NORGES BANK

# 2018

# FINANCIAL INFRASTRUCTURE REPORT

Norges Bank

Oslo 2018

Address: Bankplassen 2
Postal address: P.O. Box 1179 Sentrum, N-0107 Oslo
Phone: 22 31 60 00
Fax: 22 41 31 05
E-mail: central.bank@norges-bank.no
Website: http://www.norges-bank.no

Editor: Øystein Olsen
Design: Brandlab
Layout and print: 07 Media AS
The text is set in 9.5 pt Azo Sans Light

ISSN 1894-8634 (online)

# Contents


EXECUTIVE BOARD'S ASSESSMENT 2

THE FINANCIAL INFRASTRUCTURE IN BRIEF 3

NORGES BANK'S RESPONSIBILITY 3

1. VULNERABILITIES 4
- 1.1 Cyber security 4
- 1.2 Outsourcing and critical ICT service providers 7
- 1.3 Provision of cash services 9

2 DEVELOPMENTS 12
- 2.1 Changing payment landscape 12
- 2.2 Crypto-assets and distributed ledger technology 14
  - Special feature: Central bank digital currencies 18

3 SUPERVISION AND OVERSIGHT 20
- 3.1 Norges Bank's supervisory and oversight work 20
  - Special feature: Assessment of Norwegian FMIs against international principles 22
- 3.2 Interbank systems 24
  - Special feature: Survey of turnover in Norges Bank's settlement system 26
- 3.3 Securities settlement 32

REFERENCES 38

ANNEX 42

# Executive Board's assessment

The *Financial Infrastructure Report* is part of Norges Bank's work to promote financial stability and an efficient payment system in Norway. The Executive Board discussed the content of the Report on 2 May 2018.

Society depends on the functions performed by the payment system and other parts of the financial infrastructure. They enable private individuals and firms to pay for goods and services and banks to provide financing, while redistributing risk. A secure and efficient financial infrastructure is essential for financial stability. Norges Bank monitors the operations of interbank systems and securities settlement systems through its supervisory and oversight responsibilities. In the Executive Board's assessment, the financial infrastructure is secure and efficient. Nevertheless, a number of vulnerabilities stand out.

The payment system's centralised structure and dependence on ICT make it vulnerable to cyber attacks. An effective defence requires specialised knowledge and coordination. Norges Bank ensures that the interbank systems it supervises have satisfactory defences in place. An important element of this work is to follow up financial market infrastructure (FMI) owners' efforts to monitor and manage the cyber security arrangements of their ICT service providers. The Government intends to establish a common arena for public sector bodies with supervisory responsibility for cyber security. The aim is the exchange of information and knowledge transfer in order to increase the quality of ICT security supervision and thereby improve ICT security. This initiative will also contribute to better utilisation of scarce ICT resources.

A disruption among critical ICT service providers may put important components of the payment system – and other key societal functions – out of action. Such concentration risk can be difficult to manage by individual FMI owners. It is the Executive Board's view that it should be studied how critical ICT service providers to the payment system can best be supervised, including whether such supervision should be coordinated among relevant regulatory authorities.

Effective electronic contingency arrangements are crucial for ensuring that the payment system can be restored quickly after a disruption. Nevertheless, cash is a part of overall contingency preparedness in the event of a disruption in electronic contingency arrangements. On the basis of a proposal from Finanstilsynet (Financial Supervisory Authority of Norway) and Norges Bank, on 17 April 2018, the Ministry of Finance issued a regulation that clarifies banks' obligations to provide cash as a back-up.

Cash remains an important means of payment in normal situations. The provision of cash services is for the most part satisfactory, but vulnerable. Norges Bank is of the opinion that there is a need to clarify banks' statutory obligation to provide cash services also in normal situations.

On the initiative of Finance Norway and Norges Bank, a solution for settling real-time payments without credit risk for banks is being developed. In February 2018, seven Nordic banks announced their intention to explore the possibility of a common Nordic infrastructure, initially for real-time payments. Its aims include reducing payment costs and enhancing the cross-border payment system in the Nordic region. This initiative raises questions related to the possible participation in a foreign interbank system and the establishment of critical infrastructure abroad that need to be clarified. The Executive Board assumes that the launch of an improved solution for settling real-time payments in Norway will not be substantially later than originally planned.

Common solutions and standards and the early adoption of new technology have enhanced the efficiency of the financial infrastructure in Norway. New providers of banking and payment services can further improve efficiency. However, providers should continue to compete within the framework of a common infrastructure. Mobile payment services, for example, rely on an infrastructure of alias registers that link account numbers with phone numbers. A single alias register for all payment service providers will enhance register quality, while ensuring a level playing field and promoting a more efficient payment system.

# The financial infrastructure in brief

The financial infrastructure can be defined as a network of systems that enable users to perform financial transactions. These systems, called financial market infrastructures (FMIs) include the payment system, the securities settlement system, central counterparties (CCPs), central securities depositories (CSDs) and trade repositories.

The infrastructure must ensure that cash payments and transactions in financial instruments are recorded, cleared and settled. An efficient financial infrastructure is an essential part of a modern economy. Virtually all financial transactions require the use of the financial infrastructure. Thus, the financial infrastructure plays a key role in ensuring financial stability.

The costs to society of a disruption in the financial infrastructure may be considerably higher than the FMI's private costs. The financial infrastructure is therefore subject to regulation.

# Norges Bank's responsibility

Under Section 1 of the Norges Bank Act, Norges Bank shall "promote an efficient payment system domestically as well as vis-à-vis other countries." The payment system comprises any means, systems or instruments that can be used to execute or facilitate payment transactions. An efficient payment system carries out payment transactions swiftly, safely, at low cost and tailored to users' needs.

Norges Bank licenses and supervises interbank clearing and settlement systems. Supervisory responsibility is set out in Chapter 2 of the Payment Systems Act. Norges Bank's oversight activities are based on Section 1 of the Norges Bank Act and international principles.

Norges Bank exercises its authority in this area by:

- monitoring developments in the financial infrastructure and inducing change that can improve its efficiency;
- overseeing and supervising individual participants;
- providing secure and efficient settlement of interbank payments in banks' accounts with Norges Bank; and
- issuing banknotes and coins and ensuring their efficient functioning as a means of payment.

In the *Financial Infrastructure Report*, Norges Bank provides an account of the Bank's supervisory and oversight work since the previous *Report* and expresses where the Bank believes there is a requirement for change. The *Report* also contains a description of the vulnerabilities and current developments in the financial infrastructure.

# 1. Vulnerabilities

## 1.1 CYBER SECURITY

*The payment system's centralised structure and reliance on ICT make it vulnerable to cyber attacks. A successful attack on financial infrastructure may prevent customers from completing payments and result in heavy financial losses. A successful attack may also result in unauthorised access to or manipulation of sensitive information. The number of cyber attacks is increasing and methods are constantly changing. Attacks have an impact across countries, sectors and activities. An effective defence requires coordination and systematic efforts by both the authorities and private owners of financial market infrastructures (FMIs). The Government's work to draw up a new national cyber security strategy is an important measure in this regard.*

### Changes in banking and payment systems

Changes in banking and payment systems broaden the attack surface for cyber attacks. The revised Payment Services Directive (PSD2)[1] requires banks to open their systems to enable third-party providers (TPPs) to offer payment and account information services. This means that more operators can process personal data, account information and transaction data. Finanstilsynet (Financial Supervisory Authority of Norway) is the licensing and supervisory authority for TPPs under PSD2 and sets cyber security requirements for banks and TPPs. In line with the accountability principle, operators must themselves assess whether data and systems are adequately secured and must implement necessary measures.

Several large technology companies have also become payment service providers, some of which may become major global payment service providers due to network effects[2]. They are able to draw on large quantities of data, which may be of considerable financial value. The concentration of information can make these companies attractive targets for cyber attacks as a successful attack against them could have international repercussions.

Additional agents in the payments market increase the spread of payment information. Large international agents will be able to store substantial payment information and other information about their customers that could fall into the wrong hands and be misused. Vulnerabilities related to payment information, processing and storage could affect confidence in the payment system and financial stability.

### New technology

Artificial intelligence and quantum computers are examples of new technology that can also be used in cyber attacks.

1 The revised Payment Services Directive (PSD2) was introduced in the EU in January 2018. PSD2 has not been incorporated into the EEA Agreement.

2 See also box on digital platforms and network effects in Section 2.1.

### CYBER SECURITY

Cyber security involves ensuring that financial market infrastructures (FMIs) are available and protected against unauthorised access and that the information stored in their computer systems is reliable. That is, FMIs fulfil three important information security objectives[1]:

- **Availability:** Ensuring that a service meets certain stability requirements, so that the service and relevant information can be accessed when needed.
- **Confidentiality:** Ensuring that specified information is protected from access by unauthorised persons, and that only authorised persons have access to the information.
- **Integrity:** Ensuring that the information and information processing are complete, accurate, validated (not corrupted) and the result of authorised and monitored activities.

1 Norwegian Ministries (2012).

## VARIOUS FORMS OF CYBER ATTACK[1]

Attacks on the financial infrastructure can compromise the availability of FMIs. Attacks can also affect the confidentiality and integrity of information through the unauthorised retrieval of information and/or unauthorised payment transactions. Attacks can be of various types.

**DDoS (Distributed denial of service)**
DDoS is an internet attack that overloads a server with so much traffic that normal access for ordinary users is hampered. The intention is to compromise the availability of affected systems.

**Phishing and social engineering**
People are often the weakest link in cyber defence. Phishing is when criminals purport to be someone else in order to obtain sensitive information. Criminals increasingly use phishing and social engineering techniques to penetrate financial institutions' computer systems to retrieve sensitive information and to manipulate payment orders.

**Watering hole attacks**
A watering hole attack is a computer attack strategy in which a virus is planted on websites that are likely to be visited by financial sector employees (a watering hole). The virus infects computer systems at employees' workplaces, giving criminals access. The intention may be to only obtain information or to obtain information necessary for carrying out unauthorised transactions. In February 2017, 20 banks in Poland were infected with malware that had been distributed via the Polish Financial Supervision Authority's web server.

1 This box is based on the content of Finanstilsynet (2017a).

By using artificial intelligence, attackers can analyse and use large quantities of data for more targeted attacks. It is important that cyber security measures are similarly advanced to protect the payment system from the threats posed by artificial intelligence. Cryptography is a technique for securing data integrity and confidentiality. Encryption techniques are vital for cyber security and are essential for secure electronic communication, including between financial infrastructure participants. Quantum computers are based on different principles from those used in traditional digital technology. Such computers are in the development stage and will challenge current encryption mechanisms. If criminals gain access to quantum computers, they will be able to decrypt stolen encrypted data. The Norwegian National Security Authority (NSM) has initiated work to further develop encryption technology for national classified systems to make them resistant to quantum computers.[3]

3 NSM (2017)

### Common defence

Cyber attacks have an impact across countries, sectors and activities. Coordination and information sharing are essential to achieving an effective defence and reducing the risk of cyber attacks. In this area, the interests of the authorities and the financial sector coincide. At a national and sectoral level, collaborative bodies have been established, in addition to a joint cyber coordination centre. Nordic Financial CERT is a private coordinating body for the financial sector that coordinates cyber security and incident management. The authorities are working on a number of initiatives for further coordination (see box on cyber security and regulation on page 6).

### Supervision

Supervision by regulators is important for ensuring that market participants comply with cyber security requirements. Norges Bank's supervisory and oversight responsibilities related to cyber security are based on global standards and are discussed in more detail in Section 3. The Nordic central banks have established an annual cyber security conference to increase the level of expertise in this field. The confer-

## CYBER SECURITY AND REGULATION

The Ministry of Defence and the Ministry of Justice and Public Security are responsible for national military and civilian cyber security, respectively. The Norwegian National Security Authority (NSM) has a primary and cross-sectoral responsibility on behalf of the two ministries. The NSM is Norway's expert body for information and object security and is the national specialist centre for cyber security.

**CPMI-IOSCO**
Together with the International Organization of Securities Commissions (IOSCO), the Committee on Payments and Market Infrastructures (CPMI) has issued a supplementary guidance on cyber resilience for financial market infrastructures (FMIs) (CPMI-IOSCO 2016). Norges Bank's supervision and oversight of cyber security is based on these principles (see Section 3).

**Directive on security of network and information systems (NIS Directive)**
Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 (NIS Directive) defines measures for a high common level of security of network and information systems across the EU. The Directive requires member states to ensure that operators of essential services, including banks and FMIs, implement security measures and report incidents. The Directive also sets requirements for the exchange of information. The Ministry of Justice and Public Security is working on the implementation of the NIS Directive in Norway.

**White paper on cyber security and a new national ICT security strategy**
In June 2017, a white paper (Meld. St. 38 (2016–2017)) on ICT security was presented to the Storting. This is the first white paper on ICT security. The title: *Cyber Security: A joint responsibility* refers to the inability of either the authorities or private entities to address their digital vulnerabilities on their own.

As a follow-up to the white paper, the Government is preparing a new national ICT security strategy, which is scheduled to be finalised in autumn 2018. The Ministry of Justice and Public Security and the Ministry of Defence are leading the strategy process and seek the broad involvement of both public and private stakeholders. Norges Bank has provided input to the new national ICT security strategy. Key recommendations include performing assessments of whether the regulation of critical ICT service providers is sufficient and whether effective contingency arrangements should be required in Norway when ICT operations are offshored.[1] The Government has established a forum for public-private cooperation where strategic issues related to digital vulnerabilities and ICT security are discussed by the authorities and private stakeholders. The first meeting was held in January 2018.[2]

**ICT security commission**
In September 2017, the Government established a commission to report on regulatory requirements in the area of ICT security and the organisation of cross-sectoral responsibility. The commission is tasked with assessing whether current regulations are satisfactory and whether they address the new societal challenges posed by digital technology. The commission is also tasked with proposing specific legal and organisational changes in the area of ICT security. The commission is to present its report by 1 December 2018.

**New Act on national security**
The Storting passed a new Act on national security in February 2018. The new Act clarifies responsibilities for preventive security. Each ministry will be responsible for its own sector. At the same time, the NSM's overall responsibility is to be strengthened. Furthermore, the new Act facilitates increased interaction among public bodies and more cooperation between public and private participants to promote more effective and comprehensive preventive security work.

1 Norges Bank (2018a).
2 Solberg (2018).

ence was held for the first time in autumn 2017. In addition, central banks in the Nordic countries share lines of communication at the operational level. Finanstilsynet monitors financial institutions' cyber security through its ICT supervision.

In the face of technological advances, supervisory authorities also need to improve their cyber security skills. The Ministry of Justice and Public Security and the Ministry of Defence have been tasked with studying and establishing a common arena for authorities with supervisory responsibility for cyber security.[4] In addition, the NSM is to consider the establishment of a central body with expertise in ICT security to be used as a resource for supervisory authorities.[5] The aim is to improve exchange of information and knowledge transfer in order to increase the quality of ICT security supervision and thereby ICT security. This initiative will also contribute to better utilisation of scarce ICT resources

### SURVEY OF OUTSOURCING IN THE PAYMENT SYSTEM

The overall risk from outsourcing in the payment system may be high even though the risks related to individual participants and outsourcing arrangements are acceptable. In spring 2018, a working group comprising representatives from Finanstilsynet and Norges Bank will survey the use of outsourcing in the banking and payment system. The survey will provide a basis for the determination of whether outsourcing weakens companies' management and control of operations, and whether outsourcing in general, and offshoring in particular, will complicate the authorities' ability to manage and control enterprises in a contingency. The survey will also provide a clearer overview of key ICT service providers and concentration risk.

## 1.2 OUTSOURCING AND CRITICAL ICT SERVICE PROVIDERS

*ICT service providers have contributed to the development of efficient payment system solutions. However, the dependence of the payment system on ICT providers has led to vulnerabilities. The fact that a large number of payment system participants have outsourced their ICT operations to the same service provider entails potential concentration risk. The failure of a critical ICT service provider can have an impact on important parts of the payment system. It should be studied how critical ICT service providers can best be supervised, including whether such supervision should be coordinated among relevant regulatory authorities.*

#### Management and control

Outsourcing involves transferring the performance of tasks to an external contractor rather than performing them internally. In the payment system, ICT development and operations are largely outsourced. FMI owners are responsible for outsourced tasks and are required to have sufficient resources and qualified personnel in-house to manage and monitor the performance of their service providers and any subcontractors effectively.[6]

Extensive outsourcing of ICT tasks could impair the effective management and control of outsourced operations by FMI owners, which in turn may weaken payment system security. The use of service providers may also make it more challenging to monitor unauthorised access to systems and sensitive information. Extensive offshoring of ICT operations may impair the nation's ability to operate, develop and follow up key ICT operations in the payment system. It could also be more challenging for Norwegian authorities to deal with a contingency if crucial parts of ICT operations are performed from another country. The need for national control of the payment system in a crisis may be an argument for basing parts of ICT operations in Norway. If ICT operations are based abroad, it should be assessed whether it is necessary to have operational contingency arrangements in Norway that can take over operations at short notice.

#### Concentration risk

Professional ICT service providers may have more resources and expertise to develop more resilient solutions than individual FMI owners. A high level of

4 Meld. St. 38 (2016–2017).
5 Meld. St. 38 (2016–2017).
6 See Norges Bank (2016) and Norges Bank (2017a).

fixed costs is associated with ICT, and to realise economies of scale, several participants use the same service provider.

The outsourcing of the operation of ICT systems to a few service providers by a large number of payment system participants entails concentration risk[7]. The failure of key ICT service providers to the payment system, owing to either operational errors or attacks, could bring important parts of the payment system to a halt. The problems at the ICT service provider EVRY on 6 October 2017 affected approximately 40 banks in Norway, as well as Norway Post and Telenor. This incident illustrates the broad repercussions of the failure of a key ICT service provider.

Another trend is for an increasing number of ICT service providers to co-locate hardware at data centres to exploit economies of scale. The possibility that many FMIs can be affected by a disruption at single location represents geographical concentration risk.

### Regulation

ICT service providers are not subject to the same regulation and supervision as licensed banking and payment system participants. This means that Finanstilsynet and Norges Bank cannot impose requirements directly on the ICT service providers used by FMI owners. The requirements must be directed to licensees that are responsible for monitoring that their ICT service providers follow up.

In a report from June 2017, the Financial Stability Board (FSB) notes that managing operational risks posed by service providers is a challenge that should be given international priority.[8] The authorities should

7 Norges Bank (2017a).

8 FSB (2017).

## MANDATE ICT SECURITY COMMISSION

**FOLLOW-UP OF MELD. ST. 38 (2016–2017) ON ICT SECURITY**

**Issue 1:** Is the current regulation appropriate for achieving sound national ICT security?

**Issue 2:** Do we have an adequate allocation and organisation of cross-sectoral responsibility at the level of national ICT security?

**Issue 3:** What regulatory and organisational measures should be taken to strengthen national ICT security?

The commission will deliver its progress report in December 2018.

## THE BANK OF ENGLAND'S REGULATION OF SERVICE PROVIDERS TO SYSTEMICALLY IMPORTANT PAYMENT SYSTEMS

In 2017, UK banking legislation (Banking Act of 2009) was amended to bring service providers to systemically important payment systems within the Bank of England's regulatory remit.[1] HM Treasury designates which payment system service providers are to be subject to such supervision. The responsibility of FMIs for risk management and control in using service providers is not changed because a provider is subject to Bank of England supervision.

The purpose of the amendment is to strengthen the Bank of England's ability to promote financial stability. The amendment empowers the Bank of England to impose requirements on service providers to systemically important payment systems and enforce these requirements. The Bank of England will be able to require data directly from service providers, require that service providers perform risk analyses of external experts and impose board composition requirements on providers. In addition, the Bank of England can impose requirements on planned changes that could affect these service providers' risks, such as new product and service launches, changes in ownership and outsourcing.

1 Bank of England (2018).

determine whether current oversight frameworks for important third-party service providers to financial institutions are appropriate. This applies in particular if more than one financial institution relies on the same provider. The FSB points out that such concentration risk may entail a need for greater coordination among the authorities responsible for ICT security. In 2017, UK banking legislation was amended to bring service providers to systemically important payment systems within the Bank of England's regulatory remit (see box on the Bank of England's regulation of service providers to systematically important payment systems).

It is difficult for individual FMI owners to address concentration risk. It should be studied how critical ICT service providers, data centres and other key public functions can best be supervised. This evaluation must not duplicate the ongoing work of the Security Law Commission.[9] To ensure coherent regulation, joint supervision with the supervisory authorities of other critical infrastructure that relies on the same ICT service providers should be assessed. The Government's initiative to establish a common arena for authorities responsible for supervising cyber security is in line with this aim.[10]

## 1.3 PROVISION OF CASH SERVICES

*While the use of electronic payment methods continues to rise, cash remains important in both normal and contingency situations. Cash is legal tender for consumer transactions and is part of the payment system's contingency arrangements. The provision of cash services is for the most part satisfactory, but vulnerable. There is a clear trend towards fewer outlets for making deposits and withdrawals. In addition, a significant share of cash services is provided by market participants that are not under an obligation to maintain them. There is a need to clarify banks' responsibility to offer cash services in normal situations.*

Currently, the general public's ability to make cash withdrawals is for the most part satisfactory. Access to cash is largely based on ATMs and point-of-sale withdrawals, referred to as "cashback". Cash withdrawals from ATMs and point-of-sale cashback are bank-neutral solutions. This means that customers can withdraw cash from ATMs or at points of sale irrespective of which bank they use. The number of bank branches and ATMs is declining. As a result, point-of-sale cashback represents an increasing share of the total array of cash withdrawal services.

The general public's ability to make cash deposits is not fully satisfactory today; it is largely confined to in-store postal outlets/post office branches and deposit and cash recycling machines. Deposit and cash recycling machines are bank-specific and can only be used by banks' own customers. Under DNB's agreement with Norway Post, DNB customers can deposit cash and perform simple banking transactions at some 1 300 retail outlets and 30 post office branches. Customers of other banks can also make deposits under this arrangement, but only as giro payments, which are subject to both a NOK 100 fee per transaction and a three-to-seven-day waiting period before the deposit is posted. Thus, Norway Post's deposit services appear to be rather inefficient for customers of banks other than DNB.

The private companies Nokas and Loomis own and operate a substantial share of the ATMs and night depositories in Norway. Along with retail outlets that offer point-of-sale cashback, Nokas and Loomis thus play a key role as cash service providers. Retail outlets, Nokas and Loomis are not under any obligation to provide cash services to the public, which they offer of their own accord. They can therefore stop offering cash services if these services cease to be profitable or feasible. This makes cash services vulnerable.

### Regulation

Section 16-14 of the Financial Institutions Act establishes banks' obligation to accept cash from customers and make deposits available to customers in the form of cash. According to the preparatory works of the Act, banks are obliged to offer the public efficient and rational arrangements making deposits and using deposit accounts in accordance with customers' everyday needs.

An important part of the provision of cash services depends on agents that are not obliged to maintain these services. Nevertheless, under Section 16-14, first paragraph, of the Financial Institutions Act, it is clear that banks are obliged to ensure the satisfactory provision of cash services. If a substantial share of cash services is provided by agents that are not under

9 See box on cyber security and regulatory work in section 1.1 for more information.

10 See paragraph on supervision in Section 1.1 on cyber security.

an obligation pursuant to the Act or to a contract with banks, banks must be prepared to step in at short notice to ensure the provision of cash services at a satisfactory level.

Effective electronic contingency arrangements are crucial for ensuring that the payment system can be restored quickly after a disruption. Nevertheless, cash is a part of overall contingency preparedness in the event of a disruption in electronic contingency arrangements.[11] On the basis of a proposal from Finanstilsynet and Norges Bank, on 17 April 2018, the Ministry of Finance issued a regulation that clarifies banks' obligations to provide cash as a back-up.[12]

Norges Bank believes that there is a need to clarify the banks' legal obligation to offer cash services in a normal situation.[13] The distribution of cash in a contingency situation and in a normal situation will be based on the same infrastructure, and thus are interrelated. Norges Bank has written on this subject in a letter of 20 February 2018:

> *In Norges Bank's assessment, banks' legal obligation to provide cash services should be clarified. Such a clarification should be sufficiently detailed and, in the Bank's view, specify a proximity requirement for these services, eg, close to commercial establishments. Furthermore, Norges Bank is of the opinion that increased use of common bank-neutral solutions will likely facilitate compliance with this legal obligation in an economically efficient manner. Examples of such common solutions are bank-neutral deposit and recycling machines, which customers can use regardless of their bank, as is the case with ATMs.*

In the Financial Markets Report in 2018, the Ministry of Finance writes, among other things, that banks have a responsibility to continue to maintain satisfactory levels of national availability of cash (see box on cash availability in normal situations).

11 Norges Bank (2017a).
12 Ministry of Finance (2018b).
13 Norges Bank (2018a).

## CASH AVAILABILITY IN NORMAL SITUATIONS

The Ministry of Finance has requested that Finanstilsynet, in consultation with Norges Bank, investigate how banks are complying with the obligation in Section 16-4 of the Financial Institutions Act to make cash available in normal situations and assess whether tightening the obligation is necessary.[1] Norges Bank presented its assessments of cash services in a letter to Finanstilsynet of 20 February 2018. Finanstilsynet sent a response to the Ministry of Finance on 1 March 2018.

In the Financial Markets Report 2018, published on 27 April, the Minestry of Finance writes:[2]

> *The Government believes that it is of major importance for the general public to have access to bank deposits and payment services in a convenient format. It is reassuring that Finanstilsynet has found that cash services are available throughout the country, but developments may give grounds for concern. Banks have a responsibility for maintaining satisfactory cash services in coming years as well. This responsibility is likely most effectively handled through joint solutions, as pointed out by Finanstilsynet and Norges Bank. If banks fail to deliver on their responsibility, the Ministry of Finance could impose specific obligations on banks in a regulation. However, this may imply unnecessarily high costs compared with well-organised collaboration between banks. The Government will follow up on these issues together with Finanstilsynet and Norges Bank, and in dialogue with the financial industry, and provide the Storting with an updated overview in next year's financial markets report.*

1 Ministry of Finance (2017a).
2 Ministry of Finance (2018a).

## CASH USAGE IN NORWAY AND IN OTHER COUNTRIES

Norges Bank has conducted surveys of Norwegian households' payment habits. The surveys in 2017 and 2018 indicate that cash payments account for 11% of point-of-sale transactions.[1] In similar surveys from 2007 and 2013, cash payments accounted for 24% and 15%, respectively, of the number of point-of-sale transactions.

Even though total cash usage in Norway is declining, usage in certain businesses remains considerable. Figures from the grocery business in Norway show that cash accounts for 20–25% of the number of payments.[2]

In the Scandinavian countries, cash usage is very low compared with other countries. Table 1 shows the results from various national household surveys. In some of the euro area countries, cash payments account for up to 90% of total point-of-sale transactions. As there are some differences in survey methodology, the types of payments included and the time the surveys were conducted, the data are not fully comparable.[3]

**Table 1. Cash usage in selected countries**

| Country | Period | Share of cash in % (number) |
|---|---|---|
| Euro area, total | 2014–2016 | 79 |
| - Greece | 2015–2016 | 88 |
| - Italy | 2015–2016 | 86 |
| - Germany | 2014 | 80 |
| - France | 2015–2016 | 68 |
| - Finland | 2015–2016 | 54 |
| - Netherlands | 2016 | 45 |
| UK | 2016 | 44 |
| US | 2016 | 31 |
| Denmark | 2017 | 23 |
| Sweden | 2018 | 13 |
| Norway | 2017–2018 | 11 |

Sources: Danmarks Nationalbank, ECB, Federal Reserve Bank of San Francisco, Sveriges Riksbank, UK Finance and Norges Bank

1 See Norges Bank (2018c) for more information regarding the surveys.
2 Aera (2018).
3 Norges Bank (2018c).

# 2 Developments

## 2.1 CHANGING PAYMENT LANDSCAPE

*The payment system is undergoing significant changes. Cash usage is declining, while new ways of accessing deposit money are emerging. A solution for settling real-time payments without credit risk for banks is being developed. New agents are emerging to challenge banks' dominant role in the payment system.*

Important driving forces behind payment market developments are new technology, changes in consumer behaviour, globalisation and new regulation. These driving forces influence and amplify one another.

- Cash usage is declining, while new ways of accessing deposit money are emerging. Users expect payment solutions to match other technological developments in society. Smart phones (mobile phones) now have a substantial role in users' everyday lives as a method of communication and for the purchase of goods and services and can now also be used to make payments. Consequently, users expect their money to be available quickly and round-the-clock.

- Payment system agents adapt to technological advances. As a result, the profile of the agent, the competitive landscape and the value chain have changed. Global technology companies are developing payment solutions based on their large customer networks and ownership of technological platforms.[14]

- New regulations for payment services facilitate innovation and competition by regulating access to payment accounts. This opens up the payment market to other agents in addition to banks.

### Mobile payment solutions and instant settlement

The use of mobile phone payment apps is growing. Mobile phones can be used in a range of payment situations, such as payments between private individuals, for online shopping, to pay bills and for point-of-sale payments. New mobile payment services and a change in payment patterns are expected to emerge in the years ahead, partly as a result of regulatory changes.[15]

Work has long been in progress in the financial industry to find payment solutions that align with users' demand for immediate settlement. An instant payments solution providing immediate payment into the recipient's account was established in 2012. The mobile payment solution Vipps now allows the system's users to make instant payments.

However, the instant payments solution cannot be used for all types of payment, and the banks involved in the settlement are exposed to credit risk. Bits AS (the financial industry's infrastructure company) and Norges Bank are therefore working in collaboration to develop a solution for settlement of real-time payments without credit risk for banks, the so-called faster payments initiative, BRO (Betalinger med Raskere Oppgjør). BRO is scheduled to be in place by the end of 2019.[16]

In February 2018, seven Nordic banks announced their intention to explore the potential for a Nordic payment infrastructure, initially for the settlement of real-time payments without credit risk for banks. Its aims include reducing payment costs and enhancing the cross-border payment system in the Nordic region. Work is now in progress to assess whether the BRO project will be affected by this initiative. This matter raises fundamental issues that need to be explored, with regard to both possible participation in a foreign interbank system and the establishment of critical infrastructure abroad. Norges Bank assumes that the launch of an improved solution for settling real-time payments in Norway will not be substantially later than originally planned.

### Changes in market structure

The revised Payment Services Directive (PSD2) requires banks to open their systems to enable third-party providers (TPPs) to offer payment and account information services. PSD2 is both a response to developments in the payments market and a catalyst for further developments.[17] Several large international technology companies, such as Apple, Samsung and Google, are also moving into the payment market and are in a position to provide mobile payment services to Norwegian customers. At present, these companies' payment solutions have only been launched in some of the other Nordic countries.

14 See box on digital platforms and network effects.
15 PSD2.
16 See Norges Bank (2017b) for more information about instant payments and BRO.
17 Norges Bank has submitted its consultative response to the Ministry of Finance and the Ministry of Justice and Public Security on a proposal for rules to incorporate PSD2 into Norwegian law (see Norges Bank (2017b) and Norges Bank (2017c)).

Where there were once several mobile payment solutions to choose from, the market now features only one Norwegian mobile payment solution, Vipps. Towards the end of 2017, a planned merger of the Vipps, BankAxept and BankID systems was announced. One of the purposes of the merger is to bolster their competitive position vis-à-vis global companies. Bank ID is used for signing and identification purposes in a wide range of private and public services. BankAxept, a national debit card system owned by banks, is the most widely used card system in Norway. While the merger may provide economies of scale, it could also create obstacles for other agents aiming to establish a position in the same value chain. The merger is subject to approval by the Norwegian Competition Authority and the Ministry of Finance. The Norwegian Competition Authority approved the merger application on 27 April 2018, and it is currently under consideration by Finanstilsynet (Financial Supervisory Authority of Norway), which is preparing the matter for the Ministry of Finance.

Even though a number of developments will enhance competition, there are also mechanisms that in the longer term can weaken competition. An example is if one or a small number of multinationals become dominant payment service providers at the global level (see box on digital platforms and network effects). Furthermore, companies that control parts of the payment infrastructure may shut out competitors. For instance, only Apple Pay may use near-field communication (NFC) for contactless payments using Apple's mobile phones.

Mobile payments rely on an infrastructure of alias registers, which link account numbers with telephone numbers. A single alias register for all payment service providers will enhance register quality, while ensuring a level playing field and promoting a more efficient payment system.

Common solutions and standards and the early adoption of new technology have enhanced the efficiency of the financial infrastructure in Norway. New providers of banking and payment services can further improve efficiency. However, providers should continue to compete within the framework of a common infrastructure.

## DIGITAL PLATFORMS AND NETWORK EFFECTS[1]

In a traditional business model, value is created sequentially in each link of the value chain, where a company purchases inputs from its suppliers, processes them and then sells the finished goods to customers in the next link. A company with a platform business model creates value by facilitating interaction between producers and consumers.

Platforms themselves are nothing new. Examples of traditional platforms are exchanges or shopping centres, where buyers and sellers meet. But digital platforms are far more scalable. Examples of digital platforms are Google, Facebook and the classified ad portal Finn.no.

Digital platforms usually exhibit strong network effects. A large user base also makes it profitable for third-party providers to develop complementary services. Network effects may help give dominant platforms near-monopolies, weakening competition if these platforms exploit their market power.

Technological advances in recent years, including smart phones and social media, have been important for the popularity of digital platforms. These platforms seek to attain competitive advantages by reducing or eliminating time-consuming tasks and complexity. An example is the Norwegian payment app Vipps, which has simplified payments between private individuals. At the same time, leading platforms attract customers by virtue of their existing large customer bases, and not because they necessarily offer an optimal service. Such lock-in effects may impede competition and prevent better technological solutions from succeeding.

1 Ameln and Songe-Møller (2018).

## 2.2 CRYPTO-ASSETS AND DISTRIBUTED LEDGER TECHNOLOGY

*There are a large and increasing number of crypto-assets, also known as cryptocurrencies. Crypto-assets are associated with financial, legal and operational risk, and domestic and international financial supervisory authorities have advised against investing in such assets. Norges Bank is currently considering whether crypto-assets could pose a risk to financial stability and whether there is a need for regulation. There are potential areas of use for the underlying distributed ledger technology (DLT) in the financial infrastructure.*

### Monetary and payment functions

Crypto-assets and DLT have been the focus of considerable attention in recent years. Many crypto-assets are associated with monetary and payment functions as they constitute separate means of payment and payment systems. For some crypto-assets, the means of payment is merely an instrument to ensure the operation of other DLT-based services. For example, crypto-assets can act as payment for processing automated contracts (called smart contracts).

Crypto-assets developed to fulfil money and payment functions do not, however, have the key characteristics money and a payment system must have to meet the needs of the general public. Money is a medium of exchange, a store of value and a unit of account. The substantial day-to-day volatility of crypto-assets makes them particularly unsuitable as money. On the contrary, the rise and volatility in crypto-asset prices has made them attractive as speculative assets. The fact that crypto-assets are usually not the liability of any party presents fundamental challenges related

### CRYPTO-ASSETS AND DISTRIBUTED-LEDGER TECHNOLOGY (DLT)

Crypto-assets are encrypted digital instruments stored in a decentralised accounting system or "distributed ledger". As encryption keys are used to administer transactions, participants can in principle act anonymously[1]. The information in the distributed ledger is shared by all users and is updated by the users themselves. The system is organised such that the ledger's integrity is ensured without the need for a central operator. This is often referred to as distributed-ledger technology (DLT).

A number of crypto-assets use what is called blockchain technology to ensure the integrity of the distributed ledger. If desired, participants can compete to collect new transactions in the network in blocks and certify that they are valid and consistent with the previous blocks (the blockchain). New units of a crypto-asset can be "mined" when participants who validate blocks solve energy-intensive cryptographic "puzzles". Valid blocks are rewarded with newly issued units of the crypto-asset and/or from transaction fees associated with the relevant block. Block validation is very resource-intensive, while at the same time, gains are lost if a block is not accepted and built upon in subsequent validations. Thus the system creates incentives to update the blockchain with valid transactions[2]. A detailed description of blockchain technology is given in Norges Bank (2014) and Norges Bank (2016).

There are no restrictions on who is able to participate in most crypto-assets, but crypto-assets are emerging with restricted participation (see also box on the use of DLT in the financial infrastructure).

1 However, transaction analysis can be used to uncover information about participants' identities.
2 Less resource-intensive mechanisms have been developed for blockchain validation. Alternative distributed-ledger technologies exist that are not based on blockchains.

to trust and the stability of their value. In an efficient payment system, payments are processed quickly, safely, at low cost and tailored to users' needs. The processing capacity of the crypto-assets in use today is limited. Processing is time-consuming and the systems require considerable involvement by the participants to maintain safety. The technology must undergo further development before it can compete with modern, centralised payment systems designed for the general public.

As they lack the characteristics necessary to function as money and as a payment system for the general public, a number of central banks use the term crypto-assets rather than cryptocurrencies.[18]

18 Carney (2018).

**Financial risk**

With the substantial volatility of prices combined with uncertain valuation, investment in crypto-assets involves considerable financial risk. There is no central bank or other institution backing these assets to guarantee or promote the stability of their value. Investors who purchased crypto-assets while prices were low, have made large profits, but sudden changes can trigger a rapid fall in value, sometimes to zero. Some have also lost their investments as a result of cybercrime and unreliable crypto-asset exchanges. The financial supervisory authorities of many countries, including Norway, have warned against investing in crypto-assets[19].

Many of the new crypto-assets have been put into circulation through what is known as an Initial Coin

19 Finanstilsynet (2013) and Finanstilsynet (2018).

## USE OF DLT IN THE FINANCIAL INFRASTRUCTURE

DLT has a number of potential applications in the financial infrastructure. A common decentralised digital asset register can enhance efficiency as participants no longer need to reconcile their records with one another, which can reduce counterparty risk. Operational risk can also be reduced as this technology does not rely on a central operator. Various potential applications were discussed in Norges Bank (2016). Since then, the range of applications has widened:

- In a press release of 7 December 2017, the Australian exchange ASX announced its intention to replace the existing system for clearing and settling trades with a new DLT-based system.[1] ESMA and ECB have provided a general account of potential applications of DLT in securities markets.[2]
- "Project Stella" is a joint effort of the ECB and the Bank of Japan to explore how a secure delivery versus payment (DvP) system could be organised where the assets are stored on the same distributed ledger (single-ledger DvP) or on separate ledgers (cross-ledger DvP).[3]
- Japanese banks have evaluated the use of DLT for interbank settlement.[4] Some central banks, such as the Bank of Canada, have evaluated and tested DLT for use in central bank settlement[5].

However, the use of DLT for interbank settlement poses a number of challenges, including the immaturity of the technology and how to prevent unauthorised access to confidential information.

Norges Bank is monitoring developments in DLT, and is assessing whether DLT can contribute to the efficiency of payment systems and other FMIs within Norges Bank's remit.

1 ASX (2017).
2 ESMA (2017a) and ECB (2018).
3 ECB (2018).
4 Ripple (2017).
5 See Chapman et al (2017) and Bech and Garrett (2017).

Offering (ICO), where investors can purchase units of a crypto-asset at an early stage. The funds can be used to further develop a crypto-asset, while giving investors the incentive to promote it. Such investments are a source of considerable financial risk. ESMA, the European Securities and Markets Authority[20] and Finanstilsynet have warned about the risk of investing in ICOs. Among other things, they have pointed out the lack of investor protection, and the potential for fraud and money-laundering. A number of countries have taken initiatives to regulate ICOs and clarify to what extent they are subject to securities regulations.

**Legal and operational risk**

The legal framework around crypto-assets has not been fully developed. It is uncertain to what extent investors are protected under the law. There is also risk related to the legal responsibilities of system participants. A participant who contributes to the distribution of transactions in the network can become part of a money-laundering operation. Operational risk arises as many crypto-assets have not been adequately tested for the functions they are intended to fulfil. The development of new technology, such as quantum computers and artificial intelligence, could be exploited in a way that could jeopardise the integrity of the systems.[21]

**Systemic risk**

The FSB concludes that crypto-assets do not currently pose risks to global financial stability.[22] This is in line with the views of a number of central banks.[23] The literature provides examples of a number of ways crypto-assets can threaten financial stability:[24]

- The purchase of debt-financed crypto-assets.
- The holding of large, unsecured crypto-assets by financial institutions.
- The use of crypto-assets as collateral in the settlement of large financial transactions.
- The faltering of confidence in crypto-assets that play a major role in the payment system of securities settlement.

The impact on financial stability could increase if financial derivatives emerge that are based on crypto-assets. Such derivatives seem to be increasingly common internationally.

Norges Bank is currently considering whether crypto-assets could pose a risk to financial stability and whether there is a need for regulation (see section on regulation below). The FSB has recently announced that a methodology is being developed to assess systemic risk related to crypto-assets.[25] Such a methodology will be useful to the work in progress at Norges Bank.

**Regulation of crypto-assets**

Many countries have introduced or are considering introducing regulations governing crypto-asset trading. The purpose of the regulation and the choice of instrument can vary from country to country (see box on regulatory strategies for crypto-assets on page 17).

One of the challenges of regulating crypto-assets is enforcement. Crypto-assets that are open to all participants have no central agent, and the participants are more or less anonymous and spread across borders. Thus, other agents in the value chain, such as crypto-asset exchanges, must be regulated instead. The same applies to traditional financial institutions if these institutions are involved in crypto-assets. For crypto-assets with access-regulated participation, however, there is more scope for regulation as the participants are identifiable and there is a centralised governing structure controlling access to and development of the system.

Crypto-assets are still a relatively new phenomenon. The level of knowledge about how markets function and how regulations should be formulated is low compared with many other aspects of the economy. This increases the risk that regulations might have a detrimental effect and hamper innovation and progress. Priority should be given to regulating areas where regulation is clearly necessary to address the needs of society. Combating crime and consumer protection are examples.

Norges Bank will assess the need for regulation to prevent risks that could threaten financial stability (systemic risk) and payment system efficiency. It is

20 ESMA (2017a) and Finanstilsynet (2017b).
21 See Section 1.1 on cyber security.
22 FSB (2018).
23 See, for example, Carney (2018).
24 See for example Ali et al. (2014), He et al. (2017) and FSB (2018).
25 FSB (2018).

too early to specify the regulations that might be appropriate. As discussed above, crypto-assets will primarily affect financial stability if featured on traditional financial institutions' balance sheets and whether they are used by operators of FMIs. Norges Bank will therefore closely monitor how these institutions are involved in crypto-assets and assess whether such involvement should be regulated.

Crypto-assets and DLT-based services are often involved in cross-border transactions. Cooperation across regulatory authorities is important to ensure a consistent regulatory approach. Several international central bank bodies are discussing the regulation of crypto-assets and DLT.[26] Other authorities are also discussing regulation in their cooperation forums. Finanstilsynet, for example, takes part in ESMA's working groups.

26 See for example CPMI (2015), CPMI (2017) and FSB (2017).

## REGULATORY STRATEGIES FOR CRYPTO-ASSETS[1]

Crypto-assets can be regulated in a number of ways:

**Information/moral suasion**
Information is a lenient form of regulation. Authorities in a number of national jurisdictions, including Norway, have chosen to warn users of the risk of investing in crypto-assets. These warnings may alleviate problems with asymmetric information, but may be less effective for solving other problems, such as the use of crypto-assets for money laundering.

**Interpretation of existing regulations**
Existing regulatory arrangements can often be applied. For example, ICOs are affected by various portions of securities regulations and investors are subject to tax rules. In December 2017, political consensus was reached in the EU to amend the Fourth Anti-Money Laundering Directive to cover trade in crypto-assets. There may often be uncertainty regarding whether existing regulations cover crypto-asset-related services, and in such cases, authorities have a role in clarifying how the regulations should be implemented.

**Regulation of specific entities**
A number of countries have opted to regulate specific types of entity, such as those providing crypto-asset-related services. For example, trading venues, such as crypto-asset exchanges, have been subject to regulation. It is important to maintain consistency with other regulations when introducing specific regulation.

**Prohibition**
A ban on all crypto-assets-based transactions may be viewed as an extreme form of specific regulation. Any such prohibitions must be introduced with caution. Prohibition may simultaneously trigger regulatory evasion and stifle desired innovation and development, also in other kinds of DLT, due to the restrictive nature of prohibition.

**Broader regulation**
A broader approach to regulation may promote consistency in the regulation of crypto-assets across jurisdictions. Similarly, broader regulation of crypto-assets must also be consistent with regulations of other financial services, in order to avoid distortion of competition. A better understanding of the issues may be necessary before taking such an approach. Norges Bank is not aware of any countries that have chosen this approach to regulating crypto-assets.

1 Based on the categories in CPMI (2015).

# Central bank digital currencies[1]

A central bank digital currency (CBDC) is a digital form of central bank money made available to the general public. No central bank in an advanced economy has introduced a CBDC. But a number of central banks, including Norges Bank, are assessing whether introducing a CBDC would be feasible and if so, in what form.

The motivation for considering CBDCs varies across central banks and depends on local conditions. A characteristic peculiar to Norway is low and falling cash usage.

Cash usage is still substantial, and cash will continue to exist into the foreseeable future. However, it is possible that at some point, cash usage will be so low as to marginalise cash as a generally accepted means of payment. It must therefore be considered whether cash has any important properties that are not shared by bank deposits and whether there is a need for other central bank money in addition to cash.

Cash has a number of properties:

- It is a credit risk-free alternative to deposit money. The public can readily convert their deposits into cash, which in itself may sustain confidence in bank deposits. Cash also helps sustain competition among means of payment. Credit risk-free does not mean that cash is free from the risk of theft or other losses or costs associated with obtaining it.
- It is an independent back-up solution if electronic systems fail. Cash is not dependent on technology or a third party at the time of payment.
- It is legal tender that can be used by anyone. This means that a party to a payment may demand settlement in cash, unless the parties have not agreed otherwise. As deposit money can be exchanged for cash (legal tender), it promotes the public's confidence in deposit money.
- The use of cash is not traceable and thus ensures privacy. On the other hand, the lack of traceability makes uncovering certain types of crime more difficult.

For Norges Bank, the question is whether a CBDC is necessary or desirable for ensuring that Norway's payment system is secure and efficient. The following questions are therefore relevant:

- What are the desired properties of the payment system in the future?
- Is there a risk that important properties will be lacking, and confidence in the monetary system is

1 See Norges Bank (2018d) for a broader discussion of CBDCs.

weakened, unless Norges Bank or other authorities take action?

- If yes, is a CBDC the best instrument for ensuring these desired properties?
- Does a CBDC have any undesirable properties?

Norges Bank must also consider whether situations can arise where a CBDC is necessary to reduce the risk that other currencies will supplant the Norwegian krone.

There are two primary models for organising a CBDC system:

- In a **token-based (or value-based) model**, money is stored locally in a payment instrument, typically a payment card or smart phone payment app. Payments take place directly between parties, without the intermediation of a central third party. In this way, a token-based model resembles cash.
- In an **account-based model**, both value storage and payment handing are centralised. The money is held in accounts and is moved from one account to another in the system, just like payments using bank deposits.

Hybrid solutions are also possible that combine elements of both primary models. The use of distributed ledger technology (DLT) has potential, including for contingency purposes. However, DLT technology is immature (see further discussion in Section 2.2).

A CBDC may have an impact on private banks' balance sheets and funding, the structure of the banking sector, financial stability, monetary policy and the central bank's balance sheet and risk. The impact of a CBDC will depend on the specific design and purpose of the CBDC.

A number of factors must be addressed in the design of a CBDC. In the period ahead, Norges Bank will assess:

- the purpose of a CBDC,
- the type of CBDC solution that best serves this purpose,
- the impact of CBDC solutions and
- an economic cost-benefit analysis of a CBDC.

In its work, Norges Bank will be in contact with other central banks, academia and other national and international participants. This is a long-term undertaking, and it is too early to draw any conclusions regarding the introduction of a CBDC.

# 3 Supervision and oversight

## 3.1 NORGES BANK'S SUPERVISORY AND OVERSIGHT WORK [27]

### Supervision

Norges Bank supervises the clearing and settlement systems for transfers of funds between banks (interbank systems). The Bank awards licences and supervises the interbank systems' compliance with the Payment Systems Act and licence terms. Should Norges Bank uncover any non-compliance with the Act or licence terms, it will instruct the operator of the system to rectify the matter. As a last resort, the Bank may revoke its licence.

Norges Bank supervises:
- Norwegian Interbank Clearing System (NICS).
- DNB Bank ASA's (DNB) settlement bank system.

Norges Bank may grant exemptions from the licensing requirement for interbank systems considered to have no significant effect on financial stability. SpareBank 1 SMN's settlement bank system has been granted such an exemption.

### Oversight

Norges Bank oversees financial market infrastructures (FMIs). Norges Bank's oversight is based on Section 1 of the Norges Bank Act and international principles for FMIs[28]. If Norges bank identifies any issues that are reducing the FMI's efficiency, Norges Bank will urge its owners to rectify the deficiencies and, if necessary, raise the issue with the relevant supervisory authority.

Norges Bank oversees:
- Norges Bank's settlement system (NBO)
- SpareBank 1 SMN's settlement bank system
- The central securities depository Verdipapirsentralen's (VPS) register function, in cooperation with Finanstilsynet (Financial Supervisory Authority of Norway)
- The Norwegian securities settlement system (VPO), in cooperation with Finanstilsynet
- The three central counterparties (CCPs) LCH Ltd, EuroCCP N.V. (EuroCCP) and SIX x-clear Ltd (SIX x-clear), which are overseen in cooperation with Finanstilsynet and authorities in other countries
- CLS bank International (CLS). Norges Bank participates in a committee of representatives of relevant central banks that oversee CLS, which is led by the Federal Reserve

### NBO

The Payment Systems Act's provisions on supervising interbank systems do not apply to Norges Bank's settlement system (NBO). The Bank oversees NBO. The oversight and operation of NBO are handled by separate organisational units within the Bank. Following a decision in 2017, it has been clarified that the lines of defence in NBOs risk management do not form part of the oversight presented in this Report. One consequence of this is that Principle 2 (governance), Principle 3 (risk management framework) and some of the key considerations in Principle 17 (operational risk) of the CPMI-IOSCO principles for FMIs are no longer assessed by the unit that oversees NBO.

### Assessments according to international principles

Norges Bank evaluates the FMIs subject to supervision and oversight in accordance with international principles drawn up by the CPMI-IOSCO[29] (see box).

### Cooperation with Finanstilsynet

As Finanstilsynet's supervisory activities and Norges Bank's supervisory and oversight work partly overlap, the Bank liaises with Finanstilsynet. While Norges

27 See discussion of Norges Bank's responsibilities on page 3.
28 CPMI-IOSCO (2012).
29 See box on international authorities and central counterparties (CCPs) on page 36.

### DEFINITIONS IN THE PAYMENT SYSTEMS ACT

**Payment systems** are interbank systems and systems for payment services.

**Interbank systems** are systems for the transfer of funds between banks with common rules for clearing and settlement.

**Systems for payment services** are systems for the transfer of funds between customer accounts in banks or other undertakings authorised to provide payment services.

**Securities settlement systems** are systems based on common rules for clearing, settlement or transfer of financial instruments.

**TABLE 3.1 Financial market infrastructures subject to supervision and oversight**

| System | Instrument | Operator | Supervision/ oversight | Administrative body |
|---|---|---|---|---|
| Norges Bank's settlement system (NBO) | Cash | Norges Bank | Oversight | Norges Bank |
| Norwegian Interbank Clearing System (NICS) | Cash | Bits AS | Supervision and oversight | Norges Bank |
| DNB Bank ASA settlement system | Cash | DNB Bank ASA | Supervision and oversight | Norges Bank |
| SpareBank 1 SMN settlement system | Cash | SpareBank 1 SMN | Oversight | Norges Bank |
| Norwegian securities settlement system (VPO) | Securities Cash | Verdipapirsentralen ASA (VPS) | Supervision and oversight | Supervision of VPS and VPO: Finanstilsynet<br>Oversight of VPO: Norges Bank |
| VPS's central securities depository (CDS) function | Securities | VPS | Supervision and oversight | Supervision of CSD function: Finanstilsynet<br>Oversight of CSD function: Norges Bank |
| SIX x-clear's central counterparty system | Financial instruments | SIX x-clear Ltd. (SIX x-clear) | Supervision and oversight | Supervision of SIX: Swiss financial supervisory authority<br>Oversight: Swiss National Bank, Norges Bank and Finanstilsynet |
| LCH. Clearnet's central counterparty system | Financial instruments | LCH Ltd. (LCH) | Supervision and oversight | Supervision of LCH: Bank of England<br>Oversight of LCH: EMIR College and Global College (including Norges Bank) |
| EuroCCP's central counterparty system | Financial instruments | EuroCCP N.V. (EuroCCP) | Supervision and oversight | Supervision of EuroCCP: Dutch central bank<br>Oversight of EuroCCP: EMIR College (including Norges Bank) |
| CLS | Cash | CLS Bank International (CLS) | Supervision and oversight | Supervision of CLS: Federal Reserve<br>Oversight of CLS: Central banks whose currencies are traded at CLS, including Norges Bank |

Bank is responsible for monitoring interbank systems, Finanstilsynet monitors retail systems for payment services.

Table 3.1 provides an overview of the various FMIs and their appurtenant supervision and oversight bodies.

### Supervision and oversight 2017/2018

In its supervision oversight work over the past year, Norges Bank has attached importance to FMI owners' promotion of cyber security and control of outsourced operations. Norges Bank will continue to pay particular attention to these areas in 2018.

*Cyber security*

The oversight and supervision of cyber security arrangements are based on the supplementary guidance published by CPMI-IOSCO on this subject in 2016. In oversight and supervision meetings, particular weight is given to FMI owners' organisation of work on cyber security, protection against cyber attacks and cyber risk preparedness. Finanstilsynet normally attends these meetings. Together with Finanstilsynet, Norges Bank has also participated in individual ICT inspections.

*Outsourcing*

In spring 2018, a working group comprising representatives from Finanstilsynet and Norges Bank is surveying the use of outsourcing in the banking and payment system. Among the survey's aims is to provide a basis for determining whether outsourcing weakens FMI owners' management and control of operations (see box on the survey of outsourcing in the payment system on page 7).

# Assessment of Norwegian FMIs against international principles

In 2014, the owners of Norwegian FMIs carried out a self-evaluation against the CPMI-IOSCO principles. On the basis of this self-evaluation and other information, Norges Bank assessed the systems the same year. Since 2014, Norges Bank has performed annual reassessments of FMIs against principles not considered "observed". Assessments were also performed in the event of changes to an FMI that might affect the assessment. The main conclusion of the assessments by Norges Bank and Finanstilsynet is that Norwegian FMIs largely comply with the principles.

FMIs are evaluated against the principles that are relevant to them. The degree of compliance is based on the following criteria:

- **Observed:** Any shortcomings are minor.
- **Broadly observed:** The FMI has one or more shortcomings that give cause for concern. The FMI should follow up on these shortcomings by a specified date.
- **Partly observed:** The FMI has one or more shortcomings that could become serious if not addressed promptly. The FMI must give high priority to addressing these shortcomings.
- **Not observed:** The FMI has one or more serious shortcomings that warrant immediate action.
- **Not applicable:** The principle does not apply to the FMI.

Norges Bank urges the owners of each of the FMIs to rectify uncovered shortcomings. Norges Bank may require that FMIs subject to supervision comply with the principles. With regard to VPS/VPO, Norges Bank follows up compliance together with Finanstilsynet.

**Details of the assessments performed in 2017/2018.**
In 2017/2018, Norges Bank attached importance to FMI owners' organisation of cybersecurity work. In their evaluations, FMI owners followed the CPMI guidance on cyber resilience (CPMI-IOSCO 2016). This affects Principle 2 (governance), Principle 3 (framework for the comprehensive management of risks), Principle 8 (settlement finality), Principle 17 (operational risk) and Principle 20 (FMI links). On the basis of these evaluations, Norges Bank will perform an assessment in 2018/2019.

NICS, VPS and VPO have also been assessed against the following principles:

*NICS*
Principle 17 (operational risk) was considered broadly observed in 2017 on account of weaknesses in contingency arrangements. Norges Bank will reassess NICS against Principle 17 in 2018.

*VPO*
Principle 1 (legal basis) and Principle 13 (participant default rules and procedures) are considered broadly observed as VPS's rules for handling a participant's bankruptcy are unclear. VPS has collaborated with the settlement unit in Norges Bank to amend the rules in accordance with the regulation of 22 September 2016 on the execution of securities settlement. VPS and Norges Bank announced on 15 May 2018 that the new regulations will come into force on 18 June 2018.[1]

Principle 3 (risk management framework) and Principle 15 (general business risk) contain requirements for a recovery plan in the event of financial problems. VPS will complete such a plan before it applies for CSDR authorisation. Until the plan is completed, Norges Bank and Finanstilsynet consider these two principles broadly observed.

Principle 19 (tiered participation arrangements) is still considered broadly observed, because there are shortcomings in quantitative analyses and systematic risk assessment of indirect participants.

*VPS's CSD function*
Principle 3 (risk management framework) and Principle 15 (general business risk) apply to both VPO and VPS. For the same reason as cited for VPO above, VPS broadly observes these two principles

Principle 20 (FMI links) is considered broadly observed, as VPS does not conduct its own assessment of links in cases where securities registered in a foreign CSD are partly registered in VPS. VPS will meet this requirement before applying for CSDR authorisation.

1 VPS (2018) and Norges Bank (2018e).

**TABLE 1 Summary of the system against the principles. Year marks the date of the last evaluation**

| Principle / Type of FMI | NBO | NICS | VPO | VPS registry function | DNB (private settlement bank) | SMN (private settlement bank) |
|---|---|---|---|---|---|---|
| 1. Legal basis | 2014 | 2014 | 2018 | 2014 | 2014 | 2014 |
| 2. Governance | | 2017 | 2014 | 2014 | 2014 | 2014 |
| 3. Framework for the comprehensive management of risks | | 2015 | 2018 | 2018 | 2014 | 2014 |
| 4. Credit risk | 2014 | | 2014 | | 2014 | 2014 |
| 5. Collateral | 2014 | | | | | |
| 6. Margin | | | | | | |
| 7. Liquidity risk | 2014 | 2014 | 2014 | | 2014 | 2014 |
| 8. Settlement finality | 2014 | 2014 | 2014 | | 2014 | 2014 |
| 9. Money settlements | 2014 | 2014 | 2014 | | 2014 | 2014 |
| 10. Physical deliveries | | | | | | |
| 11. Central securities depositories | | | | 2014 | | |
| 12. Exchange-of-value settlement systems | 2014 | | 2014 | | | |
| 13. Participant-default rules and procedures | 2014 | 2014 | 2018 | 2014 | 2014 | 2014 |
| 14. Segregation and portability | | | | | | |
| 15. General business risk | 2014 | 2014 | 2018 | 2018 | 2014 | 2014 |
| 16. Custody amd investment risk | | | 2014 | 2014 | 2014 | 2014 |
| 17. Operational risk | 2017[1] | 2017 | 2014 | 2014 | 2014 | 2014 |
| 18. Access and participation requirements | 2014 | 2014 | 2014 | 2014 | 2014 | 2014 |
| 19. Tiered participation arrangements | 2014 | | 2018 | 2014 | | |
| 20 FMI links | | | 2014 | 2018 | | |
| 21. Efficiency and effectiveness | 2014 | 2014 | 2014 | 2014 | 2014 | 2014 |
| 22. Communication procedures and standards | 2014 | 2014 | 2014 | 2014 | | |
| 23. Disclosure of rules, key procedures, and market data | 2014 | 2014 | 2014 | 2014 | 2014 | 2014 |
| 24. Disclosure of market data by trade repositories. | | | | | | |

Table key:
Observed | Broadly observed | Partially observed | Not observed | Not applicable | Not part of the oversight of NBO[2]

1 Certain main considerations in this principle are not considered; see review of NBO oversight on page 20.
2 See review on oversight on page 20.

## 3.2 INTERBANK SYSTEMS

*Interbank systems are systems for the transfer of funds between banks with common rules for clearing and settlement.*

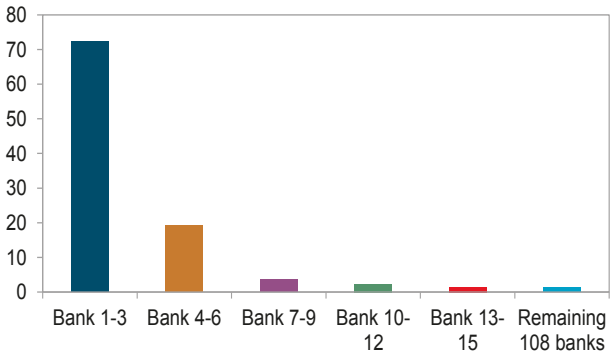
### NBO – NORGES BANK'S SETTLEMENT SYSTEM

#### The system in brief

Norges Bank is the ultimate settlement bank in the Norwegian payment system. Settlement between banks and other institutions with an account at Norges Bank takes place in Norges Bank's settlement system (NBO). All payments in NOK are ultimately settled in NBO (Chart 3.1).

Payments can be settled either one at a time (gross) or as part of a clearing (net) in NBO. While net settlements take place at set times during the day, payments submitted for gross settlement can be settled at any time throughout NBO's opening hours.

**CHART 3.2 Gross payments by banks. Percent. 2017**




Source: Norges Bank

All banks with an account at NBO can submit payments for gross settlement, but the 15 largest banks account for 99% of turnover (Chart 3.2). Analyses conducted by Norges Bank also show that most of

**CHART 3.1 The Norwegian payment system**

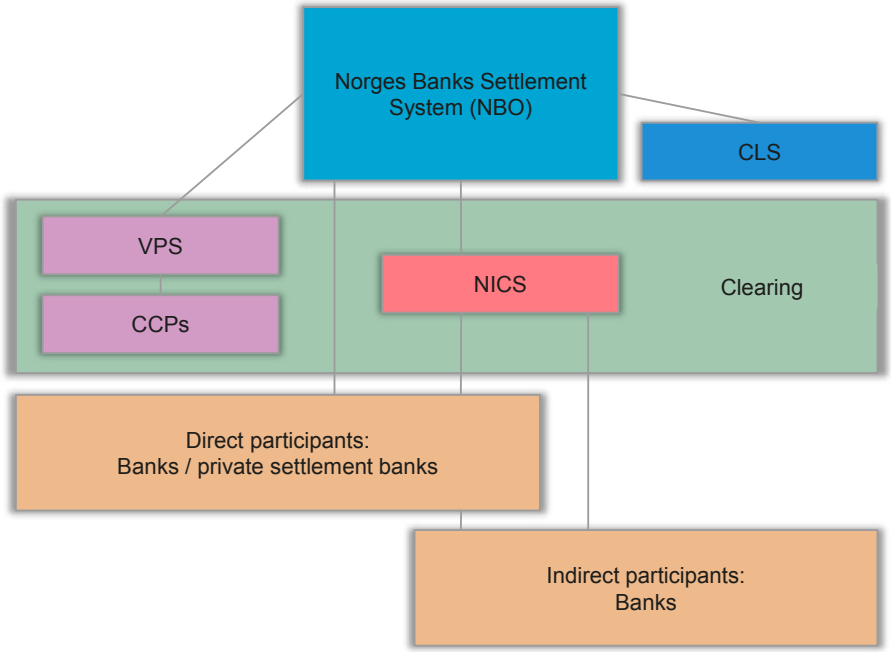



Chart is simplified for the sake of clarity.

Source: Norges Bank

the gross settlement turnover is related to the money and foreign exchange market (see box on the survey of turnover in Norges Bank's settlement system on page 26).

Norges Bank settles clearings from NICS, VPS and CLS (Chart 3.3). NICS clearings primarily include payments from private individuals, the government and businesses. The clearings from VPS are the cash legs of securities settlements. Clearings from CLS represent funding of NOK positions for cross-currency settlement in CLS.

Banks can participate directly or indirectly in NBO settlements. Indirect participants settle through a correspondent bank or private settlement bank. For further discussion of direct and tiered participation arrangements, see box on survey of turnover in Norges Bank's settlement system on page 26.

### Outsourcing

Norges Bank has entered into a licensing and maintenance agreement with the Italian company SIA S.p.A. (SIA) for the software used by NBO. This software was developed by the South African company Perago, a wholly-owned subsidiary of SIA. ICT operations for the settlement system have been outsourced to EVRY Norge AS since 2003.

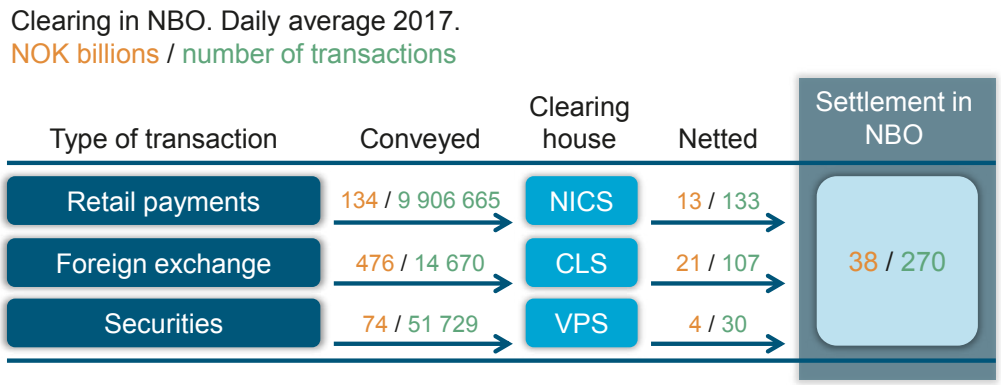
### System stability

NBO's operation was stable during the year, with the exception of technical disruptions in September and October. Owing to the same type of technical error, NBO stopped functioning on 29 September and 18 October 2017. On both dates, the errors resulted in the stoppage of payment processing for about half an hour. On 29 September, 64 payment orders totalling NOK 12.4bn were delayed by up to half an hour, while the corresponding figures for 18 October were 34 transactions totalling NOK 6.4bn. The errors have been rectified. This is the most serious error in NBO since the current settlement system was first used in 2009.

### Oversight

Over the past year, NBO has paid particular attention to cyber risk. In connection with this, the oversight unit at Norges Bank has conducted a self-evaluation against guidance on cyber security from CPMI-IOSCO (2016). The settlement unit at Norges Bank will follow up this self-evaluation in 2018.

**CHART 3.3 Net settlement in NBO**




Sources: Bits, VPS, CLS and Norges Bank

# Survey of turnover in Norges Bank's settlement system

Central banks have knowledge of the size of the turnover in settlement systems, but often have less detailed information about the purpose of the transactions settled or whether the transactions are direct or indirect (correspondent bank payments). Norges Bank has gathered data from various FMIs (NBO, NICS, CLS and private banks) and developed algorithms to analyse the turnover in NBO. On the basis of this work, Norges Bank knows the proportions of direct and indirect payments that settle in NBO and the purpose behind around 80% of the turnover in NBO.[1]

Direct participation in settlements contributes to financial stability.[2] A bank that participates directly is not dependent on other banks to settle payments, while indirect participants require a correspondent bank. A disruption at a correspondent bank can thus affect a large number of banks. When making an assessment on the impact of such a disruption, the purpose of payments must be taken into account. A failure in the settlement of a NOK 10bn payment may affect several hundred thousand households, or it may be a single money market transaction.

Norges Bank is undertaking an assessment on whether financial stability considerations warrant setting limits for tiered participation in NBO.[3] In collaboration with Norges Bank, Norwegian banks have put in place arrangements that ensure settlement of Norwegian customer payments in the event of a disruption in a correspondent bank (private settlement bank). A limit on tiered participation may apply to large foreign banks that are active in the Norwegian money and credit markets. Analyses performed by Norges Bank will inform the decision on this matter.

1 See Fevolden and Smith (2018) for more information on datasets, method and results.

2 Principle 19 in CPMI-IOSCO (2012) recommends encouraging direct participation of banks with high values or volumes of business through the FMI.

3 The Bank of England has set the limit at 2% of the average total payment activity, by value, processed each day, or 40% of the average daily value of its settlement bank's own payments (see p 374 in Bank of England (2013) for more information).

**Money and credit market transactions dominate turnover**

Most of the turnover in NBO is related to money and credit markets and foreign exchange trading (Chart 1). Around 9% are customer payments, often for the purchase of goods and services.[4] By value, domestic payments account for a daily average of NOK 13bn of the turnover in NBO. Underlying average daily gross turnover is NOK 134bn.[5]

**Large share of tiered participation in NBO**

The information gathered by Norges Bank shows that tiered participation accounts for a large share of turnover in NBO (Chart 2). In total, an average of NOK 212bn is settled each day, of which NOK 81bn, or 38%, arises from indirect participation. Large international banks without an account in Norges Bank explain most of the indirect turnover. These are primarily transactions related to the foreign exchange and interbank markets. There will thus be little impact on domestic payments if large indirect participants lose their access to settlement in NBO.

**Correspondent banks' own transactions account for most of the turnover in the NBO**

Chart 3 shows indirect participants' share of their correspondent banks' own transactions in NBO:

- Green (Category 1): Transactions from banks with an account in Norges Bank. There are seven foreign and no Norwegian banks in this category.
- Orange (Category 2): Transactions from banks without an account in Norges Bank. There are 51 foreign banks and one Norwegian bank in this category.
- Blue (Category 3): Transactions from banks with a small share (maximum 0.5%) of the turnover in their correspondent banks. There are 204 foreign and 126 Norwegian banks in this category.

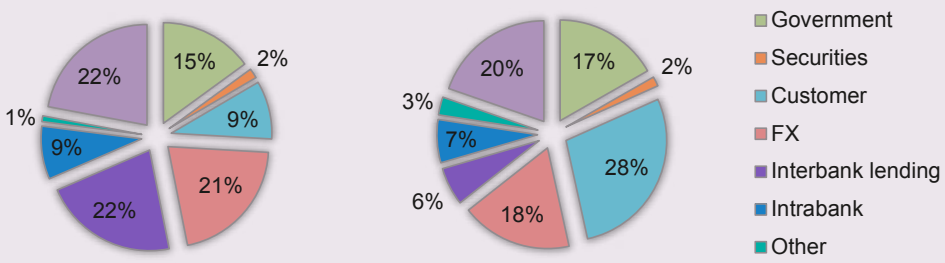
4 For 22% of turnover, no exact purpose can be determined, but it is safe to assume that this is related to the money and credit markets.

5 See Chart 3.3 in Section 3 of this *Report*.

Bar segments in category 1 and 2 show how large each indirect participant is. A bank may have more than one correspondent bank, so that the number of bar segments in the chart does not correspond with the number of banks mentioned in the bullet points above.

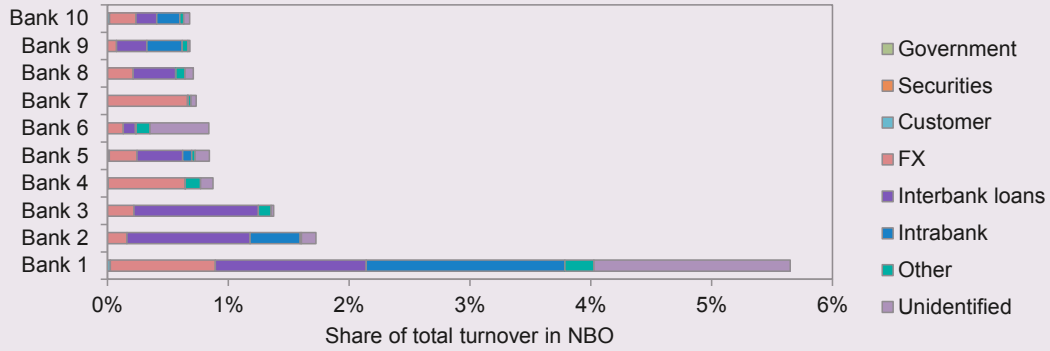
The largest indirect participant accounts for 34% of its correspondent bank's own transactions. This is a foreign bank without an account in Norges Bank and is shown with a thicker border in the chart.

**CHART 1: The purpose behind transactions settled in NBO. Left=value, Right=number.**



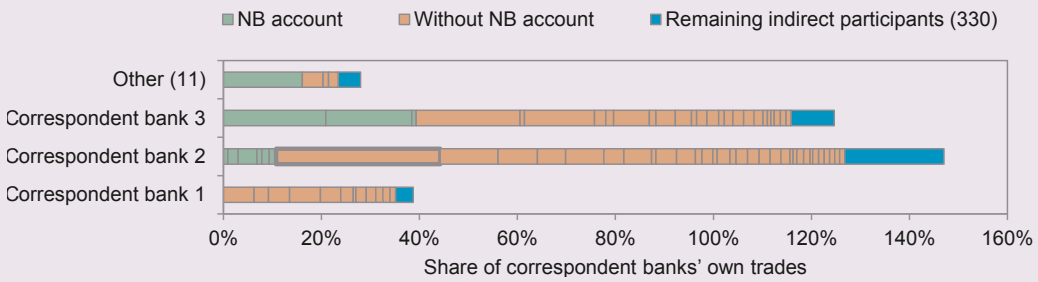

Source: Norges Bank

**CHART 2: The purpose behind the turnover in NBO of the 10 largest indirect participants**




Source: Norges Bank

**CHART 3: Indirect participants' share of correspondent banks' trades in NBO**




Source: Norges Bank

## NICS – NORWEGIAN INTERBANK CLEARING SYSTEM

### The system in brief

NICS is the banks' common platform for clearing and receipt of payment transactions. Nearly all payment transactions in Norway, including card transactions, are sent to NICS. Most of the transactions received by NICS are included in a multilateral clearing in which each bank's net position against all other banks is calculated. The clearing result is sent to Norges Bank's settlement system (NBO), where the net positions are settled. Clearings are settled five times daily each working day at 5.30 am, 9.30 am, 11.30 am, 1.30 pm and 3.30 pm.

Banks also send transactions via NICS that are not included in a multilateral clearing. These transactions are settled individually (gross) in NBO. Payments can be settled gross throughout NBO's opening hours, ie from 5.30 am to 4.35 pm. These are generally payments of more than NOK 25m.

### Outsourcing

The system operator, Bits AS, has outsourced the technical operation of NICS to Nets Norge Infrastructure (NNI). NNI also uses other companies in the Nets group to perform operational tasks.

### System stability

The technical operation of NICS has been stable in recent years. There were few disruptions over the past year. However, NICS was affected by an incident at EVRY on 6 October 2017, the result of which was that a number of banks were unable to send transactions to NICS or receive transactions from NICS. The incident resulted in settlement lags for banks that at the outset were not affected by the incident at EVRY. Bits AS has reported to Norges Bank that the deficiency that caused the lags has been rectified. On 24 April 2018, there was a disruption in the NICS system which caused the morning settlement to be delayed for more than two hours. Norges Bank is following up the incident with Bits AS.

### Supervision

In 2016, Norges Bank received an application for the transfer of responsibility for operating NICS from the NICS Operations Office to Bits AS, partly as the latter has greater capacity and expertise. Bits AS is an infrastructure company formed by Finance Norway in 2016. In June 2017, Norges Bank approved the decision to give Bits AS the responsibility for operating NICS. The license terms were updated in connection with the transfer.

In November 2016, Norges Bank received a change notification concerning the transfer of certain operational tasks from Nets in Norway to Nets in Denmark. The tasks that were transferred included system monitoring. In September 2017, Bits AS was granted provisional authorisation to make changes on certain conditions. One condition is the maintenance of operational contingency arrangements in Norway with the expertise and resources to take control of operations at a moment's notice.

In October 2017, Norges Bank received a change notification from Bits AS concerning the relocation of one of NICS' two operational sites, which increased the geographical distance between them. Furthermore, the notification also included the establishment of a new operational structure for NICS including the duplication of the operational environment at both operational sites. Greater distance is positive because it reduces the risk of the same incident simultaneously impacting both operational sites. The new operational site is however co-located with other participants in the financial infrastructure, which increases concentration risk in the payment system. Norges Bank has taken note of the change notification.

The relocation of one of the operational sites is a part of a new data centre strategy for NICS. Bits AS has previously assessed the need for a third operational site to strengthen NICS's contingency arrangements.[30] According to Bits AS, the establishment of a new data centre strategy will eliminate several of the conditions that created the need for a third operational site for NICS. Bits AS has therefore put the assessment of a third operational site on hold. In its review of the change notification concerning the relocation of one of the operational sites and changes to the operational structure, Norges Bank has not assessed whether this changes the need for a third operational site. Norges Bank has requested that Bits AS promptly explain its process for assessing the need for a third operational site.

In its supervision of NICS, Norges Bank attached particular importance to cyber risk over the last year. As part of its compliance activities, Bits AS has conducted

30 Norges Bank (2017a).

a self-evaluation against the guidelines in CPMI-IOSCO (2016). Following this self-evaluation, Norges Bank has requested that Bits AS implement follow-up measures.

In 2018, Norges Bank will conduct a re-evaluation of NICS against CPMI-IOSCO Principle 17 on operational risk. Bits AS' report on the need for a new operational site and follow-up measures related to cyber risks will be important elements of this evaluation.

## PRIVATE SETTLEMENT BANKS

### The systems in brief

There are three private settlement banks in Norway that settle other banks' payments in NBO. DNB is the settlement bank for 91 banks, SpareBank 1 SMN for 10 banks and Danske Bank for one bank.

Banks that are referred to as private settlement banks perform correspondent bank services for other banks in the domestic payment system. This means that they take over the positions of other banks after they are cleared in NICS and settle on their behalf in NBO. Following settlement at Norges Bank, the participant banks' settlement accounts are credited or debited at the private settlement bank.

Danske Bank's settlement system is too small to require oversight by Norges Bank.

### Outsourcing

Both DNB and SpareBank 1 SMN have outsourced the operation of their settlement systems. Operational services for both settlement systems are primarily provided by EVRY.

### Stability of the systems

There were two disruptions in DNB's settlement system in 2017. The disruptions occurred on 16 March and 15 June. SpareBank 1 SMN experienced a disruption on 6 October. None of the disruptions at DNB and SpareBank 1 SMN had significant consequences, and the errors have been rectified. Operation of the DNB and SpareBank 1 SMN settlement bank systems were otherwise stable during the year.

### Supervision and oversight

As DNB has a licence from Norges Bank for its settlement system, Norges Bank holds semi-annual supervisory meetings with DNB concerning its settlement system. Outsourcing and cyber risks have been included on the meeting agendas over the last year, and cyber risk assessment primarily follows the guidelines. In cooperation with Finanstilsynet, Norges Bank has also participated in an ICT inspection in order to assess whether DNB's settlement system complies with the guidelines. Certain topics in the guidelines were not considered in Finanstilsynet's ICT inspection. In consultation with Finanstilsynet, Norges Bank has submitted a letter to DNB requesting DNB to provide an account of these topics.

In March 2017, Norges Bank received a change notification concerning DNB's intention to offshore parts of its settlement system operations. On 15 September 2017, DNB was granted provisional authorisation for relocation on certain conditions. One of the conditions is that there must be operational contingency arrangements in place in Norway with the expertise and resources to take control of operations at a moment's notice. DNB has yet to exercise the authorisation.

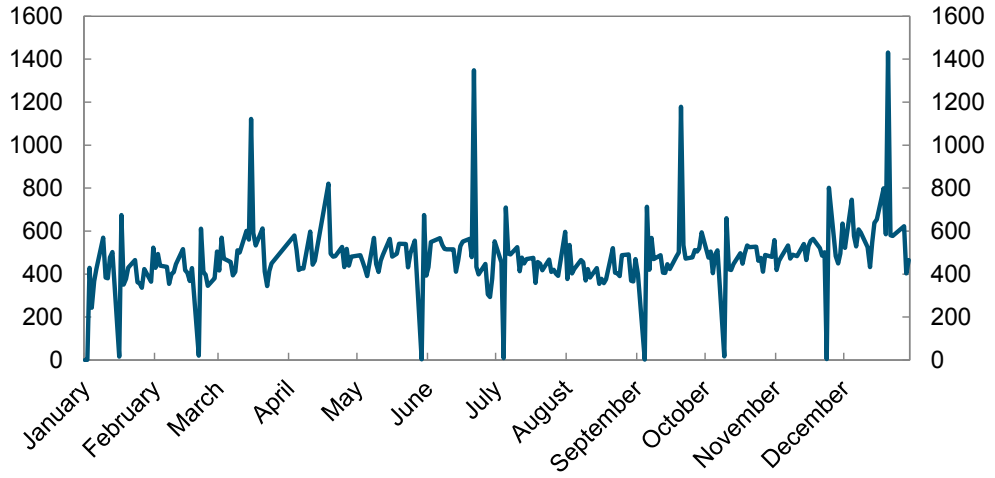
SpareBank 1 SMN does not require a licence, and this bank's settlement system is therefore not subject to supervision by Norges Bank. Norges Bank nevertheless oversees its operation and holds regular meetings. Topics at these meetings include the operating situation, exercises carried out and any system changes. An important topic at the supervisory meeting in 2018 will be cyber security.

## CLS BANK INTERNATIONAL

### The system in brief

CLS Bank International (CLS) operates the world's largest multicurrency cash settlement system, settling payment instructions related to foreign exchange (FX) transactions in 18 currencies, including the Norwegian krone (NOK). Payment instructions are settled on a gross basis across settlement members' accounts on the books of CLS. CLS calculates funding as a net position for each settlement member in each currency. Ingoing and outgoing currency payments are transacted through CLS and member banks' accounts with the various central banks. A settlement member may use another bank (a nostro agent) to make and receive CLS-related payments in currencies that is does not self-clear. In January 2017, CLS introduced two new membership categories: affiliated settlement membership and non-shareholder settlement membership.

CHART 3.4: Gross settlement of NOK in CLS for 2017. Daily total in billions of NOK




Source: Norges Bank

## BREXIT AND THE SETTLEMENT FINALITY DIRECTIVE

A large percentage of Norwegian financial institutions' transactions are settled in foreign interbank systems. Clearing and settlement agreements have traditionally not been binding on entities placed in insolvency proceedings, resulting in legal uncertainty.

In the EEA area, this uncertainty has been removed as the Settlement Finality Directive (98/26/EC) has given interbank systems the power to conclude clearing and settlement agreements that are also enforceable in the event of insolvency proceedings. The directive's provisions have been transposed into the national legislation of all EEA member states. These agreements thus provide added predictability when insolvency proceedings are opened against a participant in an EEA jurisdiction.

On 29 March 2017, the UK notified the EU of its intention to invoke Article 50 of the Lisbon Treaty and will leave the EU on 29 March 2019. However, the UK will retain the provisions of the Settlement Finality Directive on its law books and agreements with UK interbank systems will thus continue to be legally enforceable. For these agreements to be valid in other EEA countries, national legislation will have to specify that the directive's enforceability rules will also apply to interbank systems outside the EEA.

On 2 March 2018, the Ministry of Finance circulated for comment a proposal to amend the Payment Systems Act to cover Norwegian financial institutions participating in interbank systems outside the EEA. If this proposal becomes law, agreements between UK interbank systems and Norwegian participants will be protected by the Settlement Finality Directive also after the UK has left the EU. This will remove the uncertainty for Norwegian participants. Member states that have already chosen this solution are Denmark, Germany, Belgium and Spain.

Traditionally, FX transactions are settled in different countries' settlement systems and in different time zones. Parties have therefore been exposed to a risk that a counterparty will default on its leg of a foreign exchange transaction (referred to as "Herstatt risk"). In CLS, settlement of one leg of a foreign exchange transaction is conditional upon settlement of the other leg, eliminating the Herstatt risk in foreign exchange settlement. Since Norwegian banks trade foreign exchange in large amounts on a daily basis, CLS has substantially reduced Norwegian banks' Herstatt risk (Chart 3.4).

At year-end 2017, 67 banks were settlement members of CLS. DNB was the only Norwegian settlement member. Institutions that are not settlement members (third parties) may use a settlement member to settle foreign exchange transactions in CLS on their behalf. In 2017, 259 Norwegian institutions participated in this manner.

CLS rules are governed by British law. CLS Bank International, which operates the settlement system, is located in the United States and has a limited purpose US banking license.

The Ministry of Finance has circulated for comment a proposed amendment to the Payment Systems Act to ensure that UK interbank systems will continue to be protected by the Settlement Finality Directive after the UK leaves the EU in 2019 (see box on Brexit and the settlement finality directive on page 30). Withdrawal of the UK from the EU will thus not result in legal uncertainty for CLS regarding Norwegian settlement participants.

### Outsourcing

IBM provides CLS with operational services, as well as service management and support functions.

### System stability

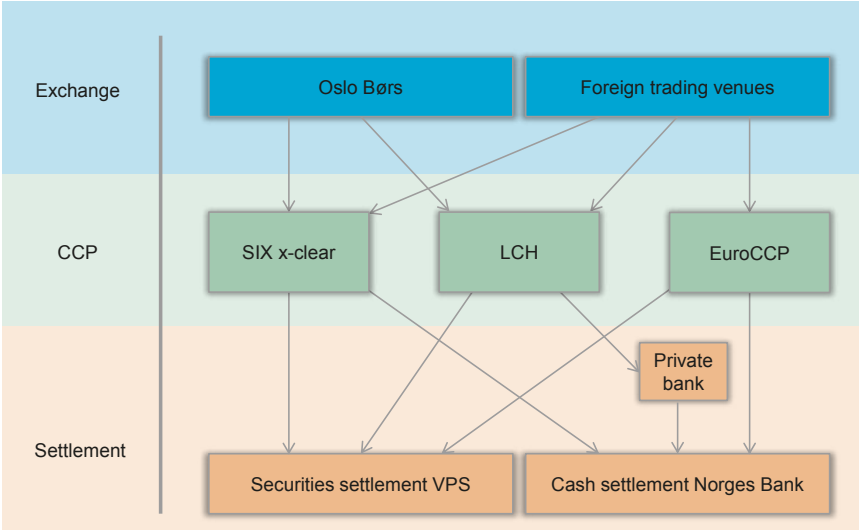
There have been no incidents that affected settlement of NOK in CLS over the past year.

### Supervision and oversight

CLS is subject to both supervision and oversight. CLS is supervised by the Federal Reserve, while 23 central banks, including Norges Bank, cooperate on oversight of CLS via the CLS Oversight Committee (OC). The Federal Reserve chairs the OC. This cooperative oversight arrangement is based on recommendations in "Principles for Financial Market Infrastructures (PFMI)" (CPMI-IOSCO, 2012).

CLS Bank has published a description of its approach to observing the PFMI in an updated disclosure framework. The central banks participating in the oversight of CLS have been given the opportunity to comment on this disclosure. CLS updates this document every two years.

**CHART 3.5 Trading, clearing and settlement of equities in NOK**




Source: Norges Bank

## 3.3 SECURITIES SETTLEMENT

Verdipapirsentralen ASA (VPS) holds a licence as the Norwegian central securities depository (CSD). VPS is also operator of the Norwegian securities settlement system (VPO). In VPO, rights to securities are registered to VPS accounts, while the cash leg is settled in NBO.

Transactions sent to VPO for settlement come from a number of trading venues and pass through several central counterparties (CCPs) (Chart 3.5). CCPs participate in VPO because they enter into equity trades on regulated trading venues, becoming the counterparty to both the buyer and the seller of the equities, a process known as clearing.

### VPS SETTLEMENT SYSTEM

**The system in brief**

The securities settlement system (VPO) performs settlement of equities, equity certificates and fixed income securities denominated in NOK. A total of 36 market participants (investment firms, banks and CCPs) participate directly in VPS. Of these, 19 also participate directly in the cash leg of settlement in NBO. Participants in settlement in NBO are banks and CCPs. There are also a number of indirect participants.

For equity trades that are cleared via a CCP, the CCPs calculate a net position per equity and a net cash position for each participant. As a result of this netting, fewer transactions are sent for settlement in VPO. Trades in NOK bonds are not cleared by CCPs.

### NEW RULES FOR SECURITIES SETTLEMENT AND CENTRAL SECURITIES DEPOSITORIES

The EU adopted the Central Securities Depositories Regulation (CSDR) in 2014. Central securities depositories (CSDs) play a key role in the issuance, settlement, safekeeping and collateral management of financial instruments. They are therefore critical institutions for securities markets. The aim of the regulation is to promote secure and efficient CSDs and securities settlement systems in the EU.

In autumn 2017, European CSDs applied to their home state authorities for new CSDR authorisations, which entitles them to offer services throughout the EU. This opens the door to competition between CSDs.

As described in Norges Bank (2017a), the Ministry of Finance is preparing the implementation of the CSDR in Norway and a new Central Securities Depository Act. The CSDR will entail changes to the Norwegian securities settlement system (VPO) and more extensive regulation of VPS. It is uncertain when the CSDR can be implemented in Norway. When the regulation is implemented, VPS will apply for CSD authorisation. Norges Bank does not currently oversee any CSDs other than VPS, but this may change under the CSDR. If foreign CSDs with CSDR authorisation wish to settle in NOK above certain thresholds, Norges Bank must collaborate with the relevant foreign authorities on oversight.

VPO settlement takes place twice a day, at 6 am and 12 noon. VPO settlement is a multilateral net settlement. The net daily settlement volume in 2017 was NOK 4.3bn, with 73% of transactions by volume settled in the early morning settlement.

Before each settlement, VPS calculates both cash and security legs of participants' positions. These cash positions are settled through the participants' VPO settlement accounts in NBO. Once the cash leg is complete, the rights to the securities are registered to VPS accounts (delivery versus payment). These rights are registered individually (gross). In 2017, such transactions in VPS averaged 52 000 per day. There are now approximately 1.35m VPS accounts and the market value of securities registered with the VPS is approximately NOK 5 600bn.

The standard procedure for securities trades on registered trading venues is settlement after two days. Some trades are not settled on the agreed date. In 2017, 96.7% of transactions and 93.6% of the value of settlements in VPO were settled on the agreed date. Most transactions that were not settled on the agreed date were settled one or two days later, and only 0.2% were cancelled.

In the period between 2016 and 2018, VPS is conducting a modernisation programme covering IT systems, organisation, skills and market practices. The programme involves, among other things, adjustment to new EU rules (the Central Securities Depositories Regulation (CSDR)). To comply with the CSDR, VPS must apply to the Norwegian authorities for a new authorisation for its activities and make changes to its services and operations. For example, VPS intends to increase the number of daily settlements from two to three. The plan is for a third daily settlement at 2:45 pm to be introduced in 2018 Q4.

### Outsourcing

VPS does not outsource the operation of its systems.

### System stability

Over the past year, there have been few disruptions in VPO, but on 5 March 2018, the early morning settlement was delayed for approximately four and a half hours due to a system change. Out of concern for participants, the subsequent late morning settlement was postponed by approximately one and a half hours. VPS has stated that it has introduced measures to prevent the recurrence of a similar disruption.

### Oversight

Norges Bank oversees VPO and VPS, while Finanstilsynet supervises VPS, including VPS's settlement operation. The Bank holds semi-annual oversight meetings with VPS, with Finanstilsynet invited as observer. Additional meetings on specific issues are conducted as necessary. Over the past year, Norges Bank's oversight activities focused on VPS's work with cyber security and preparations for the EU's new Central Securities Depositories Regulation (CSDR) (see box on new rules for securities settlement and central securities depositories on page 32).

## CENTRAL COUNTERPARTIES

### The systems in brief

Central counterparties (CCPs) enter into transactions between buyers and sellers of financial instruments and guarantee that the contracts are fulfilled (clearing) (see Chart in Box 1). Banks and other participants in financial markets thus reduce their exposure to one another, but on the other hand CCPs must handle substantial exposures. In periods of market turmoil, resilient CCPs can make an important contribution to financial stability.

The European Market Infrastructure Regulation (EMIR) entered into force in Norway on 1 July 2017[31] and includes the implementation of a clearing obligation for certain types of OTC derivatives[32] and a reporting obligation for all derivatives.

EMIR also sets out requirements for the operation of CCPs and trade repositories, and for authorities' performance of supervision work.

No CCPs are headquartered in Norway, so Norwegian market participants' trades in financial instruments are settled through different foreign CCPs. Equity trades in NOK on different trading venues are settled through Swiss SIX x-clear, Dutch EuroCCP and the UK CCP LCH EquityClear. SIX x-clear and LCH swapclear also clear equities on Oslo Børs (Chart 3.6). LCH also clears OTC interest rate derivatives.

### Oversight

Norges Bank's oversight of CCPs that are important for the financial sector in Norway is performed

31 Finanstilsynet (2017c).

32 EU (2012) EMIR (European Market Infrastructure Regulation) is the EU's regulation for OTC derivatives, CCPs and trade repositories, and the regulation was later supplemented with further provisions.

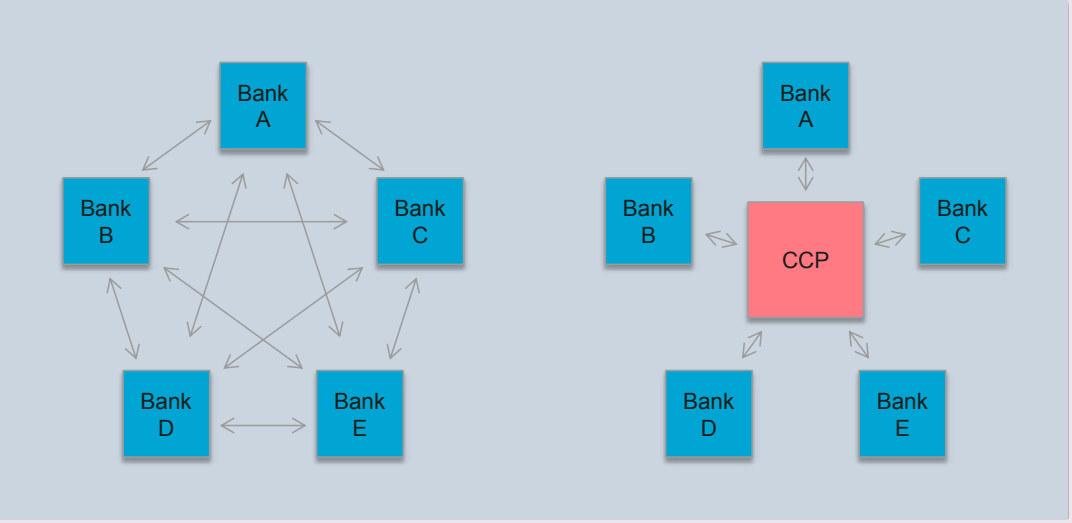
## CENTRAL COUNTERPARTIES' RISK MANAGEMENT

The prudent management of central counterparty (CCP) risk is crucial for financial sector resilience. CCPs must be capable of performing their role adequately even under extreme market stress conditions. This requires CCPs to have access to sufficient financial resources and a proper understanding of the risks they assume.

These financial resources primarily comprise margins from participants and default funds. Margins comprise cash and securities that a participant must post to cover the risks to which the participant exposes the CCP. Margins from a participant are required to cover exposures on at least 99% of days. Default funds comprise cash and securities paid in by participants to cover losses potentially inflicted on the CCP by other participants. The default fund is drawn on if the margins from a defaulting participant are insufficient to cover a loss. While margins will cover small losses, the default fund will ensure shared coverage of large losses.

CCPs conduct a number of quantitative tests of counterparty risk. For example, "backtesting" is performed to test whether posted margin will cover losses of at least 99% of days. CCPs use stress tests to verify whether they would have sufficient financial resources to function even if their two largest participants defaulted in a period of severe market turbulence. A more detailed description of financial resources and tests for CCPs is provided on pages 13 and 14 of the 2015 *Financial Infrastructure Report*.

Chart 3.6 Central counterparties



through participation in international collaborative arrangements:

- The Dutch central bank has set up an EMIR College to oversee EuroCCP.
- The Bank of England has set up an EMIR College to oversee LCH, and has also established a Global College with a broader composition than the EMIR College. Norges Bank participates in the global college without voting rights.
- Norges Bank and Finanstilsynet have signed a collaboration agreement with the Swiss authorities on the oversight of SIX x-clear.

Norges Bank regularly receives qualitative and quantitative reports from the three CCPs, and participates in an annual minimum of one meeting for each of them.

### International work

Since CCPs and trade repositories often operate in several jurisdictions, both national and international authorities must work together to establish effective regulation. International work that is relevant for Norges Bank's oversight can be divided into two main categories: 1) Recommendations and analyses at the global level and 2) Regulation and analyses at the EU level.

## INTERNATIONAL AUTHORITIES PARTICIPATING IN THE WORK ON CCP RESILIENCE

**Global level**

**Financial Stability Board (FSB)** is an international forum for central banks and governments to monitor and advise on the global financial system.

**Committee on Payment and Market Infrastructures (CPMI)** is a committee of central banks for the promotion of robust and efficient solutions related to payment, clearing and settlement systems.

**International Organisation of Securities Commissions (IOSCO)** is an association of organisations regulating the securities and futures markets. Finanstilsynet is a member of IOSCO.

**Basel Committee on Banking Supervision (Basel Committee)** promotes collaboration on banking regulation.

FSB, CPMI and the Basel Committee were created by the G10 or G20 with mainly these countries as participants.

**EU level**

**European Securities and Markets Authority (ESMA)** is the supervisory body for EMIR, which regulates CCPs and transaction repositories. As a European supervisory authority, ESMA has legal powers over Norwegian companies (e.g. banks) in certain matters.

**European Systemic Risk Board (ESRB)** is an independent agency that promotes financial system supervision in the EU. The ESRB performs analyses and advises ESMA. Norges Bank has observer status in the ESRB and participates in several ESRB task forces.

**1) Recommendations and analyses at the global level**
On behalf of the G20 Finance Ministers and Central Bank Governors, a work plan was drafted in 2015 to further develop the regulation and oversight of derivatives markets and CCPs.[33] In 2017, four reports were published as a follow-up to the plan.

- "Analysis of Central Clearing Interdependencies" (FSB, CPMI-IOSCO and the Basel Committee)[34] analyses data that identify interdependencies between CCPs and their participants. The report shows that the concentration of interdependency is very high when there are few CCPs and banks that account for most of the turnover. A relatively high level of mutual dependence was also identified between global banks and large international CCPs. The latter use the global banks as important providers of liquidity, payment and deposit services. The failure of a large bank can therefore impact a CCP in different ways.

- "Guidance on Central Counterparty Resolution and Resolution Planning" (FSB)[35] provides guidance on the resolution of CCPs and the planning of such resolution. Good planning and preparedness are crucial for preventing serious difficulties to a CCP which might result in a threat to financial stability, and contribute to the most appropriate allocation of losses.

- "Resilience of central counterparties (CCPs): Further guidance on the PFMI" (CPMI-IOSCO)[36] supplements and sheds light on the principles that were designed for financial market infrastructures (FMIs) in 2012. This guidance specifies how CCPs are to comply with the principles. It provides, for example, a detailed description of which tests to carry out and how they are to be conducted.

- "Framework for supervisory stress testing of central counterparties (CCPs)" (CPMI-IOSCO and the Basel Committee)[37] is a draft framework for authorities' stress testing of CCPs. The stress tests can be used to assess the effects of multiple CCPs responding to the same event.

33 FSB, BCBS, CPMI and IOSCO (2015).
34 FSB, CPMI, IOSCO, BCBS (2017).
35 FSB (2017b).
36 CPMI-IOSCO (2017a).
37 CPMI-IOSCO (2017b).

**2) Regulations and analyses at the EU level**
Under the auspices of the EU in 2017, legislative work was carried out and new analyses of CCPs and trade repositories were performed. Milestones of this work were:

- In May 2017, the European Commission published a proposal for EMIR 2, with only minor revisions.

- In November 2017, the Commission introduced new requirements for reporting to trade repositories, which has improved the quality of the reports. Trade repository data also provide authorities with a clearer overview of financial sector exposures and are thus important in the work to promote financial stability.

- In 2017, ESMA conducted stress tests of all euro area CCPs[38]. The tests shed light on the capacity of CCPs to absorb losses and meet their payment obligations on time. The stress test showed that European CCPs are robust, and that they can cover losses even if several participants default simultaneously.

In January 2018, ESMA also circulated for comment a proposal for guidelines on anti-procyclicality margin measures (see box on the guidelines).

38 ESMA (2017b).

## GUIDELINES ON ANTI-PROCYCLICALITY MARGIN MEASURES

In periods of market turbulence, CCPs' exposures to participants rise, and to cover these exposures, CCPs increase margin calls. In such periods, market participants are often under liquidity pressure. In 2012, the European Commission published guidelines to limit margin calls when banks are under liquidity pressure (procyclicality)[1].

However, procyclicality may be counteracted by CCPs raising the level of margins in normal periods. For example, stressed observations can be included in margin models whereby the parameters in the model are based on observations over a 10-year lookback period or by applying a margin buffer.

Norges Bank is a member of an ESRB task force with a broad focus on procyclicality across different markets. The group is to deliver its report by the end of 2019.

1 EU (2013).

# References


Aera (2018): "Skapt av handelen – for handelen" [Created by trading – for trading], Betalingsformidling 2018, presentation, Trondheim (in Norwegian only). https://static1.squarespace.com/static/562a32b0e4b0e6f4ec3104ae/t/5aaa5f5c53450a6f4dea99b7/1521114995286/Aera+Betalingskonferansen+Mars+2018+Light.pdf

Ali, R., J Barrdear, R Clews, and J Southgate (2014a): "The economics of digital currencies" *Bank of England Quarterly Bulletin* 54(3), 276–286. https://www.bankofengland.co.uk/-/media/boe/files/quarterly-bulletin/2014/the-economics-of-digital-currencies.pdf?la=en&hash=E9E56A61A6D71A97DC8535FEF211CC08C0F59B30

Ameln, M. and P. Songe-Møller (2018). "Hvorfor er digitale platformer så kraftfulle?" [Why are digital platforms so powerful?], Sprint Consulting (in Norwegian only). https://sprint.no/hvorfor-er-digitale-plattformer-sa-kraftfulle/

ASX (2017): "ASX selects distributed ledger technology to replace CHESS", Press Release, 7 December 2017. https://www.asx.com.au/documents/asx-news/ASXSelects-DLT-to-Replace-CHESS-Media-Release-7December2017.pdf

Bank of England (2018): "The Bank of England's supervision of financial market infrastructures", *Annual Report 2018*. https://www.bankofengland.co.uk/news/2018/february/supervision-of-financial-market-infrastructure-sannual-report-2018

Bech, M. L. and R. Garratt (2017): "Central Bank Cryptocurrencies", *BIS Quarterly Review,* 17 September 2017. https://www.bis.org/publ/qtrpdf/r_qt1709f.htm

Carney, M. (2018): "The future of money". Speech, 2 March 2018, Edinburgh. https://www.bankofengland.co.uk/speech/2018/mark-carney-speech-to-the-inaugural-scottish-economics-conference

Chapman, J., R. Garratt, S. Hendry, A. McCormack and W. McMahon (2017): "Project Jasper: Are Distributed Wholesale Payment Systems Feasible Yet?", *Bank of Canada Financial system Review,* June 2017. https://www.bankofcanada.ca/wp-content/uploads/2017/05/fsr-june-2017-chapman.pdf

CPMI (2015): "Digital Currencies". https://www.bis.org/cpmi/publ/d137.pdf

CPMI (2017): "Distributed ledger technology in payment, clearing and settlement – An analytical framework". https://www.bis.org/cpmi/publ/d157.pdf

CPMI-IOSCO (2012): "Principles for financial market infrastructures". https://www.bis.org/cpmi/publ/d101a.pdf

CPMI-IOSCO (2016): "Guidance on cyber resilience for financial market infrastructures". https://www.bis.org/cpmi/publ/d146.pdf

CPMI-IOSCO (2017a): "Resilience of central counterparties (CCPs): Further guidance on the PFMI", July 2017. https://www.bis.org/cpmi/publ/d163.pdf

CPMI-IOSCO (2017b): "Consultative report: Framework for supervisory stress testing of central counterparties (CCPs)", June 2017. https://www.bis.org/cpmi/publ/d161.pdf

ECB (2018): "Securities settlement systems: delivery versus-payment in a distributed ledger environment, STELLA – a joint research project of the European Central Bank and the Bank of Japan". https://www.ecb.europa.eu/pub/pdf/other/stella_project_report_march_2018.pdf

ESMA (2017a): "The Distributed Ledger Technology Applied to Securities Markets". https://www.esma.europa.eu/press-news/esmanews/esma-assesses-dlt%E2%80%99s-potentialand-interactions-eu-rules

ESMA (2017b): "Report: EU-wide CCP stress test 2017". http://firds.esma.europa.eu/webst/ESMA70-151-1154%20EU-wide%20CCP%20Stress%20Test%202017%20Report.pdf

EU (2012): Regulation (EU) No 648/2012 of the European Parliament and of the council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012R0648&from=EN

EU (2013): "Commission Delegated Regulation (EU) No 153/2013".
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013R0153&from=EN

EU (2017a): Proposal for amending Regulation (EU) No 648/2012.
https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-208_en

EU (2017b): Regulation on EMIR. Commission Implementing Regulation (EU) 2017/105 of 19 October 2016 amending Implementing Regulation (EU) No 1247/2012 laying down implementing technical standards with regard to the format and frequency of trade reports to trade repositories according to Regulation (EU) No 648/2012 of the European Parliament and of the Council on OTC derivatives, central counterparties and trade repositories.
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0105&from=EN

Fevolden, M. B. and L. Smith (2018): "What kind of payments settle in a real-time gross settlement system?", Forthcoming Norges Bank *Staff Memo*.

Finanstilsynet (2013): "Advarsel til forbrukere – informasjon om virtuelle valutaer" [Warning to consumers – information on virtual currencies], 13 December 2013 (in Norwegian only).
https://www.finanstilsynet.no/nyhetsarkiv/nyheter/2013/advarsel-til-forbrukere---informasjon-om-virtuelle-valutaer/

Finanstilsynet (2017a): "Risk and Vulnerability Analyses (RAV) 2016".
https://www.finanstilsynet.no/en/publications/risk-and-vulnerability-analyses-rav/?id=

Finanstilsynet (2017b): "Initial Coin Offerings (ICO-er) – advarsel til investorer og foretak" [Initial coin offerings (ICOs) – warning to businesses and investors], 20 November 2017 (in Norwegian only).
https://www.finanstilsynet.no/markedsadvarsler/2017/initial-coin-offerings-icoer---advarsel-til-investorer-og-foretak/

Finanstilsynet (2017c): "Gjennomføring av EMIR" [Implementation of EMIR]. Circular 6/2017, 4 July 2017 (in Norwegian only).
https://www.finanstilsynet.no/tema/emir/

Finanstilsynet (2018): "Finanstilsynet advarer forbrukere om kryptovaluta" [Finanstilsynet warns consumers about cryptocurrencies], 12 February 2018 (in Norwegian only).
https://www.finanstilsynet.no/nyhetsarkiv/nyheter/2018/finanstilsynet-advarer-forbrukere-om-kryptovaluta/

FSB (2017a): "Financial Stability Implications from FinTech".
http://www.fsb.org/2017/06/financial-stability-implications-from-fintech/

FSB (2017b): "Guidance on Central Counterparty Resolution and Resolution Planning", 5 July 2017.
http://www.fsb.org/wp-content/uploads/P050717-1.pdf

FSB (2018): "Letter to G20 Finance Ministers and Central Bank Governors", 13 March 2018.
http://www.fsb.org/wp-content/uploads/P180318.pdf

FSB, BCBS, CPMI, and IOSCO (2015): "2015 CCP Work plan".
https://www.bis.org/cpmi/publ/d134b.pdf

FSB, CPMI, IOSCO, and BCBS (2017): "Analysis of Central Clearing Interdependencies", July 2017.
https://www.bis.org/cpmi/publ/d164.pdf

He, D., R. Leckow, V. Haksar, T. Mancini-Griffoli, N. Jenkinson, M. Kashima and H. Tourpe, H. (2017): "Fintech and Financial Services: Initial Considerations". *IMF Staff Discussion Notes*.
https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2017/06/16/Fintech-and-Financial-Services-Initial-Considerations-44985

Meld. St. 38 (2016–2017): "Cyber Security — A joint responsibility".
https://www.regjeringen.no/en/dokumenter/meld.-st.-38-20162017/id2555996/

Ministry of Finance (2017a): "Letter of 20 December 2017 to Finanstilsynet".

Ministry of Finance (2017b): "NOU 2017:13 New Central Bank Act. Report of the Law Commission on the Act relating to Norges Bank and the Monetary System".
https://www.regjeringen.no/en/aktuelt/report-of-the-law-commission-on-the-act-relating-to-norges-bank-and-the-monetary-system/id2558679/

Ministry of Finance (2018a): "Financial Markets Report 2018
https://www.regjeringen.no/en/dokumenter/meld.-st.-14-20172018/id2599000/

Ministry of Finance (2018b): "New requirements on banks' contingency arrangements for cash". Press release, 17 April 2018.
https://www.regjeringen.no/en/aktuelt/new-requirements-on-banks-contingency-arrangements-for-cash/id2598131/

Norges Bank (2014): *Financial Infrastructure Report* 2014.
https://www.norges-bank.no/en/Published/Publications/Financial-Infrastructure-Report/Financial-infrastructure-report-2014/

Norges Bank (2015): *Financial Stability Report* 2015.
https://www.norges-bank.no/en/Published/Publications/Financial-Stability-report/2015-Financial-stability/

Norges Bank (2016): *Financial Infrastructure Report* 2016
https://www.norges-bank.no/en/Published/Publications/Financial-Infrastructure-Report/Financial-infrastructure-2016/

Norges Bank (2017a): *Financial Infrastructure Report* 2017.
https://www.norges-bank.no/en/Published/Publications/Financial-Infrastructure-Report/financial-infrastructure-2017/

Norges Bank (2017b): Letter of 17 August to the Ministry of Finance (in Norwegian only).
https://www.norges-bank.no/Publisert/Brev-og-uttalelser/2017/2017-08-17-brev/

Norges Bank (2017c): Letter of 12 December 2017 to the Ministry of Justice and Public Security (in Norwegian only).
https://www.norges-bank.no/Publisert/Brev-oguttalelser/2017/2017-12-12-brev/

Norges Bank (2018a): "Letter of 7 February 2018 to the Ministry of Finance".

Norges Bank (2018b): "Letter of 20 February 2018 to Finanstilsynet".

Norges Bank (2018c): "Retail payment services 2017". *Norges Bank Papers* 2/2018.

Norges Bank (2018d): "Central bank digital currencies". *Norges Bank Papers* 1/2018.

Norges Bank (2018e): "Revised terms and conditions for account management at Norges Bank (NBO)". *Circular* 2/2018.
https://www.norges-bank.no/en/Published/Circulars/2018/2-account-management/

Norwegian Ministries (2012): "Cyber Security Strategy for Norway".
https://www.regjeringen.no/globalassets/upload/fad/vedlegg/ikt-politikk/cyber_security_strategy_norway.pdf

NSM (2017): "Helhetlig IKT-risikobilde 2017" [Overall assessment of ICT risk 2017], *National Security Authority Report*, 27 September 2017 (in Norwegian only).
https://nsm.stat.no/aktuelt/helhetlig-ikt-sikkerhet-2017/

Ripple (2017): "Japan Bank Consortium Moves to Become Production-ready", 5 December 2017.
https://ripple.com/insights/japan-bank-consortium-moves-become-production-ready/

Solberg, E. (2018): "Nasjonal strategi for IKT-sikkerhet" [National strategy for ICT security], Speech, 6 March 2018, Oslo (in Norwegian only).
https://www.regjeringen.no/no/aktuelt/nasjonal-strategi-for-ikt-sikkerhet/id2592996/

VPS (2018): "Changes to the VPO NOK Rules from 18 May 2018".
https://www.vps.no/pub/changes-to-the-vpo-nok-rules-from-18-may-2018/?lang=en

## LEGISLATION

Central Securities Depository Act. Act No 64 of 5 July 2002 on the registration of financial instruments (in Norwegian only). https://lovdata.no/dokument/NL/lov/2002-07-05-64
https://lovdata.no/dokument/NL/lov/2002-07-05-64

Norges Bank Act. Act No 28 of 24 May 1985 on Norges Bank and the Monetary System, etc.
https://www.norges-bank.no/en/about/Mandate-and-core-responsibilities/Legislation/Norges-Bank-Act/

Payment Systems Act. Act No 95 of 17 December 1999 relating to payment systems, etc
https://www.norges-bank.no/en/about/Mandate-and-core-responsibilities/Legislation/Act-relating-to-Payment-Systems-etc/

Securities Settlement Regulation. Regulation No 1095 of 22 September 2016 on the execution of securities settlement] (in Norwegian only).
https://lovdata.no/dokument/SF/forskrift/2016-09-22-1095

## EU DIRECTIVES AND REGULATIONS

Central Securities Depository Regulation (CSDR). Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012.
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R0909

European Market Infrastructure Regulation (EMIR). Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories.
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32012R0648

Regulation on EMIR. Regulation (EU) 2016/1178 of 10 June 2016 supplementing Regulation (EU) No 648/2012 of the European Parliament and of the Council with regard to regulatory technical standards on the clearing obligation.
http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R1178

Revised Payment Services Directive (PSD2). Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2366

# Annex[1]

## **Table 1:** Average daily turnover in clearing and settlement systems (transactions)

| | 2001 | 2002 | 2003 | 2004 | 2005 | 2006 | 2007 | 2008 | 2009[3] | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **NICS** | | | | | | | | | | | | | | | | | |
| NICS Gross | 303 | 300 | 596 | 611 | 532 | 547 | 593 | 605 | 524 | 568 | 548 | 594 | 659 | 624 | 772 | 980 | 1 021 |
| NICS SWIFT Net[1] | 4 719 | 4 925 | 5 155 | 4 480 | 4 744 | 5 301 | 5 908 | 6 390 | 6 269 | - | - | - | - | - | - | - | |
| NICS Net (million)[2] | 3.4 | 3.7 | 4.0 | 4.3 | 4.7 | 5.1 | 5.5 | 5.9 | 6.5 | 6.8 | 7.2 | 7.8 | 8.2 | 8.7 | 9.1 | 9.5 | 9.9 |
| **NBO** | | | | | | | | | | | | | | | | | |
| Total number of transactions | | | | | | | | | 1 165 | 1 146 | 1 138 | 1 274 | 1 406 | 1 367 | 1 565 | 1 835 | 1 958 |
| RTGS Gross transactions excl. NICS | | | | | | | | | 463 | 477 | 479 | 549 | 595 | 592 | 658 | 700 | 793 |

1 Phased out in June 2010.
2 Previous NICS Retail and NICS SWIFT Net payments below NOK 25m are included as from June 2010 in NICS Net..
3 For NBO, the figures for 2009 are calculated for the period 17 April to 31 December. There is a break in the series this year.

Sources: The figures under NICS are from the NICS Operations Office. The figures under NBO are from Norges Bank

1 For tables showing developments in retail payment services, see *Norges Bank Papers* 2/2018.

## **Table 2:** Average daily turnover in clearing and settlement systems (in billions of NOK)

| | 2001 | 2002 | 2003 | 2004 | 2005 | 2006 | 2007 | 2008 | 2009[3] | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **NICS** | **211.4** | **212.5** | **248.7** | **195.7** | **200.8** | **224.8** | **254.5** | **246.6** | **213.1** | **196.5** | **221.4** | **247.8** | **253.5** | **262.8** | **285.9** | **284.1** | |
| NICS Gross | 151.2 | 149.5 | 187.8 | 129.4 | 135.5 | 155.3 | 176.8 | 165.9 | 124.1 | 107.2 | 119.1 | 138.6 | 136.0 | 140.9 | 160.1 | 158.7 | 163.3 |
| NICS SWIFT Net[1] | 16.1 | 16.2 | 12.6 | 5.2 | 5.7 | 6.7 | 7.6 | 7.3 | 6.1 | - | - | - | - | - | - | - | |
| NICS Net[2] | 44.1 | 46.8 | 48.3 | 61.1 | 59.6 | 62.8 | 70.1 | 73.4 | 82.9 | 89.3 | 102.3 | 109.2 | 117.5 | 121.9 | 125.8 | 125.4 | 133.7 |
| | | | | | | | | | | | | | | | | | |
| **NBO** | **172.1** | **169.2** | **206.8** | **152.3** | **160.8** | **185.2** | **226.1** | **224.9** | **168.4** | **162.2** | **172.1** | **201.9** | **188.3** | **198.0** | **219.3** | **221.2** | **235.8** |
| NICS Gross | 150.7 | 149.5 | 187.7 | 128.9 | 135.5 | 155.3 | 180.2 | 163.9 | 113.2 | 106.3 | 119.0 | 137.7 | 135.2 | 140.8 | 157.5 | 156.1 | 159.0 |
| RTGS Gross transactions excl. NICS | 6.9 | 4.8 | 7.2 | 11.1 | 12.1 | 16.1 | 31.1 | 45.6 | 40.2 | 42.5 | 42.4 | 51.1 | 38.5 | 42.5 | 46.0 | 49.0 | 42.1 |
| NICS SWIFT Net[1] | 5.3 | 5.5 | 2.1 | 1.0 | 0.9 | 1.0 | 1.2 | 1.1 | 0.9 | 1.1 | - | - | - | - | - | - | |
| NICS Net[2] | 6.8 | 6.9 | 6.7 | 7.6 | 8.5 | 8.1 | 8.1 | 9.2 | 9.6 | 7.1 | 6.3 | 8.7 | 10.3 | 10.8 | 11.9 | 12.4 | 13.1 |
| VPO and Oslo Clearing[4] | 2.3 | 2.5 | 3.1 | 3.7 | 3.8 | 4.7 | 5.5 | 5.1 | 4.5 | 5.3 | 4.5 | 4.4 | 4.2 | 3.9 | 3.8 | 3.7 | 4.2 |
| VPO | | | | | | 4.4 | 5.1 | 4.9 | 4.4 | 5.2 | 4.5 | 4.4 | 4.2 | 3.9 | 3.8 | 3.6 | 4.2 |
| Oslo Clearing | | | | | | 0.3 | 0.4 | 0.3 | 0.1 | 0.1 | 0.1 | 0.0 | 0.0 | 0.1 | - | 0.0 | 0.0 |

1 Phased out in June 2010.
2 Previous NICS Retail and NICS SWIFT Net payments below NOK 25m are included as from June 2010 in NICS Net.
3 For NBO, the figures for 2009 are calculated for the period 17 April to 31 December. There is a break in the series this year.
4 From May 2015, legally integrated with SIX x-clear.
5 See note 4.

Sources: The figures under NICS are from NICS Operations Office. The figures under NBO are from Norges Bank

## **Table 3:** Number of participants in clearing and settlement systems (at year-end)

| | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Norges Bank's settlement system (NBO): Banks with account in Norges Bank | **145** | **142** | **143** | **140** | **134** | **129** | **130** | **128** | **131** | **129** | **130** | **135** |
| Norges Bank's settlement system (NBO): Banks with retail net settlement in Norges Bank | 23 | 23 | 22 | 21 | 21 | 21 | 22 | 22 | 21 | 22 | 22 | 21 |
| DNB | 104 | 103 | 103 | 106 | 105 | 103 | 98 | 98 | 97 | 94 | 94 | 93 |
| SpareBank 1 Midt-Norge | 17 | 18 | 16 | 16 | 13 | 12 | 11 | 11 | 11 | 11 | 11 | 11 |
| Norwegian Interbank Clearing System (NICS) | 146 | 146 | 143 | 145 | 142 | 138 | 132 | 131 | 130 | 128 | 128 | 125 |

Source: Norges Bank

NORGES BANK
Bankplassen 2, P.O. Box 1179 Sentrum, N-0107 Oslo
www.norges-bank.no