 2015, as a result of which personal data relating to several tens of millions of customers went astray. Specific medical information was probably not stolen, nor payment card data.

Generally speaking, insurance companies, like all other financial institutions, focus a great deal of attention on and invest substantial resources in preventing and detecting external data attacks. However, there have been attacks, including DDoS attacks, on Norwegian insurance companies, and Finanstilsynet is aware that some insurance companies are concerned about industrial espionage, for instance in connection with product pricing.

3.6 Findings in other institutions

Finanstilsynet conducts some on-site IT inspections in debt collection companies and estate agencies. Moreover, estate agencies and debt collection companies undergoing ordinary industry inspections must complete a simplified self-evaluation form containing questions about their IT activities. In 2014, Finanstilsynet commented on the lack of contingency preparedness systems, failure to protect confidential information, the lack of procedures for handling security incidents and the fact that the enterprises ascribed responsibility for IT processes to the IT service provider.

3.7 Prioritisation of electricity and telecommunications for critical financial infrastructure

Finanstilsynet has been a prime mover in efforts to ensure that the financial sector has priority access to electricity and telecommunications in an emergency situation and to ensure cross-sectoral collaboration. Meetings with high-priority financial institutions revealed that they largely use the same electricity and telecom service providers. Meetings were held between the high-priority financial institutions and the main electricity and telecom service providers

[24] http://www.usatoday.com/story/tech/2015/02/04/health-care-anthem-hacked/22900925/, http://www.anthemfacts.com/

to inform the latter about the installations that underpin the priority systems. The intention was to ensure that the electricity and telecom service providers are able to give priority to the critical financial services in a crisis situation. The financial institutions have established procedures to ensure that electricity and telecom service providers are informed of changes, and Finanstilsynet will monitor that these procedures are followed in the event of system changes that affect the delivery of electricity and telecom services.

3.8 Consumers

3.8.1 Inadequate ID check on delivery of BankID

A number of erroneous deliveries of the security token used in conjunction with the BankID authentication system have been reported. This applied to 15 out of 150,000 deliveries in 2014. These errors have been seen to have very serious potential consequences for the individual consumers affected. Finanstilsynet has reason to believe that the ID check carried out has been inadequate in a number of cases. This type of delivery error usually occurs in a Post-in-Shop facility, where inexperienced shop employees do not carry out a sufficiently thorough ID check. This situation is exploited by fraudsters who have acquired a bank customer's data and ordered a new BankID security token which the bank sends by post. The ID check carried out on such occasions may be inadequate.[25]

A customer who is compromised (placed in a bad light) in this way may be put in a situation that is both difficult and unpleasant, where his or her deposit accounts may be unlawfully emptied if unauthorised persons gain access, for example, to the customer's online banking service. It is the banks' responsibility to ensure that the BankID security token is delivered to the right person, and in such cases the bank must take responsibility for dealing with the matter and indemnifying the customer against any losses. The procedures for delivery of security tokens, for instance at a Post-in-Shop or Bank-in-Shop if the bank chooses this method, should meet the same standards of quality and implementation as those followed in traditional bank branches.

3.8.2 Online transaction fraud

Many consumers have been swindled in online transactions between private individuals. There are a multitude of examples of situations in which the seller should be more alert and fails to envisage that he or she might be swindled. Goods are delivered without payment, and in some cases sent to unknown foreign addresses without any guarantee of payment. Online stores offer payment services, but a great many users do not take the trouble to use them. For online merchants, the manner in which payment services are offered becomes a question of striking a balance between user friendliness and security. To Finanstilsynet's knowledge, none of the online stores for transactions between private individuals require the mandatory use of payment services.

3.8.3 Online stores and information security

Use of online stores has soared in the past few years, which entails certain risks. In the majority of cases, it is relatively simple to see whether a website has the requisite security,

[25] http://www.dn.no/nyheter/2014/07/18/2156/Finans/det-er-grunn-til-a-vaere-bekymret

such as encryption. Consumers can see whether this is the case from a small padlock icon in the address field, next to the name of the website. On some browsers, it will be green; see the example below on Microsoft's certificate.

Figure 9: Example using Microsoft's Internet Explorer

Additionally, the user can check that the name in the address field matches the user site that the user wishes to visit.

Websites should have a system that encrypts the information entered by the consumer regarding the goods selected, log-in, payment and delivery address. The purpose of the encryption is to ensure that the information is only known to the consumer and the store. If a website does not have an encryption system, users should be extremely cautious about entering information that could be used by others. Very often, the lack of an encryption system is highly indicative of the quality of the webstore. For instance, such a lack can make it easier to carry out a "man-in-the-middle" attack, since it will be difficult for the user to detect whether or not he is in direct contact with the online store.

3.8.4 Cards and PIN codes

In 2014, Finanstilsynet assessed certain aspects of the security of payment card systems, with particular emphasis on integrity protection by means of a PIN code. Finanstilsynet concluded that in cases where the payment card has been fraudulently used with a PIN code, and the customer claims to have kept the PIN code secret, each of these cases should be followed up with in-depth, independent technical investigations in order to determine the course of events.

4 Other observations

This chapter considers the foremost threats taken up by the institutions 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 Financial institutions' risk assessment

4.1.1 Interviews

In 2014, Fnanstilsynet interviewed a variety of financial institutions in its study of ICT risk. Some threats are reported by many institutions. If they materialise, certain threats can severely damage an institution, and some can cause considerable harm and inconvenience to consumers. The threats the institutions are concerned about are described below. In some instances controls mentioned by the institutions are described.

4.1.1.1 Intruders gain access to ICT infrastructure and applications

The institutions report that attacks have gradually become tailored so as to target specific institutions. They start with phishing, infected flash drives (USBs), or social manipulation[26]. The malicious code is very difficult to detect. The attacker takes the time he needs, and moves one step at a time. A typical attack may start with the malicious code mapping the different segments of the network. After that, the malware searches for users with high-level access rights. The malware uses these rights and inserts self-signed certificates in the whitelist in the operating system, and then presents the user with a false copy of the log-in page and thus gains access to the user's log-on ID and password.

In order to counter these threats, institutions must have effective access controls. The access rights must be up to date and relevant. Administrator rights must only be used by a few specified persons and only in connection with specific tasks. The institution must log and analyse the activity of administrators and other users with high-level rights. The institution must ensure that tasks are distributed as far as possible, so that the attacker cannot use one and the same user to inflict heavy losses or high risk on the institution. The institution must be as familiar as possible with its traffic pattern (volume, services, ports, protocols) through the operating day, and take action in the event of departures from the operating pattern ("fingerprint") so that potential intruders are stopped.

Attackers prefer to use their own customised tools. If the institution has whitelists, i.e. lists of approved software, the attacker will be forced to resort to scripts or system tools that run on the computer. The use of such tools and techniques makes it more difficult for the attacker to hide, and increases the "noise" associated with the attack, which may make it easier to detect.

[26] The attacker succeeds in impersonating a trusted person, and abuses this trust and infects the institution.

4.1.1.2 Complexity

Many institutions indicate that the ICT systems are so complex that they constitute a risk to stable operations, and inhibit innovation. The complexity arises as a result of functions that are no longer in use, have been replaced by a new functionality or have been incorporated into other functions that are not deleted from the production environment. This may result in a number of drawbacks and costs. The functions may, for example

- occupy resources (memory, hard disc) during testing and production
- have to be administered (JCL, production planning)
- be included in security backups and disaster recovery and business continuity plans and testing
- entail unnecessary updates
- entail unnecessary licence expenses
- contain security holes that attackers may exploit

Added to this comes the complexity resulting from the fact that a number of core systems are based on technology that is 20–40 years old.

The institutions should have procedures to ensure that functions that are no longer used, or used very little, are removed, discontinued over time or merged with other functions. Finanstilsynet's view is that individual institutions should review and clear up their systems in this respect.

4.1.1.3 Disaster recovery

In 2014, some major institutions of significance to the financial sector were hit by malware or other factors that put parts of their operations out of commission, thereby revealing vulnerabilities in the institutions.

Damage control has very high priority for an institution that is under attack, and can only be carried out if the institution has an overview of which functions and users are affected. This information is to be found in logs, and e-mail logs can disclose which users have opened an infected attachment. Firewall logs may also provide indications of attacks. The combination of e-mail logs and firewall logs may heighten suspicion of an attack. E-mail logs show that the user has opened a malicious attachment, and the firewall shows that messages are going to an unknown address that proves to be the attacker's control centre. Server logs can provide further indications of malware infecting the user. Logs will also be the primary source of information in the event of disruptions due to factors other than attacks. A number of institutions report that internal detector controls should be better. Many also report that they give priority to log analysis, both as a preventive measure and for damage control after an attack.

The institutions find that re-installing data and software takes longer than expected. In such a situation, the institutions want to restore the most important functions and services first. This presupposes consensual prioritisation of functions/services.

It also presupposes a knowledge of which systems support which business functions. Knowledge of systems means that the institution knows the name of the relevant executable

modules and appurtenant dataset names, which in their turn are specified in the software that carries out the actual re-installation of these modules and datasets.

4.1.1.4 Social media

A number of institutions expressed concern about the escalating use of social media. Confidential information, negative remarks, incorrect information and information about the institution's customers can fall into the hands of unauthorised persons.

Attackers use information about the institution's employees which appears on social media to craft a "personal" e-mail with a link to malware. The contents of the e-mail give the impression that the sender knows the recipient, and the trust that the recipient feels causes her to open the attachment, which proves to contain malware.

It can be challenging for institutions to protect themselves effectively against the spread of information via social media. Staff training can have some preventive effect.

4.1.1.5 EMV/chips

ATMs and EFT/POS payment terminals are specially designed for secure handling of card transactions and PINs. The terminals and the software in the terminals are difficult for attackers to access. Systems are now being launched in which mobile phones function as EFT/POS terminals at the merchant's premises, and card information lies in the user's mobile phone. The terminal, the card and the protocols used are thus more exposed to attack than previously. This represents a substantial risk and a great challenge which institutions must take into account when designing new systems.

4.1.1.6 Cyber attacks

Many institutions regard external attacks as a growing threat. Recent events show that a number of interest groups attack individual institutions, infrastructure enterprises and national ICT infrastructure in order to achieve political and/or economic gain.

ICT operations may use rented lines or the internet, or a combination of the two. Offshore operations take place partly over the internet. Internet traffic is exposed to attacks from a global community of attackers. Remote operation via the internet may also increase the probability of disruptions by comparison with local, rented lines.

Some countries engaged in conflict have been excluded from the credit card systems. If the central card infrastructure is attacked, there is a risk that all countries will lose access. In such a situation, the Norwegian national card system (BankAxept) may be important.

4.1.1.7 Dependence on the internet

Financial institutions contend that their operations are totally dependent on an internet connection.

- The use of digital certificates presupposes checking against certificate revocation lists.
- The use of software presupposes communication linked to checking of licences.
- Software upgrading takes place over the internet.

The list provides some examples. The institutions are vulnerable to failure of the internet connection.

4.1.1.8 Delivery of BankID – security token

An account of erroneous delivery of BankID security tokens is provided in 3.8.1. Some enterprises report that they have discontinued this type of delivery.

BankID can be used to gain access to a number of personal, public services. If BankID falls into the hands of unauthorised persons, the victim may suffer severe losses and inconvenience. BankID functions in such a way that a BankID issued by any Norwegian bank can be used in any other Norwegian bank. Fraudsters have succeeded in opening an account in a new bank in the victim's name and using the BankID in the new bank to draw funds from the victim's account in the victim's bank. The victim is unable to prevent the establishment of BankID in the new bank. Through its design, BankID thus puts Norwegian bank customers at risk.

At present it is not possible to opt out of the establishment of BankID. The possibility of creating a function whereby a bank customer can opt not to allow the establishment of a BankID in his or her name should therefore be considered. As a BankID in the possession of a fraudster can have such serious consequences for the victim, banks should consider whether post offices and banks in shops should be used for delivering security tokens. In the event that the bank chooses to continue using this method, there must be sound procedures both for the delivery and for mitigating the loss and inconvenience victims may suffer as a result of fraud.

4.1.2 Questionnaire

In December 2014, Finanstilsynet conducted a questionnaire survey of 26 institutions. In the questionnaire, Finanstilsynet asks the institutions to rate themselves with respect to their vulnerability to potential threats and lack of or inadequate controls. The vulnerabilities fall naturally into six risk areas. The most pronounced findings are commented upon under the respective risk areas.

The institutions were also asked to rate their vulnerabilities as increasing, stable or decreasing. The general trend is stable or decreasing. Possible explanations for this are that the institutions consider that they have adequate measures to make them less vulnerable, or that they consider that some threats will diminish "on their own" in the time ahead. This may apply to the threat of malware, which according to some institutions has declined recently.

Some institutions provided detailed and very sound comments regarding threats and controls. The comments provide Finanstilsynet with insight into the institutions' rating of threats and countermeasures, and provide valuable input for future follow-up.

4.1.2.1 Support for strategic decisions

The risk is that IT will not function satisfactorily as support for strategic decisions, customer services or case processing.

A number of institutions feel that there is high risk associated with poor data quality, which may lead to incorrect decisions.

Several institutions consider the IT systems to be complex. The lack of overview of the interrelationships among the systems makes it difficult to foresee the consequences of changes in the systems. This is probably the reason that the institutions feel that there are defects and deficiencies in the systems.

4.1.2.2 Operational irregularities

A number of institutions stated that operating the institution's ICT systems is complex. The number of services that have to be operated has increased steadily, and the services are expected to be available almost around the clock. This places great demands on the quality of operations and there is little time available for upgrading and maintenance. See also the discussion in 4.1.1.2.

Some institutions face major changes in their operating and/or development service providers, and mark this as high risk in their responses.

Pressure on service providers appears to represent high risk for a number of institutions. Services that have appeared on the market recently have proved to have security loopholes and deficiencies. This may be indicative of a not insignificant pressure with respect to time-to-market.

Attacks on data are considered to be a significant risk. Espionage and ransomware have been found to be on the increase recently.

4.1.2.3 Data are not adequately protected

Data protection is a growing challenge. New privacy protection rules make this a challenging area. Several institutions regard intrusion into the institution's systems as a major risk with respect to data protection.

4.1.2.4 ID theft

Malware and misuse of rights in connection with IT theft are regarded as a major risk by a number of institutions. See also the discussion in 4.1.1.1.

4.1.2.5 Misuse of access to IT systems

The misuse threat includes misuse of access to IT systems for personal gain, for example insider trading, misappropriation from customer accounts, internal accounts or accounts where there is little movement.

The threat associated with misuse of rights for insider trading is not regarded as very high.

4.1.2.6 Money laundering

Several institutions consider it a challenge to develop systems that flag suspicious transactions with high precision.

4.2 Risk areas identified by security companies and internet service providers (ISP)

4.2.1 Interviews

In the autumn of 2014, Finanstilsynet had discussions with some key players in the field of security and monitoring systems in Norway, and reported on the most prominent threat areas noted by the authority as a result of these discussions.

4.2.1.1 Small number of infected PCs in Norway

There is a general decline in the number of traditional virus attacks worldwide, and Norway is one of the countries least infected by PC viruses. DDoS attacks have also had less impact over the past year. However, there is every reason to maintain the defences against malicious attacks via the internet, as failure to do so can have serious consequences for both institutions and their customers. These may be direct financial losses, damage to reputations and lost business opportunities.

The fact that the consequences of DDoS attacks have lessened is attributable to institutions putting in place effective protective mechanisms against such attacks. As a general rule, emphasis in Norway has been placed on protecting consumers against viruses, and software, internet and other service providers have all improved their protection and enabled consumers to keep their PCs updated. Although the infection rate in Norway is low, Java continues to be the prime cause of infected systems. Security is still poor, although it has improved substantially in recent years. BankID's move away from Java is a significant improvement for the banking sector.

Although it has not manifested itself in Norway, there have been international reports of a development known as reflection[27] attacks. These use weaknesses/loopholes in NTP services, for example, in such a way that DNS servers may amplify the attack. Such attacks can be carried out relatively easily once the attacker finds such weaknesses, which are also reported on hacker forums on the internet.

Internet service providers (ISPs) should play a more active part in combatting DDoS and spam. Institutions should take this up when they enter into agreements for the purchase of services from ISPs.

DDoS attacks can be used to distract attention from other types of internet attacks.

4.2.1.2 Advanced Persistent Threats (APT)

Advanced persistent threats are found to be the greatest threat posed by the internet, and are on the increase. The increase has targeted sophisticated industry in particular, but financial institutions must also be on the lookout for these attacks. In 2014, major international banks tended to be the target in the sphere of finance, because they offer a broader "client base" for fraud. As methods are refined, this may change. In the future, small and medium-sized enterprises (SMEs) are expected to be important targets for criminals, because they are

[27] The NTP service sends synchronisation messages to units or services in the local network. The attacker sends a message to this service, and uses it to forward the message to relevant units and services, thereby amplifying the attack.

assumed to have less comprehensive security measures. This also applies to small institutions, which must ensure that their local networks are well secured although the majority of the systems are outsourced to and secured by external service providers. In 2014, enterprises that actively monitor the market noted an increase from 40 to 80 targeted attacks in Norway.

Access to an institution is often obtained by way of employee PCs. This is achieved most easily through "user participation": the employee has clicked on a link, been fooled into opening an attachment or responded to a phishing e-mail. User participation is found in almost 50 per cent of the cases where such intrusion is detected. Raising the awareness of employees is the most important countermeasure, and requires training, attitude-building work and tests. Criminals also exploit unfaithful servants who can be recruited by means of enticements or threats.

After penetrating a PC connected to the internet, an attacker will look for "secure" sites to park the malware. These are units that are subject to little or no monitoring. The institution must therefore ensure that its malware protection can also monitor all connected units, for example printers. The Internet of Things is becoming more and more prominent in the networks of institutions, and all devices connected to their networks must be secured.

The building up of industry-specific CERTs is a good contribution to defence against internet attacks. Nonetheless, better cooperation between the various sectors in this area is desirable, as they have a lot to learn from one another. Extended collaboration between all parties concerned (government, police, ISPs, owners of websites and security operators) is likely to result in improvements. Countries with governments that are aware of these threats and place emphasis on security are found to have a generally low infection rate.

4.2.1.3 Mobile phones – smart phones and tablets are converging

Mobile devices such as smart phones and tablets are fairly secure in themselves. The applications run in a "sandbox" which prevents an application from infiltrating or collecting data from other applications. Note, however, that this requires that the developers are competent and adhere to a stringent security programme.

There is a general view that malware reaches mobile devices about five years later than it reaches PCs. There are no known cases of malware in Norway, but malware for Android and Windows telephones is proliferating internationally. Apple has a more stringent regime for applications, and thus far has proved less vulnerable to malware. The operating systems and functions of smart phones and tablets are beginning to converge. They are also coming closer to one another in size.

4.2.1.4 Institutions must ensure that information does not fall into the wrong hands

In order to avoid fraud, it is important that sensitive information does not fall into the wrong hands. Negligence on the part of employees may lead to leakage without their being aware of it. Many institutions give priority to getting their products out onto the market fast, and some development groups have not always given priority to security. Employees in the institution may then seek simple ways of sharing information, and take work home with them. Simple cloud services are available in homes, making it easy for an employee or a group to use them without clearing such use with the institution's security managers, which may easily result in information being exposed to unauthorised persons.

Security officers may concentrate solely on the process, without working on practical implementation. Even well documented processes must be subjected to practical testing, and internet security should be checked by means of penetration tests. Processes and solutions are not credible until they have been tested, and the testing should be conducted regularly. The institution must also have held exercises on the steps to be taken should it be subjected to an attack, or if data should fall into the wrong hands. What is needed in order to see how things fit together and design good solutions is a combination of security knowledge and network expertise. Personnel who combine these areas of expertise are in short supply in many institutions. Nor do training institutions offer such a combination in their course programmes. Frequently, the institutions themselves have to provide the training. Some have found from experience that it is advisable to use sound network expertise as a basis on which to build security expertise.

The current access systems authorise access to storage addresses or domains. These storage sites contain large volumes of data, and the individual user therefore usually gets access to more data than necessary, or to data that should have been protected from the user in question. The network topography is essential to security. Institutions' networks should be set up such that authorisation can be given for appropriate areas and/or in appropriate manners.

Storage and access systems based on who needs what are on the way in, as is the system that retrieves authorised data without the user having to deal with the storage area and how it is organised, or where it is located.

Security behaviour is important. The 80/20 rule can be applied to the distribution between human and technological weaknesses. It is important that all employees have a sound understanding of security and are aware of threats posed by the internet. Training and awareness-raising activities must be regular items in the institutions' annual planning.

4.2.1.5 Erosion of ICT expertise in financial institutions

The Norwegian financial industry has traditionally made extensive use of outsourcing. There is a tendency for more and more ICT services to be outsourced, however, and increasingly to foreign companies. At the same time, service providers that were previously owned by the institutions or by domestic interests are being sold to foreign (non-industrial) owners. This development is exerting pressure on ICT expertise both in financial institutions and in Norway generally.

Surveys of large industrial projects point to the necessity of having access to both IT expertise and procurement expertise, and inadequate expertise in this latter field has caused developers to suffer major overruns. If the internal expertise is eroded, institutions will also be in less of a position to set the correct requirements for service providers, and checking of deliveries may also be deficient. In a project setting, there is a risk that requirements will be set for the procurer that the party in question is not capable of fulfilling, such as requirements relating to functionality specifications, testing and other resources. As a result, outsourcing may become more expensive than using internal resources, and the institution's room for manoeuvre and market adaptation skills may be negatively impacted.

4.2.2 Reports from security organisations

Finanstilsynet wishes to highlight the most typical vulnerabilities applying to the financial sector, as seen by large international security companies such as ENISA[28], which works closely with EU institutions such as the European Banking Authority (EBA), the European Securities and Markets Authority (ESMA) and the European Insurance and Occupational Pensions Authority (EIOPA), and Cisco, a major supplier of technology to the financial sector.

4.2.2.1 The ENISA Threat Landscape 2014

According to the ENISA "Threat Landscape 2014" report, there have been many positive signals about combating of cybercrime in the course of 2014. The closure of central botnets and arrest of Blackhole developers resulted in a marked decline in attacks related to the use of the combination of botnets and Blackhole code.

ENISA's report presents changes in the volumes of different types of threats, as well as ranking by seriousness and the change compared with the previous year's ranking.

There was a sharp increase in data hacking in 2014, and according to ENISA's reporting system the frequency of hacking has increased by 25 per cent over the past year. As a rule, the purpose of the hacking was to obtain client data or other business-critical information from the institutions.

The manner in which the hacking takes place varies. Institutions may, for example, have poor password quality, which makes it relatively simple for unauthorised parties to access an institution's computer systems. Networks or applications may be vulnerable, or standard software not up-to-date.

One survey showed that more than 50 per cent of the hacking was due to inadequate end-user security. Phishing and malware often do the greatest damage.

Attacks in 2014 were increasingly sophisticated and targeted attacks of steadily higher quality.

4.2.2.2 Cisco – Annual Security Report 2015

Cisco's security report considers the ongoing race between attackers and defenders, security companies and security functions in financial institutions, and how the users are becoming a steadily weaker link in the security chain.

Some main points:

- In 2014, only one per cent of known security loopholes were actively exploited for cybercrime.
- Even if the best security systems are used, it must still be ensured that the quality of the monitoring processes and measures to counter vulnerabilities is good.
- Known vulnerabilities in Java were reduced by 34 per cent in 2014.

[28] The European Union Agency for Network and Information Security, which works for EU institutions and member countries.

- The volume of spam increased by 250 per cent from January to November 2014.
- In a global perspective, the security loophole in the SSL protocol, known as “Heartbleed”, still presents a major risk. Cisco reports that 56 per cent of all SSL installations have still not been upgraded.
- Malware developers are now using plug-ins on web browsers to distribute code, which has been very effective up to the present because users do not think of this as a hazard.

4.2.2.3 Finanstilsynet’s summing up

Finanstilsynet’s view, based on the above reports, is that the threat of cyber attacks is growing because the tools used are becoming more sophisticated and the methods used more varied. The attacks carried out are targeted and often executed by organisations that base their business operations on criminal activities. This type of organisation tends to have access to resources with extensive ICT knowledge, necessary data capacity and ready access to funding for their operations.

5 General trends

In the following, Finanstilsynet presents some development trends that will, or can be expected to, impact financial institutions' use of ICT and entail changes in risk and vulnerability for institutions, users and financial stability alike.

5.1 Cybercrime (digital crime)

Increasing attention is being paid nationally and internationally to cybercrime and IT security, in pace with the escalation of ICT- and internet-based crime. The EBA regards the operational risk associated with institutions' use of ICT as high, and it is expected to remain high in the immediate future[29]. The same applies to EIOPA and ESMA.

The EBA issues clear recommendations that financial institutions should give higher priority to IT-related risk and intensify ICT controls and reviews, and that they must cover all segments of the value chain (for example, ICT service providers and third-party service providers). The EBA also asks national supervisory authorities to ensure that banks, insurance companies, investors and other operators allocate sufficient resources and display the necessary care for prudent management of their digital environments to secure them against cybercrime attacks.

Targeted attacks on Norwegian enterprises increased in 2014, and the financial sector was one of several vulnerable sectors. Targeted phishing in combination with APT and other methods is used to penetrate a company's network to retrieve information. The attacks known by the names of Carbanak or Anunak, which impacted Russian banks in particular in 2014, serve to illustrate these methods. The attacks caused heavy losses[30].

There are resolutions and cooperative agreements through the UN and at regional level (EU, APEC, ASEAN, etc.) and collaboration with Interpol. The challenge is posed by nation states that are not involved in these collaborations, and the fact that systems for criminal purposes can be quickly moved to liberal locations, such as countries with inadequate legislation in this area, to avoid difficulties.

Defining a physical location for systems and data is a growing challenge, particularly since the advent of cloud-based systems. Data can be in many places at the same time, making it difficult to decide which rules of law are applicable. Cybercrime is a global problem made possible by nation states that do not have the legislation and/or executive power to enforce legislation in this area, or that are involved in it themselves.

The potential for cybercrime will increase with the growth of interconnections of "things" with sensors and control systems (the Internet of Things) through the internet. Theoretically, all "things" will be accessible from anywhere in cyberspace, limited only by the quality of the object's security systems and procedures.

[29] See 7.2 https://www.eba.europa.eu/documents/10180/934862/EBA+2014.6941+RAR+web.pdf
[30] Attack scenarios are thoroughly described and documented by both Kaspersky and FoxIT: https://www.fox-it.com/en/press-releases/anunak-aka-carbanak-update/

5.2 Changes in the service provider market, organisation and ownership and outsourcing situation

In 2014 there were major changes in both the ownership of important providers of services to the financial sector and in the service providers (outsourcing partners) chosen by some of the financial institutions. An account of these changes is provided below.

Finanstilsynet has not ranked providers of services according to skill, product range or security. The authority regards it as important that service providers comply with laws and regulations and offer secure services according to best practice. Further assessment is the responsibility of the institutions that outsource services. Service providers are all different, nonetheless, and it is important that the outsourcing institutions benefit from any possible new advantages. The right change may therefore also bring with it improvements in the spheres of both functionality and security.

A change of service providers means new contractual partners for the institution. It is important, then, that the institution includes in the negotiations requirements for both modern and fault-tolerant infrastructure and the possibility of subsequent upgrading, so as to be able to benefit from the technical advances that are still expected.

Having more suppliers operating the financial ICT infrastructure reduces the operational risk overall. This may be a strength, because in a failure situation the customer has the possibility of having services provided by an alternative supplier.

In the event of sale or change of ownership of the service providers, it is important that established contacts and cooperation procedures are also preserved, and that agreements between the companies are also established with new owners. It is primarily the institutions that are outsourcing services that must ensure that this is taken care of.

Experience shows that changes and moves are a significant source of error. The institutions must meticulously follow up changes by adapting procedures and testing new systems and configurations.

It is not certain what real significance these changes will have for financial institutions' expertise and management of IT activities, or for expertise on banking systems as a whole in Norway. Finanstilsynet is concerned that outsourcing to foreign-owned enterprises may erode Norwegian expertise on IT systems for the financial sector.

Nets is an important and key service provider in the sphere of Norwegian payment systems. The services cover both shared operational infrastructure such as NICS, BankAxept and BankID and contractual services with individual enterprises (e.g. invoicing and ATM services). Nets is the dominant player in the payment services market, and is systemically critical for such services in Norway. Nets is also a key payment systems provider in Denmark.

The banks sold Nets to an international consortium consisting of Advent International[31], Bain Capital[32] and ATP[33]. So far this has resulted in some changes in governance and

[31] Advent International is an American global private equity company with emphasis on the acquisition of companies in western and central Europe, North America, Latin America and Asia.

[32] Bain Capital is a global securities firm based in Boston, Massachusetts. It specialises in private equity, venture capital and credit products.

management, but no transfer of important operational tasks.

Evry has emerged through takeovers and mergers as a prominent provider of services to Norwegian banks, and is also a major player in other industries. In 2014, several savings banks renewed their contracts with Evry. Those banks that do not use Evry have outsourced their operations to foreign-owned operators. In autumn 2014, Evry's owners signalled that sale of the company is under consideration. In December 2014, they announced a heads of agreement with Lyngen Bidco AS, which is indirectly controlled by Apax Partners LLP.

Irrespective of its future ownership, Evry has decided to move its operations to a new data centre, Greenfield Data Centre, which is under construction at Fet, near Oslo. The relocation project will start in 2015.

Storebrand Bank has moved its operations to Skandinavisk Data Center (SDC) in Denmark. Its online banking services suffered operational disturbances during the transitional period.

Sandnes Sparebank decided in autumn 2014 to join the Eika Alliansen group, and plans to move its IT operations to SDC.

In 2013, **DNB** chose HCL as its new partner for operation of a decentralised platform. The servers are being moved to the Green Mountain Data Centre at Rjukan, Norway. Tata Consulting Services is to supply management and development services. The move is in progress. The mainframe is still being operated by Evry.

Nordea has insourced its midrange systems (including midrange computers and servers) from Nordic Processor. The move is in progress.

5.3 Developments in payment services

As stated in 3.2, technological advances strongly affect developments in payment services and payment systems through financial institutions' use of technology, through new operators establishing themselves, or through the advent of foreign operators.

These developments are taking place in payment services for mobile devices in particular, but also in security systems, where technological advances are paving the way for the development of more effective, user-friendly services. The technology also offers possibilities for making use of the services more secure at the same time, but the threat picture is increasing in step with the broader use of such services. One of the biggest malware growth areas is in mobile telephony, and this threat is expected to increase in pace with the steadily accelerating use of mobile phones for daily activities. It is important to establish antivirus and anti-phishing measures as a form of proactive security, rather than merely the reactive security offered by sandboxes. The pace of development in mobile payment systems is expected to remain high in the years ahead.

QR codes[34] such as those used by mCASH in its mobile payment system are an example of how new technology is being used in mobile payment solutions, and scanning of QR codes is

[33] ATP is the Danish pension fund.
[34] QR codes (Quick Response codes) are two-dimensional bar codes: http://en.wikipedia.org/wiki/QR_code

used instead of NFC.

Major international operators are also establishing themselves in Norway as the competitive arena becomes more open, mainly as subsidiaries or through agent services or cooperation with existing operators. This is exemplified by Visa's pan-European mobile digital wallet V.me, which Visa and partners started pilot testing[35] in Norway at the end of 2014 and which they plan to launch at the end of 2015[36].

Eika Gruppen is already well established with its swipe and go[37] solution for contactless card transfer, and will start testing its mobile solution for contactless payment in early 2015[38]. BankAxept, the leading payment card in Norway, intends to present a solution for contactless payment in 2015.[39]

Changes are also taking places in the sphere of cards and security. In autumn 2014, Zwipe[40] partnered with Mastercard to launch a pilot project in collaboration with Sparebanken Din. This is a prototype for fingerprint identification for use with contactless payment cards, and is expected to be launched commercially in the course of 2015. In these cards, the PIN code is replaced by biometric data stored directly in the card. In due course it must be expected that this technology will also be implemented on mobile devices.

It is anticipated that in the future other operators will attempt to establish themselves and their solutions in the Norwegian market, and that operators with a very dominant position in the market may quickly create major changes in the landscape. When the revised Payment Systems Directive comes into force, it will reduce obstacles to establishment such as access to payment accounts and make establishment easier for new payment service operators. At the same time, these changes will create new risks and vulnerabilities associated with payment systems which will have to be dealt with.

Mobile devices will acquire a significant role in payment services, as a medium for making payments, as a carrier of digital wallets and as a carrier of security systems. Just when contactless card payment and contactless mobile device payment become the predominant means of payment depends largely on when the payment recipients implement the necessary technology.

User-friendliness, simplicity and speed appear to be the critical factors in the battle for the mobile payment services market. There is a risk that this weighting may be at the expense of an emphasis on security.

Finanstilsynet believes that it is important that the institutions set at least the same security requirements for mobile payment solutions as for the traditional online banking solutions, i.e. that they perform thorough security and vulnerability analyses, implement measures and take steps to quality assure their development processes and ensure that sensitive information is not transferred over the internet and is adequately protected. It is important that the institutions conduct risk and vulnerability assessments of the entire value chain, including

[35] http://www.visaeurope.com/newsroom/news/vme-pilots-in-4-new-european-markets
[36] http://annualreport.visaeurope.com/
[37] https://eika.no/om-oss/kontaklosbetaling
[38] http://www.aftenposten.no/digital/Kampen-om-mobilbetaling-hardner-til-7721564.html
[39] https://www.fno.no/contentassets/9f9e2dc2b5a4464ea0b60ac1ba451cd6/oyvind-apelland--bankaxept-as.pdf
[40] http://www.tek.no/artikler/dette-norskutviklede-betalingskortet-gjor-pinkoder-til-en-saga-blott/164531

information storage. There is vulnerability associated with the value chain, as there is with the mobile application itself, as is clearly illustrated by an incident in USA-based CHARGE Anywhere LLC[41].

In order to meet these challenges, Finanstilsynet is drawing up regulations to the Act relating to Payment Systems which set requirements for the performance of risk and vulnerability analyses. A number of security requirements are proposed.

In 2014, Finanstilsynet developed a special evaluation form based on Cobit for mobile banking[42] for use in connection with supervision, and which the institutions themselves can use to assess their ICT activities associated with mobile devices and mobile payment services.

5.4 Changes in the Norwegian regulatory framework

5.4.1 Regulation of outsourcing

In 2014, there were a number of legislative amendments that regulated aspects of outsourcing. July 1st, 2014, saw the entry into force of a new legal provision, section 2-17a of the Financial Institutions Act, which stipulates which tasks can and cannot be outsourced, and that the use of a contractor does not free the institution from responsibility for the activity that is outsourced. Section 4 c of the Financial Supervision Act entered into force on the same date, regulating the duty of notification to Finanstilsynet 60 days prior to the implementation of an outsourcing contract, and Finanstilsynet's right to intervene in the planned outsourcing. New regulations were then circulated for comment which will regulate exceptions from this notification requirement with respect to the type of financial institution and activity to be outsourced. The regulations will enter into force in 2015.

5.4.2 Amendments to and new regulations

There are also plans to amend the ICT Regulations which require that agreements on outsourcing and amendments to such agreements must be dealt with by the institution's board of directors. Debt collection agencies, which are not required to report incidents at present, will be required to do so. New regulations under the Payment Systems Act are also planned which will require that risk and vulnerability analyses be performed as part of the basis for decision-making before a new payment service is launched and in the event of incidents or changes having a bearing on the security level. Finanstilsynet intends to circulate the proposed regulatory amendments for comment in 2015.

5.4.3 Amendments to the regulatory framework for insurance

As mentioned in 3.5.3, the rules for group occupational pension schemes have been undergoing major changes for several years. These include both regulatory amendments already in force, such as the new Act on Mandatory Occupational Pensions, and to which the pension schemes are in the process of adapting, and regulatory amendments in the offing,

[41] http://www.itgovernanceusa.com/blog/electronic-payment-company-charge-anywhere-suffers-five-year-breach/?utm_source=Email&utm_medium=Macro&utm_campaign=S01&utm_content=2014-12-12
[42] http://www.finanstilsynet.no/no/Tverrgaende-temasider/IT-tilsyn/Egenevalueringssporsmal/

such as a draft act on a new disability pension in private occupational pension schemes with tax benefits, and a new type of defined benefit old-age pension adapted to the new national insurance system. The amendments to the regulatory framework are still in progress and entail substantial ICT work for the pension schemes. As 3.5.3 shows, change means increased risk, and in combination the changes constitute a not insignificant risk, which companies must manage.

5.4.4 Changes in rules for securities

The US Foreign Account Tax Compliance Act (FATCA) will give rise to changes and new system designs. Pursuant to FATCA, an agreement between the US tax authorities and the Norwegian Ministry of Finance requires the disclosure of information on American taxpayers who are clients of Norwegian financial institutions.

5.5 Coordination and changes in EU rules and regulations

In the course of 2014 there were a series of EU processes associated with proposals for new, or amendment of existing directives, regulations, technical standards and guidelines which will have a bearing on Norwegian conditions as they are incorporated in Norwegian legislation.

The changes are wide-ranging, and thus represent a potential compliance risk. Changes in the system portfolio are generally a significant source of error. Extensive regulatory changes will therefore imply risk against which financial institutions must take precautions.

The proposals may also entail changes in responsibility and risk among operators in the payment services value chain, and they may introduce new risks. One undesired consequence may be that customers experience reduced security when using payment services, and that this may be reflected in eroded confidence.

5.5.1 Networks and information security

There have been extensive and demanding discussions in the EU pertaining to several of the areas in the proposed Network Information Security Directive (NIS Directive)[43]. This has considerably slowed progress in the negotiations on the proposed NIS Directive, which will continue in 2015. The financial sector is one of several that will be covered and impacted by the Directive. This subject was discussed in Finanstilsynet's 2013 RAV report.

5.5.2 Payment services

In the area of payment services, there was an extensive process in 2014 to complete the new Payment Services Directive (PSD2)[44]. This work has not yet been completed, but is now in the final stages. Agreement was reached in the Council of Europe at the end of November, forming a basis for the commencement of negotiations with the European Parliament. The one crucial new area in the Directive concerns payment initiation service providers and account information service providers and their right to initiate payments and retrieve account

[43] http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_en.pdf
[44] http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ecofin/146078.pdf

information on behalf of payers. The other important area is requirements relating to the management of operational and security risk associated with payment systems and authentication requirements, where previous references to the NIS Directive have now been replaced with the text of the Directive. The EBA has now been made responsible for drawing up more detailed guidelines for several areas covered by the Directive.

A similar process has been under way to complete the regulation of interchange fees for card-based payments, the MIF Regulation[45]. In December 2014, a compromise was reached between the European Parliament and the Council of Europe, and a formal resolution is expected in the course of spring 2015. Among other things, this will mean a requirement of a cap on interchange fees, a requirement that card schemes must be separated from processing of card payments, and requirements associated with co-branding of cards.

The Directive and the Regulation were both discussed in Finanstilsynet's 2013 RAV Report.

A working party in which Finanstilsynet participates has been established under the EBA. The working party has a mandate to:

- prepare guidelines in connection with the proposed revision of PSD2, including guidelines for security, guidelines for reporting of incidents and guidelines for notification from one EEA country (home country) to another of permission for an institution to engage in operations in the other EEA country on the basis of a licence issued in the home country.
- identify any risk that may arise from innovative payment services and that is not addressed in any of the existing or proposed directives, and where it is required that guidelines or recommendations for dealing with these risk be drawn up.
- prepare guidelines on the security of internet-based payments[46] based on the published recommendations of SecuRe Pay[47]. These were adopted on December 2014 and will apply from 1 August 2015.
- implement mandates laid down in the adopted MIF Regulation, including technical standards for separation of card schemes from processing of card payments.

The EU regulation that extends the banks' deadline for making the transition to credit transfers and direct debit in euros, including completion of the transition to a Single Euro Payments Area (SEPA), was adopted for incorporation in the EEA Agreement on 12 December 2014. The incorporation requires amendment of Norwegian law, and will therefore only enter into force after this has been done. SEPA Direct Debit is a joint European payment system for direct debit in euros, and in the longer term may entail changes in national direct debit payment systems such as the Norwegian "avtalegiro" and "autogiro".

5.5.3 Regulation on electronic identification and trust services

The purpose of the regulation is to pave the way for increased electronic interaction through mutual acceptance of systems for electronic identification (eID) and electronic signature and other trust services across national borders in the EU /EEA. Today's national rules are not

[45] http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%205119%202015%20INIT
[46] https://www.eba.europa.eu/regulation-and-policy/consumer-protection-and-financial-innovation/guidelines-on-the-security-of-internet-payments
[47] http://www.ecb.europa.eu/pub/pdf/other/cardfraudreport201307en.pdf?1b8fb7a7abcf9c9f5a0dd8e6eada19e2

harmonised and constitute a barrier. The regulation was adopted in 2014, and work is now in progress on rules and regulations for its introduction which are expected to be adopted by EU bodies in the course of the spring and autumn of 2015. At national level, concern has been expressed regarding the crime situation and civil protection in Norway if, as a consequence of the regulation, the requirement for acceptance of safety levels is set too low, and Norway cannot decide the level itself.

5.5.4 Banks

The Single Supervisory Mechanism (SSM) was established in November 2014 and consists of the European Central Bank (ECB) and national euro area supervisory authorities. Through the SSM, the ECB will have responsibility for oversight of the largest banks in the euro area. Countries that are not members of the euro cooperation may also choose to take part, but at present are not included.

The most central regulatory framework for banking is the new Capital Requirements Directive (CRD IV), which entered into force in January 2014. The regulations entail extensive new reporting and probably a need for considerable ICT adaptation. The Bank Recovery and Resolution Directive (BRRD), with common rules for dealing with failing banks, entered into force in the EU in January 2015. All banks must prepare recovery plans with concrete, implementable measures for managing financial crises.

5.5.5 Securities

Over the next few years, new regulation of securities activities in the financial infrastructure in Europe will have a considerable impact on Norwegian securities firms and appurtenant infrastructure. The new rules must be expected to demand many adjustments to systems and substantial investment in the development of new systems, often with a short deadline for implementation. Short deadlines may put considerable pressure on the development of system specifications and the systems themselves. Securities firms will also have to invest significant resources in testing and implementation. Delays may therefore easily occur, and the result of development carried out under time pressure may be systems with defects and deficiencies.

Examples of imminent regulatory changes in the EU are the European Market Infrastructure Regulation (EMIR) and the Market in Financial Instruments Directive (MiFID II) – the new investment services directive. These changes will entail new reporting requirements for institutions, with challenges relating to a pan-European choice of system and probably considerable work in making the appurtenant local adaptations. There will also be new reporting requirements for short sales.

Under MiFID II, securities firms will have more data-reporting obligations. One of the most challenging requirements will probably be that all transaction data for financial instruments must be reported to the existing transaction reporting system (TRS). Reporting must take place to the relevant financial authority in EU/EEA countries. The TRS will be substantially expanded to meet the new reporting requirement. Another, completely new reporting requirement is position-reporting for commodity derivatives and emission allowances/allowance derivatives. For transactions effected in marketplaces in EU/EEA countries, the marketplace will normally report positions on behalf of their members.

5.5.6 Insurance

The new European regulatory framework for financial stability in insurance companies, Solvency II[48], enters 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.

5.5.7 Anti-money laundering measures

In December 2014, the Council of Europe and the European Parliament reached agreement on a draft fourth anti-money laundering directive[49] and revision of the regulation on information on the payer that must accompany transfers of funds. A formal EU resolution is expected in the course of spring 2015. The draft implements the revised recommendations of the Financial Action Task Force (FATF) of February 2012. The draft has also been expanded to specify that information about the payment recipient (name, account number or the equivalent) must accompany the entire payment chain in addition to the current requirements regarding payer information (name, account number, address or the equivalent).

5.6 Joint efforts by the financial industry

Banks, other key financial sector operators and Finance Norway cooperate on security, the development of shared infrastructures, services and common standards. The results of incidents, surveillance, analyses and statistics are exchanged and discussed and action decided upon.

The financial industry's self-regulation is under pressure as a result of amendments to laws and regulations, influenced not least by changes being introduced by the EU, but also by national changes. The changes, which are intended to provide better consumer protection and a more open market, may result in increased or new threats and vulnerabilities that the financial industry must deal with. One such example is the requirements in PSD2[50] that trusted third parties must be able to access account information in the registrar bank or payment service provider. The financial services industry, acting through the Norwegian Banks' Standardisation Office (BSK) has regarded this requirement as part of its work of reviewing security aspects.

In 2014, BankAxept and BankID were established as separated limited companies as part of the business orientation of the banks' joint services. BSK is responsible for setting requirements and monitoring security and standardisation on behalf of the banks. BSK's initiative for establishing a cross-sectoral national standardisation scheme for IT security is one of the measures in the efforts to ensure ICT security for the financial services industry.

In the course of the first year since its inception in 2013, FinansCERT has put an operational organisation in place. Finanstilsynet's understanding is that the banks acknowledge the importance of this establishment, and that it will contribute to cooperation and coordination of

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

[49] http://www.consilium.europa.eu/en/press/press-releases/2015/02/150210-money-laundering-council-endorses-agreement-with-ep/

[50] Payment Services Directive 2

action on undesirable incidents in order to reduce vulnerabilities in the industry. FinansCERT provides regular information to the industry on the threat picture and developments in it. Finanstilsynet believes that FinansCert's collaboration with NorCERT and other sectoral CERTs is important nationally as well as for the financial industry. More financial service providers should preferably join FinansCERT to enable the organisation to assume the role of sectoral CERT and cover all areas of the financial industry.

In autumn 2014, the Java-free version of BankID, BankID 2.0, was delivered. User problems connected with Java will disappear gradually as service providers change their IT systems, and with them the security risk ensuing from Java vulnerabilities. However, the new system does not enable banks to obtain information about the security level of users' PCs as readily as before. Banks have to take this into account when designing services and by introducing compensatory controls. The launch of BankID 2.1 is planned for the first half of 2015, and the system will make it easier to sign documents, among other things.

Finanstilsynet is aware that the industry has placed emphasis on the quality of the identity control in the Post Office's personal delivery confirmation (PUM) service in connection with the issue of the security token that is used in combination with BankID, and that the industry is planning to take steps to improve this.

According to plan, the BSK's work to modernise the banks' online transaction exchange system ("Baltus") will be completed in 2015, and will provide a flexible, secure infrastructure for routing and transport of transaction-related financial enquiries among banks linked to the common Norwegian infrastructure. The banks, working through BSK, have also prepared a plan for transition to ISO 20022. This work will entail major changes in the Norwegian payment infrastructure over the next few years, and it is important that the work take place in a coordinated and controlled manner, in the interests of both security and stability.

In 2014, the industry established a joint account and address register[51] that will increase the security and quality of Norwegian payment services and provide a basis for simpler new services. It involves establishing links between telephone number, owner and account number, which are used in immediate payment systems[52] on mobile devices[53].

5.7 Virtual currencies

Virtual currencies, or cryptocurrencies, are still in focus. In 2014 there were more than 550 different virtual currencies.

Virtual currencies are neither issued nor guaranteed by any government body, nor are they subject to oversight. Users therefore have no legal protection other than general legislation.

In December 2013, the EBA warned consumers against the possible risk of buying, effecting transactions with or holding virtual currencies.[54] The EBA monitored the risk associated with

[51] https://www.fno.no/verktoy/avtaler-og-regelverk/bank-og-betalingsformidling/betalingssystemer-og-felles-bankinfrastruktur-/Betalingstjenester-og-fellesfunksjoner/
[52] http://www.dinside.no/931446/endelig-kommer-straksbetalinger-i-nettbanken
[53] https://sn.no/om-oss/infoartikler/ny-mobilbank
[54] http://www.finanstilsynet.no/no/Artikkelarkiv/Aktuelt/2013/4_kvartal/Advarsel-til-forbrukere---informasjon-om-virtuelle-valutaer/

virtual currencies in 2014 and, with input from Finanstilsynet, compiled a report[55] on whether virtual currencies can and should be regulated.

The conclusion of the EBA report was:

- The apparent risks far exceed the apparent benefits, particularly in a European context.
- More than 70 risk areas were identified, and their underlying drivers were assessed.
- Addressing all these risks would require an extensive regulatory regime of a strongly global nature, which would be time-consuming to develop.
- An appropriate short-term measure would be for national supervisory authorities to advise financial institutions, payment service providers and e-money institutions against buying, holding or selling virtual currencies.
- A proposal that exchange sites or the like for virtual currencies be included in the revision of the Anti-Money Laundering Directive (AMLD4).

In the wake of the publication of the report, the governments of several countries have issued warnings and advised the financial services industry against involvement in virtual currencies. Banks in some places have also terminated accounts with Bitcoin companies.

In the USA, which is one of the countries with a liberal attitude to virtual currencies, the New York State Department of Financial Services (NYDFS) has published its revision of proposed cryptocurrency regulation[56]. The proposal contains requirements for registration, compliance with laws, rules and regulations, capital, storage and protection of customer assets, supervision, anti-money laundering measures, a cyber security programme and measures, business continuity and contingency systems and consumer protection.

FATF has followed up the risk associated with money laundering and terrorist financing associated with the use of virtual currencies. FATF is busy preparing guidelines for a risk-based approach that involves applying existing recommendations also to virtual currencies. This may imply, for example, that companies that engage in currency exchange and the like must be licensed/registered, perform customer controls (“know your customer”) and comply with requirements regarding information about the sender and the recipient of transfers.

5.8 Cash and electronic systems

The incentives and practical reasons for making Norway a cash-free society are many. Cash processing is costly, and cash-distribution logistics are demanding[57]. If electronic systems are to entirely replace cash, they must meet the needs currently filled by cash, such as that cash is the only means of payment you can demand to be allowed to use for making a payment. One of the main requirements to be met before electronic money can be equated with cash, is availability to consumers. Emergency solutions for electronic services must be of a quality that ensures consumers of the same access to making electronic payments as to making cash

[55] http://www.eba.europa.eu/-/eba-proposes-potential-regulatory-regime-for-virtual-currencies-but-also-advises-that-financial-institutions-should-not-buy-hold-or-sell-them-whilst-n

[56] http://insidebitcoins.com/news/nydfs-releases-revised-bitlicense-proposal/29578
http://www.dfs.ny.gov/legal/regulations/revised_vc_regulation.pdf

[57] http://www.hrrnett.no/kontantfritt-norge-i-2020/
http://www.nhoreiseliv.no/2013/08/09/ny-rapport-om-kontantfritt-reiseliv/

payments.

The Standing Committee on Finance and Economic Affairs' recommendation for a new Act relating to Financial Undertakings[58] contains a proposal for a new rule on banks' responsibility for cash services. It is proposed that it be made obligatory for banks, in line with customers' expectations and needs, to receive cash from customers, and to enable customers to make cash deposits.

[58] https://www.stortinget.no/globalassets/pdf/innstillinger/stortinget/2014-2015/inns-201415-165.pdf

6 Risk areas

6.1 Overview

Finanstilsynet has analysed threats, vulnerabilities and controls that are discussed in this RAV analysis. Table 11 below summarises Finanstilsynet's appraisal of the risk associated with the individual control area or security goal.

The topics reviewed and forming the basis for the summary are listed as keywords in column 2 of the table below. The topics are "neutral"; in other words, "Access controls" is a vulnerability if the access controls are deficient. Conversely, good access control will be a strength for the security goal. Note too that the topic may be relevant for several security goals, even if it is not listed for all security goals in the table. The topics listed for a security goal are not exhaustive for the security goal, but are those mentioned most in this report on the basis of findings and observations.

The security goals in the table are not listed in order of priority.

Column 3 provides Finanstilsynet's assessment of the risk of the security goal in column 1 not being attained. Column 4 indicates whether the risk appears to be increasing, stable or decreasing.

The security measures applied vary from one institution to the next. Finanstilsynet is aware that, on closer examination, some institutions may have concluded that the costs associated with further protection are too high in relation to the security that is achieved, and that the institution chooses to accept the vulnerability and the risk it entails.

Table 11

Security goals	**Topic assessed Vulnerability /controls**	**Risk: H(igh) M(edium) L(ow)**	**Trend**
Integrity Information and information systems are correct, valid and complete.	Data quality Data models Change protection (hash) Double storage Structured vs unstructured data Access controls	H	↗
Confidentiality Information and information systems are accessible only to those who are supposed to have access.	Authorisation Identity checks Internal guidelines Encryption (quality) Logging	M	→

Security goals	Topic assessed Vulnerability /controls	Risk: H(igh) M(edium) L(ow)	Trend
	Logical/physical access Key management Signing Social media ID theft: action		
Availability Information and information systems are available within the availability requirements that are specified.	Dependence on the internet Events – exercise and testing Changing suppliers Changing software and data Moving operations Complex operating environment Hardware defects Network defects Surveillance Redundancy Sabotage Security back-ups Protection of national, central infrastructure Denial of service attacks Incident trends Maintenance, housekeeping and deletion	M	↗
Decision-making support: “IT functions satisfactorily as support for strategic decisions, customer management, business processing and reporting”.	Deviation analysis Integration of data components in different systems Integration between systems Impact analysis Segment analysis Early warning Total customer picture “What if” analyses	M	→

Source: Finanstilsynet

6.2 National financial stability

If payments and some other financial services are unavailable, after a short time 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. Lack of overview of financial positions may then threaten financial stability. In such situations, the nation is vulnerable to external influence.

Institutions of significance to the financial sector were under attack in 2014. The effect of the attacks was mitigated by countermeasures taken by the institutions.

Experience gained from 2014 shows that one attacker alone, even with limited resources, can do a great deal of damage. There are also groups of potential attackers who have access to very extensive resources. Attacks causing major, lasting damage can threaten financial stability.

6.3 Financial institutions

As in previous years, changes in systems and environments appear to be the most frequent cause of error or risk driver. Financial institutions must continue to focus special attention on this area. Many institutions have a complex operating environment while they are in the process of changing service providers. This means an additional risk which must be taken into account in insourcing and outsourcing projects. Interoperability procedures must be adapted and tested.

In 2014 there were situations where disaster recovery systems were implemented or where implementation was planned. These revealed that unexpected and undesirable situations associated with the systems still occur. Continued high priority must be given to this important area.

Social manipulation, targeted attacks and Big Data threaten confidentiality and the integrity of systems, and emphasis must be placed on these aspects in the future.

Incidents indicate that not all institutions have sufficient control of their operations. Situations arise in which datasets are not closed, with the result that batch updates do not take place. A process that locks a database and stops further processing, or inadequate recovery points, causes double updates. The risk increases further because some institutions appear to have fallen behind with their housekeeping. In other words, they have not regularly removed functions from the operating environment that are no longer used, or have failed to combine functions where this is advisable.

6.4 Consumers

During the execution of a payment, consumers must carry out controls that are essential for security. Banks normally urge customers to ensure that there is a lock icon on the website. The lock indicates that an encrypted connection has been established between the customer and the website, and that a certificate has been used to establish it. This is not sufficient. In

order for the control to be effective, the customer must check that the certificate has been issued to the site she wishes to use.

This is an example of it being challenging for users to understand the security mechanisms and risk associated with digital systems. It is difficult for users to be sufficiently alert.

From time to time, disagreements arise between the consumer and the bank as to the causes of and responsibilities associated with transactions recorded on the customer's account which the consumer does not recognize. Substantial resources in the form of investigations and legal assistance may be required to clarify the situation. The individual consumer is often not qualified to talk about technical aspects associated with the handling of transactions in the bank's services, and consumers have less resources than banks for calling on technical and legal assistance. This can result in causes not being adequately clarified.

Banks use the postal service for physical distribution. In some cases, banks require that the postal service, or its subcontractors, take copies of the user's passport. The reason for this is the bank's wish to document that the package has been delivered to the right person. Thus the user of the bank is required to leave a copy of an important and personal ID document (passport), which may be misused.

Users whose identity is stolen may be subject to purchases and orders being made in their name. When large purchases are made, merchants will carry out a credit check.[59] Consumers who want to reduce the consequences of ID theft are urged to block credit checks. Blocking is effected by the consumer supplying a copy of his or her passport to every credit information institution, along with instructions that credit checks must not take place. The consumer has thereby again left a number of copies of an important, personal ID document (passport), which may be misused. The consumer wishes to reduce the probability of suffering the consequences of ID theft. However, the result may be that the customer increases the risk of being subjected to ID theft.

Consumers are not qualified to assess threats and vulnerabilities in financial services. In practice, they have to follow the industry's advice, and assume that the institutions have built adequate security into their systems. It is therefore important that the industry provides the users with good and full information about the risk and consequences of ID theft. The advice given by the industry must take proper account of consumers' interests.

[59] https://idtyveri.info/min-id-er-misbrukt/

7 Monitoring by Finanstilsynet

7.1 IT-inspections risk and other contact with institutions

Monitoring of institutions' IT risk primarily takes the form of supervisory inspections. In 2015, Finanstilsynet will be focusing on the supervisory units and service providers that have the greatest influence on financial stability and well-functioning markets.

Particular attention will be paid to outsourcing of key ICT systems in the banking sector. Financial institutions that make major changes in their IT operations, including outsourcing, increase operational risk.

Finanstilsynet will continue its monitoring of contingency preparedness and disaster-recovery systems, risk assessments, implementation of measures associated with legacy core systems and operating stability and structural changes in the supervisory units' service providers.

Attention will also be focused on the institutions' management and follow-up of access control.

On the basis of risk assessments, both general IT monitoring and IT monitoring focused on particular topics will take place. The most important basis for monitoring is verification of compliance with the ICT Regulations and use of various supervisory modules (self-evaluation forms) based on best practice. The most common self-evaluation forms are available on Finanstilsynet's website.

7.2 Work with payment systems

Verification of compliance with laws and regulations is an important responsibility, while development of the regulatory framework is essential in such a dynamic area. Finanstilsynet is working on draft amendments to the ICT Regulations. Amended rules and regulations will be followed up and incorporated in the supervisory system as relevant.

When major changes are made in payment systems, either through the development of new systems or by outsourcing, Finanstilsynet will attach importance to such changes since they may entail greater operational risk.

7.3 Follow-up of incidents

The number of serious incidents increased in 2014. There are ongoing, major changes in some institutions, which increases the risk of faults and failures. In 2015, Finanstilsynet will closely monitor the trend in serious incidents, and place emphasis on finding the root cause and taking steps to prevent recurrences.

7.4 Contingency preparedness

The BFI will continue its work, which includes monitoring the stability of the payment infrastructure, reviewing incident scenarios and assessing whether responsibilities in crisis situations are sufficiently clearly defined. Two exercises are scheduled.

7.5 Further development of supervisory tools

International best practice such as COBIT, ITIL and ISO form the basis for the self-evaluation methods used by Finanstilsynet in its supervision of IT and payment systems. These provide a basis for resource-effective oversight. It is essential that supervisory tools are up to date with best practice.

In the work of developing supervisory tools and methods, Finanstilsynet cooperates closely with the supervisory bodies of other countries and the EU, including the EBA's IT Oversight Department.

7.6 Follow-up of the threat picture associated with digital crime

Finanstilsynet will continue its close follow-up of developments in cybercrime and focus particular attention on institutions' contingency measures against the growing threat picture and their management of incidents.

8 Glossary

Term/abbreviation	Meaning
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.
Advanced Persistent Threat (APT)	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.
AML	Anti-Money Laundering
APEC	Asia-Pacific Economic Cooperation
ASEAN	Association of Southeast Asian Nations
BASH	Standard command processor on many GNU/Linux systems (freeware)
BFI	The Financial Infrastructure Crisis Preparedness Committee to coordinate action in the event of financial sector crises. Chaired by Finanstilsynet.
Big Data	The concept is not well defined, and is used with slightly varying meanings by different operators and in different contexts. It implies large quantities of data collected from both internal and external sources, in both structured and unstructured form. It requires substantial storage capacity and high processing power in order to extract information of value. The expectation is that this should enable informed decisions to be made rapidly in difficult cases.
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.
Business intelligence	Methods and technologies for converting raw data into useful and meaningful information about the business. Popularly defined as user-friendly interpretation/presentation of large quantities of data.
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 trading.
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.
EBA	European Banking Authority
EIOPA	European Insurance and Occupational Pensions Authority.
Executable	Of software that can be run on a computer
EMV	Europay, Mastercard and Visa
ENISA	European Union Agency for Network and Information Security
ESMA	European Securities and Markets Authority
FATCA	Foreign Account Tax Compliance Act
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.
Forking	Trapping money in ATMs so that it cannot be released, nor can it be withdrawn by the ATM. When the customer has gone, the money is picked up by the fraudster.
Whitelist	Register of approved/accepted addresses, such as certificates and e-mail addresses.
Internet of Things (IoT)	At present a somewhat undefined concept. The general principle is that various technological items can be connected to the internet in many different ways, for example for identification purposes, or in a more sophisticated way via a WiFi network. Many devices have built-in computers and can communicate with other devices and service centres. The deployment of sensors for acquiring data is also included in

	the concept. The technology makes it possible to have services performed from anywhere, by anyone, by means of any compatible device.
Information Systems Audit and Control Association	An independent, non-profit organisation. Works on developing and promoting the use of globally accepted and 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.
Jailbreaking	For iPhone: changes a telephone's security settings, for example by allowing the use of an operator other than the one to which the telephone is locked (if it is locked to an operator). The service provider does not support such changes, and security holes may ensue.
JCL	Job Control Language. Name of scripting language used by IBM mainframe operating systems to instruct the system how to run a batch job or start a subsystem.
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
Miscalibration	Often used about judging information on the basis of the wrong starting point/premises, so that incorrect conclusions are drawn.
Multisourcing	Distribution of deliveries among a number of service providers, but in this context such that different products are procured from different service providers.
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 (hold the card or mobile phone near the payment terminal).
NTP	Network Time Protocol. Used to synchronise the clocks in networked computers.
Offshoring	Procuring services from outside the country.
Outsourcing	Procuring services from outside one's own institution.
Overconfident	Self-assured because of a large quantity of information. May overlook vital factors that are not included in the information

	base.
Overlay services	Third-party services in the customer-bank interface.
Passporting guidelines	A payment service provider or e-money provider in an EEA country can freely establish themselves in another EEA country provided that neither the home country's nor the host country's authorities have major 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.
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.
PSD2	New payment services directive from the EU (so far at draft stage).
Ransomware	A type of malware that restricts access to ICT systems that are infected, and demands a ransom.
Rooting	For Android: Like 'jailbreaking' for Apple/iPhone. See 'jailbreaking'.
SSM	Single Supervision Mechanism. The ECB's oversight of systemically important banks.
SSL	Secure Sockets Layer. An old encryption method, now replaced by TLS.
Strong authentication	Authentication employing several methods, e.g. pin code + password.
Sandbox	A virtual container (protected area) where it is possible to run a program without it affecting other programs.
SecuRe Pay	European Forum on the Security of Retail Payments
Strong authentication	Three methods are involved in authentication: something one knows, something one is, and something one has. For example, password, fingerprint and access card. In two-factor authentication, also called strong authentication, two of these methods are used in combination.
TLS	Transport Layer Security. A protocol that is used to encrypt messages and deliver them safely and prevent eavesdropping and "counterfeiting" between e-mail servers.
Token/Tokenization	A token is a sequence of characters and functions as an alias.

TPP / Third Party Providers	Concept 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.

FINANSTILSYNET
P.O. BOX 1187 Sentrum
NO-0107 Oslo
POST@FINANSTILSYNET.NO
WWW.FINANSTILSYNET.NO