REPORT

DANMARKS NATIONALBANK

5 MAY 2020 — NO. 3

Oversight of the financial infrastructure

- Denmark has a modern, efficient and resilient payments infrastructure. Danmarks Nationalbank considers that the infrastructure largely complies with the requirements of international standards for organisation, risk management and crisis response.
- Across infrastructure systems and solutions, there is a strong management focus on strengthening cyber resilience. The level of maturity of this work has increased in recent years with strengthened risk management and participation in the so-called TIBER-DK cyber tests.
- Part of the work regarding cyber resilience takes place at sector level. FSOR's (Financial Sector Forum for Operational Resilience's) risk analysis runs in parallel with the risk work undertaken by the individual actors, and FSOR's crisis response ensures coordination between everyone involved. During the COVID-19 pandemic, the crisis response has been used to obtain information and for knowledge sharing.

CONTENT

2 A MODERN AND RESILIENT PAYMENTS INFRASTRUCTURE

7 INTERBANK PAYMENTS

10 RETAIL PAYMENTS

13 CLEARING AND SETTLEMENT OF RETAIL PAYMENTS

16 SECURITIES SETTLEMENT

20 PAYMENTS AND SECURITIES SETTLEMENT IN EURO

22 SETTLEMENT OF FOREIGN EXCHANGE TRANSACTIONS

Important infrastructure

Kr. 618 billion

in payments are settled each banking day on average

Read more

TIBER-DK infrastructure test

Ethical hackers

help identify areas of improvement and strengthen cyber resilience

Read more

A modern and resilient payments infrastructure

Denmark is one of the most digitised countries in the world. This also applies to the payments sector, where consumers, firms, financial institutions and public authorities send electronic payments totalling more than kr. 600 billion on an average day through the Danish payments infrastructure.

A well-functioning payments infrastructure is the backbone of the economy. If things do not work, disruption will follow, and, in the worst-case scenario, a breakdown of the payments infrastructure can threaten financial stability. That is why Danmarks Nationalbank oversees that the core systems and solutions of the infrastructure comply with international safety and efficiency standards.

This report presents the main conclusions from the oversight of the Danish payments infrastructure in 2019.

The Danish payments infrastructure is described in Box 1.

Danmarks Nationalbank's oversight

Danmarks Nationalbank oversees that payments and financial transactions in Denmark can be effected in a safe and efficient manner. Its oversight comprises the core systems and solutions in the Danish payments infrastructure:

1. Kronos2 (interbank payments)
2. the Sumclearing, Intradagclearing and Straksclearing (retail payments)
3. the VP settlement system (securities transactions)
4. Dankort, Betalingsservice and credit transfers (the most important payment solutions)
5. International systems of relevance to Denmark.

Danmarks Nationalbank's oversight is based on international standards and guidelines and is described in its oversight policy (*link*).

International standards are extensively complied with

Denmark has a modern, efficient and resilient payments infrastructure. That is the conclusion of Danmarks Nationalbank's oversight.

Infrastructure systems and solutions run smoothly and there are rarely any disruptions in the exchange of payments and the settlement of securities and foreign exchange transactions.

The core systems/solutions comply extensively with the requirements of international standards concerning organisation, risk management and crisis response. Those responsible for the core systems/solutions are continuously working to increase resilience and comply with Danmarks Nationalbank's recommendations on how to strengthen the infrastructure.

Efforts were made in 2019 across systems and solutions to strengthen risk management and risk reporting. Here, there is a particular focus on strengthening supplier management and risk reporting from supplier to system owner. Moreover, the risks arising from interdependencies between the core infrastructure systems are now systematically incorporated into the risk management of each system.[1]

Incorporating risks from suppliers and related systems into the risk management provides a comprehensive overview and a good basis for prioritising and addressing risks. Managing both risks inflicted by others and risks inflicted on others is a key element of the CPMI-IOSCO principles. And it is key to creating a resilient interaction between infrastructure actors.

Cyber threat calls for resilient infrastructure

The threat of cybercrime continues to make increased demands on the resilience of the infrastruc-

1 Risks arising from interdependencies are identified in the Risk Forum for Interdependencies (Risikoforum for Gensidige Afhængigheder – RGA), which is a formalised cooperation between Danmarks Nationalbank, VP and Finance Denmark. For a description of the RGA, see Danmarks Nationalbank, Oversight of the Financial Infrastructure, *Danmarks Nationalbank Report*, no. 3, June 2019 (*Link*).

The Danish payments infrastructure

Box 1

Each banking day[1], payments averaging kr. 618 billion, corresponding to almost one fourth of GDP, are settled via the Danish payments infrastructure.

Danmarks Nationalbank's payment system, Kronos2, plays a central role in this infrastructure, both in relation to settlement of large, time-critical payments between banks (interbank payments) and by virtue of Danmarks Nationalbank's role as settlement bank for other payment and settlement systems. Interbank payments amounting to kr. 87 billion are settled in Kronos2 on a daily basis.

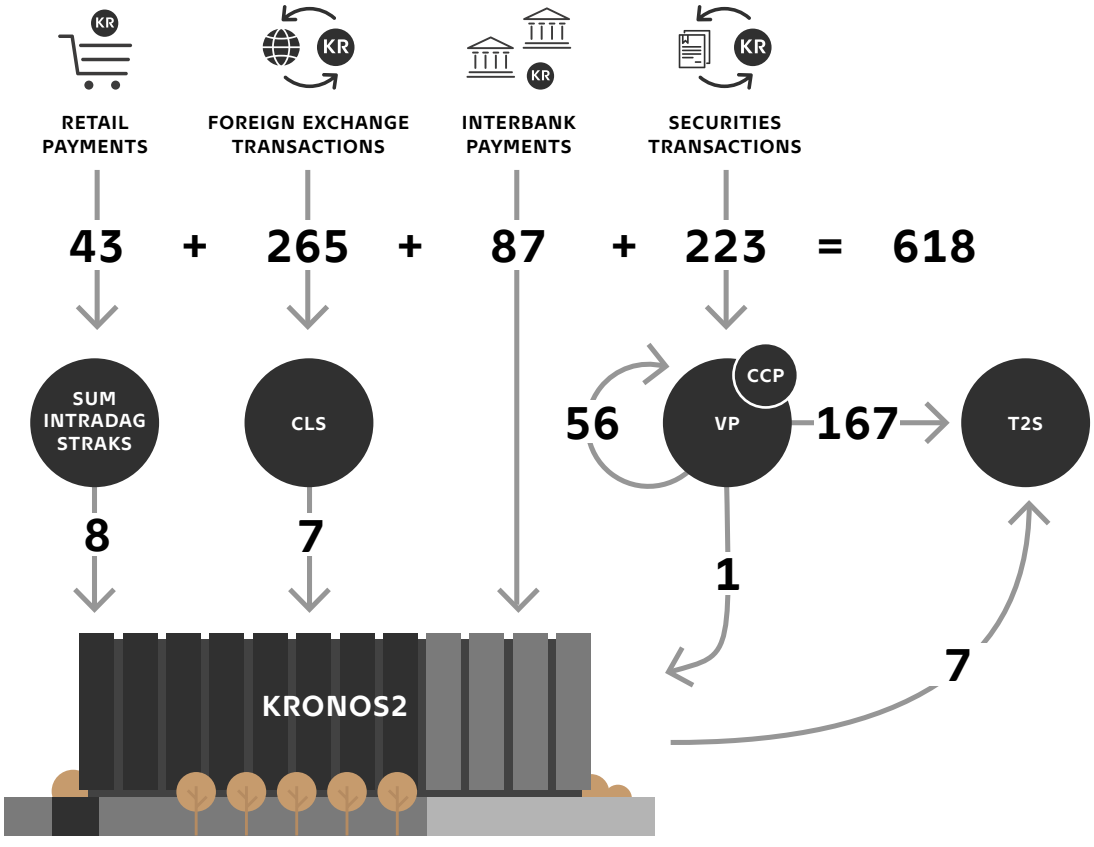
Retail payments are payments between consumers, firms and public authorities, e.g. by Dankort or as credit transfers. Depending on their type, retail payments are cleared and settled through the Sumclearing, the Intradagclearing or the Strakscleaning (retail payment systems).

Foreign exchange transactions in CLS comprise e.g. FX spot, FX forward and FX swap transactions.

Securities transactions in VP comprise trading in bonds, equities and investment fund shares. The main part of the securities settlement, equalling kr. 167 billion, takes place on the trans-European securities settlement platform, TARGET2 Securities (T2S), while the rest, i.e. kr. 56 billion, are settled via VP's own platform. Some securities transactions, such as equities transactions, are cleared via a central counterparty, CCP.

The payment and settlement systems in the infrastructure, i.e. CLS, VP and the three retail payment systems, settle their participants' net positions in Kronos2 or T2S. Net positions are calculated by offsetting participants' claims and obligations in the respective systems. This netting reduces the participants' liquidity requirement for settlement considerably compared with a situation in which all payments are settled individually. For example, netting reduces the daily liquidity requirement for settlement of retail payments from kr. 43 billion to kr. 8 billion, equivalent to a reduction of 81 per cent. Likewise, netting reduces participants' liquidity requirement for settlement on T2S from kr. 167 billion to kr. 7 billion, equivalent to a reduction of 96 per cent.

Payment flows, kr. billion, averages per banking day in 2019



1. Some types of payment can be made 24/7/365, others only during bank opening hours. But for all payments, final settlement and exchange of amounts between banks take place on banking days, i.e. when banks are open for business.

ture. Cyber resilience includes both the ability to protect systems from attack, detect possible intrusions into the systems and, not least, to be able to restore operation with correct data after a cyber attack.

Danmarks Nationalbank's oversight is continuously in dialogue with those responsible for the core infrastructure systems on their work in the cyber field. In 2019, Danmarks Nationalbank undertook assessments of the systems according to specific international guidelines that focus on cyber security, see Box 2.

Working with cyber resilience

Across infrastructure systems and solutions, there is a strong management focus on strengthening cyber resilience, and the level of maturity of this work has increased in recent years. This is reflected by the strengthened risk management and risk reporting. This involves continuous efforts to mitigate the identified risks, including cyber risks.

Part of the work to mitigate cyber risks and increase cyber resilience takes place at sector level and by participating in various sectoral collaborations as set out below.

FSOR and FSOR risk analysis

Those responsible for the core systems and solutions participate in FSOR (Financial Sector Forum for Operational Resilience), which has worked on various aspects of cyber resilience since 2016.

A methodology for ongoing risk analysis at sector level has been developed under the auspices of FSOR. The analysis provides a comprehensive overview of operational risks that could affect the entire sector and potentially threaten financial stability. Based on the risk analysis, common risks can be addressed jointly. Building on a systematic risk analysis ensures that the work undertaken is providing the greatest value.

FSOR's risk work runs in parallel with and supports the risk work of both the Risk Forum for Interdependencies (RGA) and the individual actors. For example, FSOR has a particular focus on involving the suppliers of the infrastructure. Dialogue has been initiated with the most critical suppliers to achieve a common understanding of the interdependencies and the risks that may arise in this respect. In this way, the work of FSOR supports each actor's supplier management work.

Cyber resilience assessment Box 2

Danmarks Nationalbank's assessment of the cyber resilience of the core systems is based on the CPMI-IOSCO's Guidance on cyber resilience for financial market infrastructure (CPMI-IOSCO's cyber guidance).[1]

The CPMI-IOSCO's cyber guidance was published in 2016 and is a set of guidelines that elaborates on CPMI-IOSCO's Principles for financial market infrastructures from 2012 – in particular concerning principle 2 (governance), principle 3 (framework for the comprehensive management of risks) and principle 17 (operational risk).

The guidelines are divided into five main areas:
1. organisation and management
2. identification of risks
3. protection against attacks
4. detection of attacks
5. restoration of normal operation.

In addition, there are three cross-cutting areas comprising testing, learning and development as well as awareness-raising.

In 2018, the ECB announced its expectations for cyber resilience in critical infrastructure in Cyber resilience oversight expectations (CROE).[2] CROE complements the CPMI-IOSCO's cyber guidance and is used by the ECB in its assessments of the Eurosystem's critical infrastructures.

CROE can be a useful guide to how the cyber resilience of Danish systems can be strengthened while ensuring a high level of compliance with the CPMI-IOSCO cyber guidance.

1. CPMI-IOSCO, Guidance on cyber resilience for financial market infrastructures (*Link*).
2. ECB, Cyber resilience oversight expectations (*Link*).

FSOR's risk analysis has led to the creation of a unique connection between the risk work of the individual actors and the risk work undertaken by the RGA and at sector level. This means that risks can be addressed at multiple levels at the same time. FSOR also has the possibility to escalate risks to national level if they relate to several sectors that are critical to society and are as such best addressed at national level. FSOR risk analysis is – as far as is known – the first of its kind in the world.

TIBER-DK

Testing is an important tool in strengthening cyber security. By continuously testing systems, procedures and plans, specific areas of potential for improve-

ment are identified. Those responsible for the core infrastructure systems and solutions participate in TIBER-DK, a Danish Threat Intelligence Based Ethical Red-teaming test programme, see Box 3. In a TIBER test, a simulated cyber attack is launched against participants' live systems to detect and correct vulnerabilities before they are exploited by cyber criminals.

NFCERT and CIISI-EU

Knowledge sharing is another important element in the fight against cybercrime. The core infrastructure systems/solutions are all part of Nordic Financial CERT, NFCERT, a joint Nordic sectoral collaboration on the collection and sharing of information on cyber threats and cyber attacks.[2] Knowledge sharing is intended to strengthen the ability to detect, prevent and respond more quickly to a cyber attack. NFCERT also offers expert assistance in the event of a cyber attack.

Danmarks Nationalbank also participates in CIISI-EU (Cyber Information and Intelligence Sharing Initiative), a new public/private knowledge-sharing initiative between key financial actors in Europe, Europol and the European Union Agency for Cybersecurity (ENISA). The initiative has common features with NFCERT, but in some respects has a greater scope.

FSOR crisis response

FSOR has established the crisis response plan for the Financial Sector which can be activated in the event of serious operational incidents such as a cyber attack. The purpose of the crisis response plan is to ensure coordinated action across the sector, just as it liaises with NOST, the National Operative Staff, to coordinate efforts that are critical to society.

The crisis response is tested several times a year. It allows participants, including those responsible for the critical systems/solutions, to test and improve their own crisis response.

During the COVID-19 pandemic, FSOR crisis response has been effective in ensuring knowledge sharing and coordination between NOST and the financial sector. Information from NOST has been shared with FSOR members twice weekly via a virtual platform, and information on the employee situation in the critical infrastructure functions has been obtained daily and passed on to NOST.

Infrastructure development

The payments infrastructure is continuously modernised and developed. In 2018, Danmarks Nationalbank implemented a new, up-to-date RTGS system, Kronos2, and the settlement of securities transactions in Danish kroner was connected to TARGET2-Securities (T2S). On the euro side, the ECB has been working since 2016 to consolidate T2S, TARGET2 and TIPS on a common platform.

TIBER-DK Box 3

Danmarks Nationalbank is the authority for the TIBER-DK programme (Threat Intelligence Based Ethical Red-teaming) and has developed the TIBER-DK framework based on the TIBER-EU in close cooperation with the Danish financial sector.

The framework describes how participants can identify vulnerabilities in their critical functions in an ethical, sound and consistent way in order to learn how to improve cyber resilience. As knowledge sharing among the participants is an integral part of the TIBER-DK framework, the participants will learn from both their own and others' tests.

The TIBER-DK test targets the functions that are critical both for the individual participant and for society, and the test covers people, processes and systems. In the test, a red team (hacker team) conducts controlled, simulated attacks on these live critical functions. The attacks are realistic as they are based on intelligence-based threat data and mimic current threat actors and their tactics, techniques and procedures.

In the preparation and performance of a TIBER-DK test, the focus is on risk management to ensure that the tests are carried out in a responsible manner. Similarly, the TIBER-DK framework comprises instructions on how to maintain the confidentiality of the test and results.

The TIBER-DK programme tests the largest financial institutions, infrastructure companies and data centres in Denmark.

2 NFCERT has participants from all five Nordic countries. Most Norwegian and Danish banks participate in NFCERT.

In 2019, the Danish retail payment systems were also brought into play: In the short term, Mastercard has plans to buy, among other things, Betalingsservice and the retail payment systems from Nets. At the same time, a number of Nordic banks are working to establish P27, a new common infrastructure for clearing and settling retail payments in and between Denmark, Sweden and Finland.

In April 2020, Euronext entered into an agreement with VP Securities' (VP's) largest shareholders to acquire a majority of the shares of VP.

The different projects are described in more detail in the sections below on oversight of individual payment and settlement systems.

Interbank payments

Interbank payments are payments between financial institutions. Such payments are typically characterised by being time-critical and of high value. They are settled in real-time gross settlement, RTGS systems, which settle payments individually and immediately.

Kronos2 is Danmarks Nationalbank's RTGS system for interbank payments in Danish kroner. Kronos2 settles not only interbank payments but also monetary policy operations and net positions from connected payment and settlement systems.

Use

There are 94 direct Kronos2 participants, mainly Danish banks, mortgage banks and branches of foreign banks.

In 2019, an average of approximately 5,800 daily interbank payments with a total value of kr. 87.4 billion were settled in Kronos2, see Table 1.

In connection with the transition to Kronos2 in August 2018, transfers to the Sumclearing, Intradagclearing and Straksclearing declined substantially, see Table 1. In 2017, kr. 273.8 billion was transferred, while in 2019 it was kr. 40.5 billion. Previously, all of the participant's disposable current account liquidity was transferred to the night-time settlements using the 'Maximum liquidity' function. Kronos2 automatically sources the necessary liquidity for the night-time settlements in the Sumclearing and Intradagclearing.

The migration of Danish kroner to TARGET2-Securities (T2S) in October 2018 has also had an impact on

Transactions in Kronos2 Table 1

Kr. billion, averages per banking day	2015	2016	2017	2018	2019
Interbank payments	**99.3**	**83.0**	**74.0**	**83.0**	**87.4**
- Of which customer payments	12.8	11.5	11.5	13.6	14.0
Monetary policy operations	**37.5**	**28.7**	**39.9**	**36.9**	**48.4**
- Of which sale of certificates of deposit	37.3	28.6	39.9	36.9	48.4
- Of which monetary policy lending	0.2	0.1	0.0	0.0	0.0
Transfers to settlement systems	**379.9**	**283.4**	**316.3**	**237.3**	**115.1**
- Of which to Sumclearing, Intradagclearing and Straksclearing	334.9	242.7	273.8	177.2	40.5
- Of which to VP settlement	35.5	31.7	32.5	40.6	46.4
- Of which to CLS	9.6	9.0	10.0	19.6	28.2
Net positions settled	**27.6**	**25.1**	**24.8**	**24.1**	**16.3**
- Of which Sumclearing, Intradagclearing and Straksclearing	7.6	7.6	8.0	8.1	8.3
- Of which VP settlement	12.7	10.6	10.1	9.1	1.0
- Of which CLS	7.2	6.9	6.7	6.8	7.0

settlement in Kronos2. Following the migration, the professional actors' settlement has been moved to T2S, while private investors' transactions continue to be settled on VP's own platform. The settlement in net positions from the VP settlement has decreased from kr. 10.1 billion in 2017 to kr. 1.0 billion in 2019.

Operational reliability
Overall, the operational reliability of Kronos2 was satisfactory in 2019. There have been few incidents caused by operational errors and the complex interaction with the other infrastructure systems. The causes of the incidents have been identified and measures have been taken to prevent their recurrence.

Liquidity
Overall, participants had ample liquidity for settlement of payments in Kronos2. Chart 1 shows the participants' excess liquidity cover.

The ample liquidity among Kronos2 participants contributes to smooth settlement of payments. A stress test analysis of liquidity based on data from Kronos during the period 2 January 2007 to 3 August 2018 shows that payment settlement and participants' liquidity were resilient towards different types of stress.[3] The liquidity in Kronos was, among other things, tested in a scenario where a large participant is removed from the payment settlement and in one where the participants' intraday credit is restricted. Data from Kronos2 show that the participants' payment behaviour has changed slightly, but there is still ample liquidity.

International standards
Danmarks Nationalbank is continuously working to comply with international standards for safe and efficient payment systems.

By conducting regular stress tests as described above, Danmarks Nationalbank complies with CPMI-IOSCO's requirement to perform stress tests on the liquidity in the system.

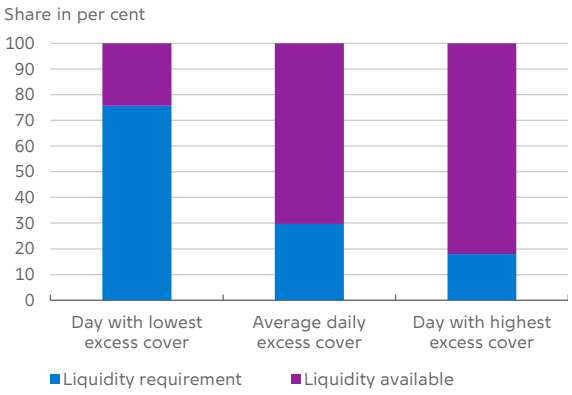
In 2019, Danmarks Nationalbank strengthened the management and reporting of risks related to Kronos2. This included introducing more systematic risk reporting and a greater focus on risks related to critical suppliers. Furthermore, risks identified in co-operation with VP and Finance Denmark have been incorporated into the risk management of Kronos2. These measures follow up on the conclusions of a review of the risk management of Kronos2 in 2018 in accordance with CPMI-IOSCO's requirements for the risk management framework.

In addition, in 2019, Danmarks Nationalbank initiated an assessment of Kronos2's observance of all CPMI-IOSCO's principles. It covers all areas of Kronos2, including the legal basis, the overall organisation and the management of all kinds of risks that may arise in connection with payment settlement in Kronos2.

Cyber resilience
Danmarks Nationalbank is continuously following developments in the threat landscape and continued to work in 2019 to strengthen cyber resilience. This includes work to meet the tightened requirements of the SWIFT Customer Security Programme (CSP) and to implement CPMI's endpoint security strategy[4].

Among other things, Danmarks Nationalbank introduced a tool to detect if a payment instruction in Kronos2 deviates from normal payment patterns.

Ample liquidity among Kronos2 participants in 2019 Chart 1



Source: Danmarks Nationalbank.

3 See Thomas Christian Nilsson, Liquidity stress test shows that Kronos is resilient, *Danmarks Nationalbank Analyse,* no. 9, May 2019 (*Link*).

4 CPMI, Reducing the risk of wholesale payments fraud related to end-point security (*Link*).

This should help reduce the risk of criminal transactions in Kronos2. In addition, security in the IT systems associated with Kronos2 has been strengthened. Danmarks Nationalbank thus complies with all requirements of SWIFT CSP and the ECB's Connectivity Guide.

Concurrently, there is an increased focus on ongoing awareness campaigns aimed at training staff in cyber and IT security. Training employees is an important element of cyber security.

Danmarks Nationalbank is also looking at the requirements for participants' endpoint security[5]. The resilience of a payment system against criminal transactions depends both on the security of the system itself and on the security of participants. Therefore, it is central to CPMI's strategy that payment system owners place appropriate requirements on participants to implement security measures at the endpoints they control.

System updates

Danmarks Nationalbank is continuously working to strengthen the resilience of its systems. Among other things, work is being undertaken to strengthen the existing Extreme Contingency solution, which ensures that the settlement of payments will continue in the event that Kronos2 is affected by a major incident or failure. It is envisaged that the solution will be tested with the financial sector in 2020.

5 A payment system is linked to other financial infrastructures, service providers and participants (i.e. banks and other financial institutions) via messaging networks. Jointly, these parties and the associated networks make up a complex 'ecosystem' for settlement of payments. In CPMI terminology, an endpoint is defined as a point in place and time at which payment instruction information is exchanged between two parties in the ecosystem.

Retail payments

Most payments between consumers and firms are made electronically with payment solutions such as Dankort, online banking transfers, Betalingsservice and MobilePay. In 2019, the daily value of electronic retail payments averaged kr. 29.1 billion.[6] Danmarks Nationalbank oversees the most important payment solutions in Denmark, see Box 4.

Operational reliability
The operational reliability of the Dankort and Betalingsservice systems was satisfactory in 2019.

However, there was one specific episode in March 2019 where an operational error affected an extensive number of Dankort payments. Payments could be made in stores, but they were not sent for clearing and settlement. That meant that about one quarter of all Dankort payments during the episode were deposited into the stores' accounts with a few days' delay. Nets subsequently ensured that the technical issues that caused the incident will not be recurring.

Nets' sale of Betalingsservice to Mastercard
In August 2019, Nets and Mastercard entered into an agreement for the purchase of, among other things, the retail payment systems and Betalingsservice by Mastercard.

The deal is subject to approval by the competition authorities. The deal has been notified to the Danish Competition and Consumer Authority (KFST), which has performed a number of investigations and has now referred the matter to the European Commission for consideration.

If the deal is approved, Nets and Mastercard will enter into a temporary service agreement to help ensure a smooth, secure and stable transfer of the operation of Betalingsservice from Nets to Mastercard. Following the acquisition, Mastercard will be able to obtain assistance from Nets for an extended period of time to ensure that Betalingsservice will run smoothly.

6 The value of the transactions in the retail payment systems as calculated per calendar day, as described in the section *Clearing and settlement of retail payments*.

Danmarks Nationalbank's oversight of payment solutions Box 4

Danmarks Nationalbank oversees the most important Danish payment solutions, currently Dankort, Betalingsservice and credit transfers.

Oversight of Dankort comprises the pure Dankort cards as well as the Dankort side of co-branded cards (primarily Visa/Dankort).

Oversight of credit transfers is part of the oversight of the retail payment systems (the Sumclearing, Intradagclearing and Straksclearing), see the section *Clearing and settlement of retail payments*.

Developments in the various payment solutions offered in the Danish market are monitored on an ongoing basis to assess whether targeted oversight of these solutions is required.

MobilePay is primarily used for transfers between private users, but also for shopping in stores, online purchases and payment of recurring invoices. Average daily turnover for MobilePay was kr. 0.3 billion in 2019.[1] By comparison, Dankort payments totalled kr. 1.1 billion per day in 2019.[2]

The new payment solutions in the Danish market, Apple Pay and Google Pay, still have only quite limited market shares.

1. MobilePay, *(Link)*.
2. Nets' statistics on fraudulent use of the Dankort, (*Link*).

Danmarks Nationalbank is following the process of Nets' sale of Betalingsservice to Mastercard. The oversight of Betalingsservice will be directed at Mastercard once the acquisition is complete.

The incidence of Dankort fraud continues to decrease

According to Nets, fraudulent use of the Dankort totalled kr. 30.9 million in 2019, corresponding to 0.08 per thousand of total consumption.[7] As a result, the positive development of recent years continues with declining incidence of fraud, see Chart 2. Fraudulent use is decreasing both online, in stores and in connection with cash withdrawals.

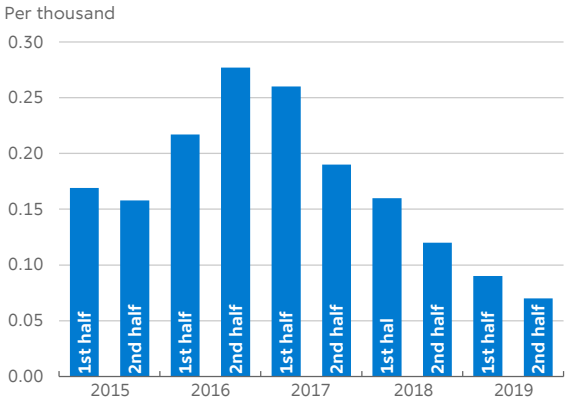
Fraudulent use of stolen or lost Dankort cards for trading in stores or withdrawing cash from ATMs has decreased by 25 per cent since the 2nd half of 2018 to 0.049 per thousand in the 2nd half of 2019.[8]

The police and Nets are working to prevent fraudulent use of stolen cards. Together, Nets and the police have identified the places and times where the risk of having your card and PIN stolen is at its highest. This information is used in conjunction with Nets' surveillance system that will trigger an alarm if an unusual pattern is detected in the use of a card.

According to Nets, use of contactless payments may also have contributed to reducing fraud. Today, three out of four payments using the Dankort are contactless.[9] As the PIN does not need to be entered for contactless payments below kr. 350, no-one can watch the cardholder enter it.

The incidence of fraudulent use of the Dankort on websites has declined by 62 per cent from the 2nd half of 2018 to the 2nd half of 2019 to 0.14 per thousand.[10]

Fraudulent use as a share of total Dankort-based consumption Chart 2



Note: Fraudulent use is calculated on a half-yearly basis.
Source: Nets.

This type of fraudulent use typically takes place by the criminal getting hold of the card details digitally (card number and accompanying CVV/CVC code). This may happen if, for example, a web shop is subjected to a hacker attack where card details are copied.

Nets considers the decrease in fraudulent use in online shopping to be attributable to primarily two factors. Firstly, the security solution Dankort Secured by Nets is increasingly used. With this solution, the user in online transactions must not only state the Dankort details but also enter a code sent by SMS from Nets before purchases exceeding kr. 450 can be completed. Secondly, Nets has made improvements to its surveillance system which warns of and rejects suspicious transactions.

7 Nets' statistics on fraudulent use of the Dankort, (*Link*).
(Note: Nets' data for fraudulent use is not directly comparable with Danmarks Nationalbank's statistics of fraudulent use of payment cards, which cover both Dankort and international cards used in Denmark.)

8 Nets' statistics on fraudulent use of the Dankort, (*Link*).

9 Fraudulent use of the Dankort almost halved in a year, 28 April 2020 (in Danish) (*Link*).

10 Nets' statistics on fraudulent use of the Dankort, (*Link*).

International standards

In 2019, Danmarks Nationalbank made an assessment of Betalingsservice's observance of the ECB's standards for direct debit schemes.[11] The assessment showed that Betalingsservice largely complies with the requirements set by the ECB, but that there is also potential for improvement in certain areas. Nets has subsequently addressed all recommendations and remarks in the assessment.

Against this background, Nets has strengthened the management and operation of Betalingsservice in several respects:

- Enhanced processes, organisation and reporting have been established in the compliance field.
- Regulatory changes have been made to ensure that firms' payment fees become more clear to consumers.
- The process of identifying and assessing financial risks for creditors and financial institutions has been extended.
- A dedicated and unified system for IT risk management is being implemented.
- A monitoring solution that ensures speedier alert and response in the event of suspicious activity in systems or networks is being implemented.
- The response and risk management have been strengthened based on the experience gained in connection with major incidents in and attacks on other companies.
- The focus on and requirements for the risk management of critical suppliers have been tightened.

Regulation

The EU Payment Services Directive (PSD2) was implemented in Danish law by the Payments Act on 1 January 2018. Among other things, PSD2 aims to make electronic payments more secure and to enhance competition in the EU payments market. However, many of the most important provisions only took effect in their final formulation from 14 September 2019 when the EU Regulation on strong customer authentication and common and secure open standards of communication entered into force.

This legislation introduces, among other things, new payment services – payment initiation services and account information services. The banks must, among other things, be ready with technical solutions allowing customers to make payments via a payment initiation service provider in the market without any agreement existing between the bank and the service provider in question.

As regards the requirements for strong customer authentication[12], the European Banking Authority (EBA) has chosen to allow an extended implementation period of 15 months, which runs from 14 January 2019 to 31 December 2020. The extension, which only applies to online card payments, is intended to ensure that the transition to the new requirements will not lead to major disruption to e-commerce in the EU.

In Denmark, PSD2 has, among other things, included continued work on the roll-out of Dankort Secured by Nets in the Danish web shops to comply with the requirement of strong customer authentication for payments. At the beginning of 2019, Dankort Secured by Nets was used for 15 per cent of total turnover using Dankort online. By early 2020, this figure had risen to 30 per cent.

For Betalingsservice, PSD2 has meant that strong customer authentication has been introduced when consumers set up payment agreements through their bank or Nets.

11 Danmarks Nationalbank, Betalingsservice Assessment, *Danmarks Nationalbank Report*, no. 4, October 2019 (*Link*).

12 I.e. two-factor authentication such as Dankort Secured by Nets.

Clearing and settlement of retail payments

Retail payments in Danish kroner are cleared and settled in the Sumclearing, Intradagclearing and Straksclearing, also known as the retail payment systems. The systems are owned by Finance Denmark, managed by e-nettet and operated by Nets.

The Sumclearing is used for clearing of Dankort and Betalingsservice payments once a day on banking days. The Intradagclearing is used for clearing of credit transfers such as online banking transfers, payroll transactions and public sector payments. At fixed times, the systems calculate the participants' net positions, corresponding to the sum of payments to and from the banks' customers. The net positions are sent to Kronos2, which exchanges the amounts between the banks.

In the Straksclearing, credit transfers are executed in a matter of seconds 24/7. This is possible because the banks in advance reserve liquidity in Kronos2 for the transfers. The actual exchange of liquidity between the banks takes place six times a day on banking days. The Straksclearing is used primarily for online banking transfers and payments via MobilePay.

Use

There are 53 direct participants in the retail payment systems and 29 indirect participants, who settle via direct participants. The value of transactions in the systems averaged kr. 42.9 billion per banking day in 2019, see Table 2.

The number of transactions in the Straksclearing has continued to rise, see Chart 3.[13] One reason is that transactions in MobilePay are cleared in the Straksclearing. Figures show that MobilePay is used by more than four million Danes.[14]

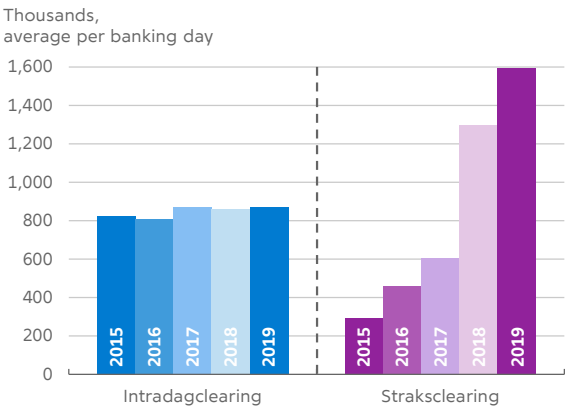
Although there has been an increase in the number of transactions in the Straksclearing, the total value

Value of transactions in the Sumclearing, Intradagclearing and Straksclearing Table 2

Kr. billion, average per banking day	2015	2016	2017	2018	2019
Sumclearing	16.7	17.2	17.8	19.8	20.7
Intradagclearing	17.8	18.4	19.7	20.1	20.8
Straksclearing	0.6	0.8	0.9	1.2	1.4
Total	35.1	36.4	38.4	41.1	42.9

Source: Nets.

Number of transactions in Intradagclearing and Straksclearing, 2015-19 Chart 3



Source: Nets.

13 The number and value of transactions in the Straksclearing are not equal to the volume of payments. For example, a MobilePay payment may entail two transactions in the retail payment systems.

14 MobilePay, (*Link*).

of these transactions is still low, see Table 2. This is because the Straksclearing is primarily used to transfer small amounts. Approximately 45 per cent of transactions in the Straksclearing have a value of less than kr. 100, whereas transactions in the Intradagclearing are typically somewhat larger, see Chart 4.

Operational reliability
The retail payment systems' operations were satisfactory in 2019. Compared to previous years, there have been significantly fewer incidents in the systems and there have been no major incidents that Danmarks Nationalbank has followed up on.

Liquidity
Participants reserve liquidity in accounts at Danmarks Nationalbank for settlement of their net positions in the retail payment systems. If a participant does not reserve sufficient liquidity, its settlement is postponed, and new net positions are calculated for the other participants, who risk not receiving the expected liquidity.

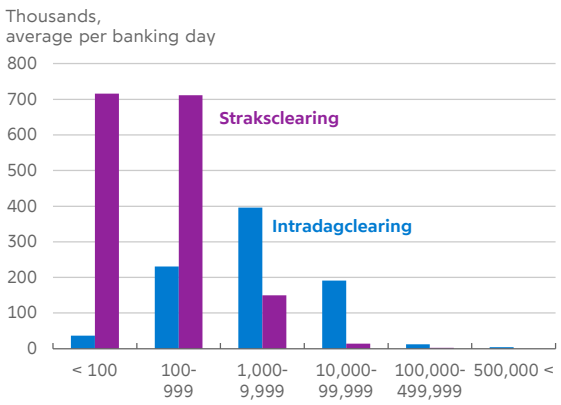
In 2019, there were only three cases where a participant's settlement was postponed due to a lack of liquidity. This is partly because most of the participants use the automated liquidity management tools in the systems.

International standards
In 2018, Danmarks Nationalbank published an assessment of the retail payment systems observance of the CPMI-IOSCO principles.[15] Finance Denmark has in 2019 complied with the recommendations made by Danmarks Nationalbank in the assessment.

Supplier management has been strengthened and additional and stricter operational and IT security requirements have been imposed, including a two hour recovery time objective for the safe resumption of critical operations following disruptive events.

A more systematic risk reporting has been established from Nets to Finance Denmark, and it is ensured that risks are reported to relevant management levels.

Number of Intradagclearing and Straksclearing transactions by amount, 2019 Chart 4



Note: Straksclearing has a limit of kr. 500,000 per transaction.
Source: Nets.

In addition, Finance Denmark conducts regular tests of contingency plans and default procedures, just as it has recently performed a stress test to gain insight into the liquidity risks that may arise if settlement is postponed for one or more participants.

Danmarks Nationalbank has initiated an assessment of the retail payment systems observance of the CPMI-IOSCO's cyber security guidance, which elaborates on the cyber security aspects of the CPMI-IOSCO principles. This work is based on Finance Denmark's self-assessment of the systems.

System updates
Work is ongoing to strengthen the resilience of the retail payments infrastructure.

The financial sector has, among other things, established a new data network for the clearing and settlement of retail payments, called e-connect. The network is provided by TDC and must meet high standards for safety, redundancy and operational reliability. Migration of network traffic of the retail payment systems to e-connect was completed in mid-2019.

15 Danmarks Nationalbank, Assessment of the Danish retail payment systems, *Danmarks Nationalbank Report*, no. 5, May 2018 (*Link*).

In the past, there have been examples of incidents in the night-time settlement that have significantly delayed entry to customers accounts. Against this background, the sector is working to adjust the settlement, so that – in the event of an incident – the settlement cycles at 3:00 am and 6:00 am can be settled manually and therefore earlier. This will give the data centres more time to complete their book-entry before the start of the day. The solution is expected to be implemented by mid-2020.

Nets' sale of the retail payment systems to Mastercard

In August 2019, Mastercard and Nets entered into an agreement for Mastercard's purchase of, among other things, Nets' retail payment systems. The deal is subject to approval by the competition authorities before it can be considered final.

If the deal is approved, Mastercard will in the future replace Nets as the supplier of the retail payment systems. In connection with the deal, an agreement will be concluded between Mastercard and Nets, which will enter into force on the day of the acquisition, and which obliges Nets to operate clearing-related systems for an extended period of time until the operation has been migrated to Mastercard. In the short term, Mastercard therefore plans to continue operating at IBM's and Nets' data centres in Denmark and Norway, respectively.

Both Danmarks Nationalbank and the system owner, Finance Denmark, as well as Nets and Mastercard focus on ensuring that the operations are not interrupted when the retail payment systems are transferred to Mastercard.

P27 – common retail payment system for Denmark, Sweden and Finland

Throughout 2019, a number of Nordic banks collaborated on the establishment of a new Nordic infrastructure for clearing and settlement of retail payments in and between Denmark, Sweden and Finland.[16] The collaboration is called P27, referring to the fact that there are approximately 27 million inhabitants in the Nordic region.

According to P27, economies of scale can be achieved by sharing a single platform, just like a common system will pave the way for shared products across the Nordic region. At the same time, the system may result in more efficient cross-border payments.

The ambition for the banks behind the initiative is for P27 to eventually replace the national retail payment systems in Sweden, Finland and Denmark, including the Danish retail payment systems. The banks have established a company in Sweden with branches in Denmark and Finland to operate P27. In addition, the banks have chosen Mastercard as the supplier responsible for the development and operation of the system.

As things stand today, Danmarks Nationalbank has oversight and supervisory powers vis-à-vis Finance Denmark, which owns the systems, while the Danish Financial Supervisory Authority performs IT supervision of Nets, which is responsible for the operation of the systems. Both authorities are following the project closely and are in dialogue with P27 to ensure that there will be adequate oversight and supervision of clearing and settlement of Danish retail payments in the future.

In addition, the project is being discussed with the Nordic central banks and financial supervisory authorities, where they are, among other things, examining the possibility of establishing a Nordic cooperation on oversight and supervision of P27.

Finance Denmark and the sector are examining how to time the settlement for P27 and the current retail payment systems if both systems settle in Kronos2. This work includes looking into liquidity management and data centres' capacity.

16 The banks behind the initiative are Danske Bank, Nordea, Handelsbanken, SEB, Swedbank and OP Financial Group. DNB was part of the initiative but withdrew with the Norwegian sector from the project in March 2019.

Securities settlement

VP settlement is the Danish securities settlement system for securities trading. VP Securities A/S, VP, also undertakes registration of ownership of securities and handling of periodic payments, issues, redemptions etc.

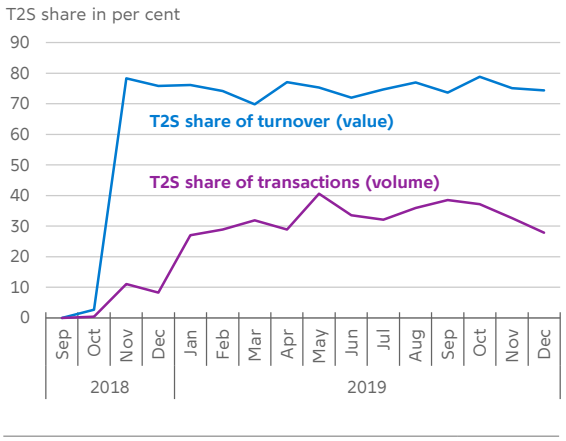
Sale of the majority share in VP to Euronext
In April 2020, Euronext N.V. and the five largest shareholders in VP, including Danmarks Nationalbank, entered into the agreement that Euronext acquires approximately 70 per cent of VP's share capital with the intention of gaining full ownership. The agreement is contingent upon the approval of the Danish Financial Supervisory Authority in accordance with the Central Securities Depositories Regulation, CSDR. The transaction is expected to be completed at the beginning of the third quarter of 2020.

Euronext is a pan European stock exchange and market infrastructure group with a number of corporations in European countries. Euronext acquired the Oslo Stock Exchange and the Norwegian Securities Depository in June 2019. In selling the shareholding, Danmarks Nationalbank emphasized that Euronext is, from a financial stability point of view, an owner who can develop VP and ensure harmonized and competitive securities management services in Denmark.

VP continues as a Danish company regulated according to CSDR under the supervision of the Danish Financial Supervisory Authority, while Danmarks Nationalbank oversees VP and is, in relation to CSDR, a so-called relevant authority.

Use
In October 2018, Danish kroner migrated to the European securities platform TARGET2-Securities (T2S). Following this, VP's settlement of securities transactions between participants has taken place on T2S, while private investors' securities transactions are still settled on VP's own platform.[17] Approx. 33 per cent of transactions and 75 per cent of the value is settled on T2S, see Chart 5. It is thus primarily large transactions that are settled via T2S.

Settlement share on T2S Chart 5



Source: VP.

The VP settlement system has 119 participants, of which 57 are non-resident market participants. Securities transactions totalling an average of kr. 223.4 billion per banking day were settled in 2019, cf. Table 3. This equals an increase of 32.5 per cent relative to 2018 driven by growth in the settlement of bond transactions.

Operational reliability
The operational reliability of the VP settlement system was satisfactory in 2019. However, there have been a few incidents which have affected the interaction between T2S, VP and Danmarks Nationalbank's systems. VP has followed up on all incidents and implemented measures to reduce the risk of recurrence. This has been done in cooperation with T2S and Danmarks Nationalbank, where appropriate.

In March, there were delays in securities settlement due to a communication failure in Danmarks Nationalbank's Kronos2. The failure was corrected, and VP settled all trades within the monetary policy day.

17 See Danmarks Nationalbank, Oversight of the financial infrastructure, *Danmarks Nationalbank Report*, no. 3., June 2019, page 15, for a more detailed description of VP settlement on T2S. (*Link*).

Equities, investment fund shares and bonds settled in VP, averages per banking day Table 3

Year, average per day	Total		Bonds		Equities		Investment fund certificates	
	Number of transactions, thousand	Value, kr. billion.	Number of transactions, thousand	Value, kr. billion.	Number of transactions, thousand	Value, kr. billion.	Number of transactions, thousand	Value, kr. billion.
2015	67.1	206.2	3.4	158.5	33.4	41.4	30.2	6.3
2016	63.6	175.9	2.8	131.8	30.9	37.6	29.9	6.6
2017	66.9	162.7	2.7	118.4	32.4	36.6	31.8	7.7
2018	65.5	168.5	2.6	119.0	29.4	40.8	33.5	8.8
2019	67.1	223.4	4.2	180.9	33.0	34.9	29.8	7.6

Note: Values have been calculated on the basis of the securities leg of a trade, i.e. the market value of the securities transferred from the seller to the buyer.
Source: VP.

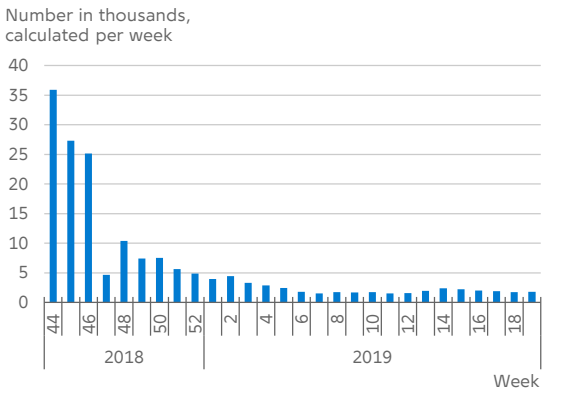
In April, T2S had to postpone the night-time settlement due to a collateral failure. The postponement delayed the settlement in VP and affected the handling of collateral in Kronos2. T2S quickly corrected the failure and has strengthened its emergency procedures to be able to deal with similar incidents more quickly.

In December, a system adjustment in VP's systems resulted in miscommunication between VP and Danmarks Nationalbank's portfolio system. Due to this failure, the portfolio system did not record collateral correctly. VP corrected the failure on the same day.

Unmatched trades
Before a trade can be settled, VP must receive and match instructions from the two parties concluding the trade. With many thousands of trades every day, there will always be a small number of trades that cannot be matched because the parties' instructions are not consistent. The parties may, for example, have different views on the terms of the trade, or one of the parties' instructions may be incorrect.

The migration of Danish kroner to T2S also required adjustments to the instructions format. Not all participants adjusted the format correctly, which meant that many instructions could not be matched during the period immediately after the migration. VP and the participants managed to adjust the format and handle the many unmatched trades. The number of unmatched trades was normalised and returned to a low level during the first quarter of 2019, see Chart 6.

Normalisation of unmatched trades Chart 6



Source: VP.

Settlement ratio
According to Article 5 of CSDR, securities transactions must be settled two days after the transaction date. The settlement ratio indicates the percentage of the transactions settled in a timely manner.

Since the second quarter of 2019, the settlement ratio for transactions settled in T2S and on the VP

platform has stabilised at the level of VP's settlement ratio from before the migration of Danish kroner to T2S in 2018, see Chart 7.

Liquidity
When a participant has insufficient liquidity in its securities settlement account, one or more transactions cannot be executed. This may cause problems for that participant's counterparties, which may not be able to meet their obligations as a result. A sanctioning system can help to discipline participants so that they make sufficient liquidity available for settlement.

A pan-European penalty system is being developed on the T2S platform to issue sanctions in case of transactions not settled in a timely manner due to a lack of securities or liquidity. The new penalty system has been delayed and is now expected to be operational in February 2021. VP is envisaging that the new system will replace the current penalty system on the VP platform to follow the pan-European standard.

International standards
In connection with Danmarks Nationalbank's assessment of the VP settlement system's observance of the CPMI-IOSCO's principles for financial market infrastructure in 2016, four recommendations were issued to VP.

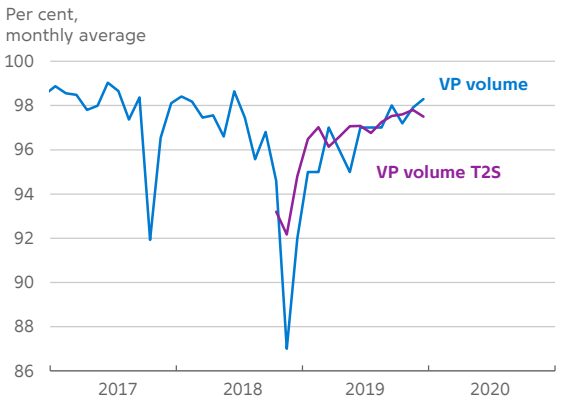
VP has complied with three of the recommendations. The final recommendation stipulates that VP should adjust its recovery plans to take better account of different critical scenarios. VP has revised its recovery plan, which is currently being assessed by the Danish Financial Supervisory Authority and Danmarks Nationalbank, which cooperate on supervision and oversight of VP.

Danmarks Nationalbank is also involved in the European oversight of T2S and has, among other things, provided input to an assessment of T2S 's observance of the CPMI-IOSCO principles, as set out in the section *Payments and securities settlement in euro*.

Cyber resilience
VP is continuously working to strengthen its cyber resilience. Specifically, in 2019, VP strengthened its data protection, access controls, system and network security and conducted training and awareness campaigns for employees.

On 25 October 2019, VP published the Danish Financial Supervisory Authority's report on the supervision

High settlement ratio in 2019 Chart 7



Note: In the chart, the settlement ratio is stated on the basis of the number of transactions.
Source: VP.

inspection of VP Securities A/S, with a particular focus on cyber security. The report concluded that VP is focusing on risk, including cyber risk, but the Danish Financial Supervisory Authority also found that VP should be ordered to improve its governance of critical IT vendors in relation to IT security, including cyber security. VP has submitted new material to the Danish Financial Supervisory Authority, following up on the orders.

At the end of 2019, VP entered into a new contract with its critical IT provider. The contract gives VP more flexibility than before. VP will, for example, be able to adjust its capacity to peak conversion periods. The contract also provides VP with the possibility to set up requirements for the supplier's risk management.

In 2019, Danmarks Nationalbank performed an assessment of VP's compliance with CPMI-IOSCO's cyber guidance, which elaborates on the cyber security aspects of the CPMI-IOSCO principles. The preliminary conclusions were discussed with VP which then updated part of the assessment basis. The assessment will continue in 2020.

System updates
VP is preparing to set up the future pan-European penalty system, which will involve adjustments to both the VP's and the participants' systems.

CCP clearing

In Denmark, trading in equities from the large-cap and mid-cap segments and repos is settled via a central counterparty, CCP, see Box 5.

On the Danish market, three CCPs – EuroCCP, LCH Clearnet and Six X-clear – clear stock equities transactions, while Nasdaq Clearing clears repo transactions.

Ongoing supervision to ensure that CCPs comply with the regulatory requirements is conducted by the national supervisory authorities in collaboration with supervisory colleges, comprising supervisory authorities and central banks from the primary countries in which the CCP is operating. There are no Danish CCPs, but Danmarks Nationalbank monitors developments for the foreign CCPs that are particularly relevant to Denmark, e.g. via its participation in the EuroCCP supervisory college.

EuroCCP is a Dutch CCP responsible for a large part of the clearing of Danish equities and is therefore considered to be of vital importance to Danish securities settlement. In December 2019, one of the five owners – the Chicago Board Options Exchange (CBOE) – made an offer to take full ownership of EuroCCP. The consolidated ownership is not expected to change EuroCCP's strategic focus, but will allow EuroCCP to develop its derivatives business. The acquisition is expected to be completed in the first half of 2020, subject to its approval by the Dutch authorities.

What is a CCP? Box 5

A CCP intermediates between the parties to a transaction, assuming the risk for both the buyer and the seller from the transaction date until the transaction has been finally settled. So if either of the parties to the transaction defaults within this period, the CCP still has an obligation to the other party. However, this also means that risks are concentrated in the CCP, and therefore the CCP is subject to a number of regulatory requirements[1] to ensure the completion of the transaction.

1. See 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 *(Link)*.

Payments and securities settlement in euro

Payments and securities transactions by Danish banks in euro are settled in TARGET2 and TARGET2-Securities (T2S).

TARGET2 is the trans-European RTGS system for settlement of interbank payments in euro. TARGET2 also handles transfers for settlement in other euro payment systems such as T2S. T2S is the trans-European system for settlement of securities transactions in euro and in Danish kroner.[18]

Use

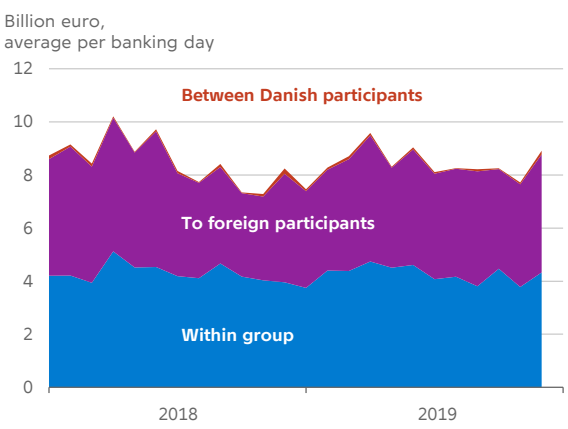
There are 26 Danish participants in TARGET2. In 2019, Danish participants' daily interbank payments averaged 8.4 billion euro. Danish participants use TARGET2 mainly for intergroup payments and payments to non-resident participants, see Chart 8. Exchange of euro mostly takes place with participants in Germany, Finland, France and the Netherlands.

A total of 21 central securities depositories from 20 countries now settle via T2S, including VP. A bank may settle via T2S as either a direct participant, if the bank has a so-called Dedicated Cash Account, or as an indirect participant via another participant's access.

A Dedicated Cash Account must be set up through one of the central banks in the EU. Thirteen Danish banks hold a Dedicated Cash Account in euro at Danmarks Nationalbank for payment in or receipt of euro in connection with T2S settlement. Other Danish banks may have set up a Dedicated Cash Account through other EU central banks.

Euros cannot be deposited permanently in Dedicated Cash Accounts. Banks must therefore also have access to a TARGET2 account to which euros can be transferred at the end of the settlement day. The majority of Danish banks have concluded agreements with correspondent banks. Some of the largest banks have established a TARGET2 account through their branch in a central bank in the euro area. This also enables them to borrow euro on an intraday basis.

Interbank payments in TARGET2 Chart 8



Note: The chart shows payments submitted by Danish participants via TARGET2. Daily averages have been calculated on a monthly basis.
Source: Danmarks Nationalbank.

Operational reliability

The operational reliability of the local TARGET2 components for which Danmarks Nationalbank is responsible was satisfactory in 2019. There were only minor incidents, which did not affect the execution of payments in euro.

International standards

Oversight of TARGET2 and T2S takes place in collaboration with the EU central banks. Danmarks Nationalbank participates in the joint oversight headed by the ECB which takes place in working groups with the participation of the national central banks.

In 2019, the ECB completed an assessment of T2S based on a selection of the CPMI-IOSCO principles for financial infrastructure. The assessment was approved by the Governing Council in October 2019.

18 T2S can handle multiple currencies. Besides the euro, Danish kroner is the only other currency connected to T2S. Read about the settlement of Danish kroner in the section *Securities settlement*.

Danmarks Nationalbank has provided input to the assessment and participated in meetings with the T2S operator. The assessment will not be published, but Danmarks Nationalbank and VP are familiar with the content, and Danmarks Nationalbank will participate in the follow-up on the assessment in 2020.

In addition to oversight, T2S is also subject to supervision. Along with other European central banks and supervisory authorities, Danmarks Nationalbank and the Danish Financial Supervisory Authority participate in a Cooperative Arrangement that defines common frameworks and coordinates oversight of T2S.

System updates

The ECB has been working in recent years to modernise the European payments infrastructure.

In 2016, the ECB launched a consolidation project to bring together TARGET2, T2S and TIPS (Target Instant Payment Settlement) on one platform, thereby achieving operational savings through consolidation of cross-cutting functions. As part of the consolidation, TARGET2 will be replaced with a more up-to-date RTGS system.

TIPS and T2S already allow for settlement of currencies other than euro. In connection with the consolidation, TARGET2 will also be able to handle currencies other than euro.

In parallel with the consolidation, a single gateway – the European System Market Infrastructure Gateway – to the Eurosystem's payment and settlement systems will be established with the aim of providing participants with easier and cheaper access to the systems.

Finally, the ECB is developing a new collateral management system called the European Collateral Management System (ECMS). At first, ECMS can only be used to provide collateral in euro.

Settlement of foreign exchange transactions

CLS Bank International (CLS) is an international settlement system for foreign exchange transactions. CLS is owned by large, international banks and settles transactions in 18 participating currencies, including Danish kroner.

In CLS, the two payments in a foreign exchange transaction are settled simultaneously (Payment-versus-Payment, PvP). This reduces the settlement risk, i.e. a risk that one party in a foreign exchange transaction fails to uphold its obligation. In the case of foreign exchange transactions settled outside CLS, e.g. through correspondent banks, the parties incur a settlement risk because the payments are settled independently of each other.

Danmarks Nationalbank participates in the cooperative oversight of CLS, see Box 6.

Use

More than 95 per cent of all foreign exchange transactions in Danish kroner are settled via CLS.[19] This is an increase from 2016, where it was about 80 per cent.

Both Danish banks and firms can settle foreign exchange transactions via CLS. One Danish bank participates directly in CLS settlement. Those who are not direct participants can settle foreign exchange transactions in CLS via one of the nine participants who offer indirect participation to the Danish market.

Five participants have a CLS settlement account at Danmarks Nationalbank, three of which offer handling of incoming and outgoing payments for CLS settlement on behalf of the other participants.

The average daily value of transactions in Danish kroner was kr. 265 billion in 2019. This is an increase of 12 per cent relative to 2018, see Chart 9. The number and value of trades are particularly large around quarter change and on days around foreign holidays.

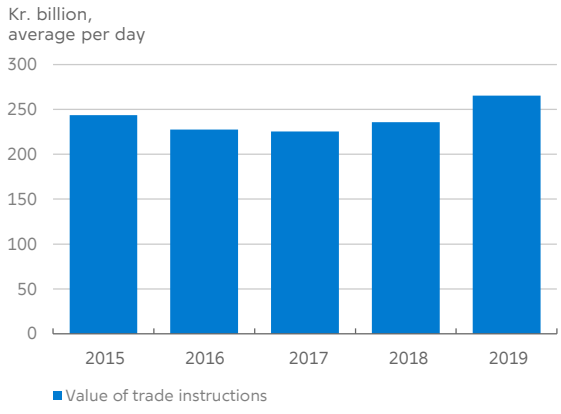
Oversight of CLS Box 6

Oversight of CLS is based on the CPMI-IOSCO principles. Every second year, CLS publishes an updated disclosure of the system's observance of the principles.[1]

Oversight of CLS is carried out by a joint CLS Oversight Committee[2], which is a forum for cooperation between the central banks of the participating currencies, whereby they can carry out their national oversight responsibilities. Danmarks Nationalbank participates in this work, which is organised by the Federal Reserve, the Fed. The Fed is also the supervisory authority for CLS. Danmarks Nationalbank's oversight is focused on matters of importance to the settlement of transactions in Danish kroner.

1. CLS, Principles for Financial Market Infrastructures Disclosure, 2018, (*Link*).
2. Federal Reserve System, Protocol for the Cooperative Oversight Arrangement of CLS (*Link*).

Value of trading instructions in CLS Chart 9



Note: Daily averages calculated on a monthly basis.
Source: CLS Bank.

19 Estimate based on BIS, Triennial Central Bank Survey, Foreign exchange turnover in April 2019, Bank for International Settlements, September 2019 (*Link*) and data from CLS Bank.

Operational reliability and liquidity
Pay-ins to CLS take place via the national RTGS systems, in the case of Danish kroner via Kronos2. Hence the operational reliability of CLS depends on the reliability of the RTGS systems. In 2019, there were no incidents in Kronos2 which affected the deadlines for CLS settlement.

The Danish participants reserve sufficient liquidity for CLS settlement.

System updates
In 2019, CLSNow[20] was launched. CLSNow is a service to settle trades individually within the same day via PvP. This allows participants to better manage their liquidity across currencies. Settlement in CLSNow also reduces settlement risk. Settlement is currently possible in Canadian dollars, euros, British pounds and US dollars. The service will potentially be expanded to all CLS currencies.

20 CLS, CLSNow (*Link*).

PUBLICATIONS

NEWS

News offers a quick and accessible insight into an Analysis, an Economic Memo, a Working Paper or a Report from Danmarks Nationalbank. News is published continuously.

ANALYSIS

Analysis from Danmarks Nationalbank focuses on economic and financial matter. Some of the analyses are published with a regular frequency e.g. *Outlook for the Danish economy and Financial stability*. Other analyses are published continuously.

REPORT

Report comprises recurring reports and reviews of the functioning of Danmarks Nationalbank. For instance Report includes the *Annual report* and the annual publication *Danish government borrowing and debt*.

ECONOMIC MEMO

Economic Memo is a cross between Analysis and Working Paper and it often shows the ongoing study of the authors. The publication series is primarily targeted at professionals and is solely available in English. Economic Memo is published continuously.

WORKING PAPER

Working Paper presents research projects by economists in Danmarks Nationalbank and their associates. The series is primarily targeted at professionals and people with an interest for academia. Working Paper is published continuously.

The report consists of a Danish and an English version. In case of doubt regarding the correctness of the translation the Danish version is considered to be binding.

DANMARKS NATIONALBANK
HAVNEGADE 5
DK-1093 COPENHAGEN K
WWW.NATIONALBANKEN.DK

This edition closed for
contributions on 15 April 20XX

DANMARKS
NATIONALBANK