Challenges for the payment system

Speech by Deputy Governor Jon Nicolaisen, Finance Norway's payments conference, 16 November 2017

Please note that the text below may differ slightly from the actual presentation.

Introduction

The payment system is changing along a number of dimensions. These changes will not only have an impact on the way we make payments, they will most probably also contribute towards promoting and even accelerating the structural changes we have already seen in the financial industry.

Today, I will briefly outline some of the most important challenges we are facing. We can perhaps call the sum effect of these challenges a change programme. For this programme to succeed, cooperation is necessary, both within the financial industry itself and between the business community and the authorities. The authorities and the financial industry largely have coinciding interests. We all share the same aim: that Norway will continue to have an efficient, robust and modern payment system.

PSD2 and new payment service providers

In recent years, the EU has issued a number of regulations which we must adhere to. The revised Payment Services Directive (PSD2) is particularly important. The purpose of PSD2, together with other regulation, is to secure cheap, modern and efficient payment services. PSD2 will enter into force in the EU in two months' time. A consultation process has been initiated on proposals to implement the directive in Norwegian law. In addition, detailed EU guidelines must be in place before PSD2 can have its intended effect.

PSD2 takes account of two new types of payment services: payment initiation and account information services.

- Payment initiation permits third parties (in addition to customers and customers' banks) to initiate payments from customers' accounts. A third party may, for example, be a company that offers a payment application for smart phones.
- Account information means that third parties gain access to customer account information and can provide customers with aggregated online information for multiple payment accounts.

This change separates ownership of the account systems from the provision of payment services. This is intended to facilitate innovation and competition for customer services, on top of the account infrastructure.

Payment initiation and account information may be offered as independent services or as part of a wider array of services. Platform-based service providers in particular will likely explore the possibilities for offering payment services bundled with other services.

PSD2 will, in principle, promote a more efficient payment system. At the same time, we must be prepared for the possibility that an altered market structure and technological innovation may lead to new vulnerabilities and risks. This may necessitate further regulations. Norges Bank will consider measures if they are required. The aim must be the continued existence of a robust and efficient payment system.

The payment market is characterised by network effects and platform competition. Global technology companies, such as Facebook Messenger, Google, Apple and Samsung, are relevant providers of payment services. These companies are able to capitalise on their popularity among users. In the long term, this may adversely affect competition and efficiency, since it is difficult for other providers to challenge large networks. There is also a danger that the owners of popular technological platforms could exclude other payment service providers from offering services on their platforms. If this proves to be the case, this is a matter for the competition authorities.

Under PSD2, also commercial undertakings can seek authorisation as payment initiation service providers. Mobile phone apps can combine direct advertising, loyalty programmes, storage of receipts with actual payments.

Even so, banks will play a key role. Banks will also be able to provide payment services to persons who do not hold an account with the bank. This may strengthen interbank competition for payment customers.

New technology must be used for the good of society. In principle, it is up to the business sector and customers to find suitable methods of payment. At the same time, we must ensure the security of the payment system. New payment service providers will increase the dissemination of payment information. This may also increase the risk that payment information gets into the wrong hands. Vulnerabilities related to accessing, processing and storing information may affect the public's confidence in the payment system. It may ultimately be appropriate to implement new measures to ensure that this information is processed in a secure manner.

Fast payment solutions

The general public increasingly expects to be able to transfer funds on any day of the week and outside traditional opening hours. They also expect that payees will be credited quickly. In the future, there will have to be a good reason *not* to credit payees immediately, rather than with a delay, as is the case currently.

This means that the payment system must meet new requirements. In Norway, there is a provisional instant payments solution, which an increasing number of banks are adopting. It is positive that the solution is becoming more widely used, but it has its drawbacks. For even though participating banks have entered into a loss-sharing agreement, banks still incur

credit risk before payments are settled and the solution cannot be used for certain types of payments.

Bits and Norges Bank are therefore jointly developing a better solution, called BRO in Norwegian "*Betalinger med raskere oppgjør*" (payments with faster settlement). BRO will be an efficient underlying infrastructure that is intended for all types of payments. The solution will be in place by the end of 2019.

Norges Bank has initiated an in-house project to make the necessary adjustments to the settlement system. The Bank will do its share to enable banks to settle payments to each other without incurring credit risk. Customers will also be able to make instant payments in larger amounts.

Customer services will also have to be modified. Banks should take the lead in making the necessary improvements so that customers can benefit from better real-time payments as quickly as possible. Vipps will replace international credit cards with debiting through BankAxept and instant account-to-account payments as underlying payment instruments, making payments more efficient. When real time-payments based on BRO replace the current instant payments solution, in principle, all payments can be made this way, depending on what customers choose.

Mobile payment technology

Mobile payment technology is evolving. User-friendly smartphone payment apps have spread rapidly over the past few years. After a preliminary phase with several payment providers, Vipps now dominates the Norwegian market. Vipps is established as a separate company and has many partner banks.

Today, mobile apps are primarily used when card terminals are not available. In this respect, up to now, they have been an alternative to cash. Looking ahead, we must expect that their use will extend into new areas. Paying for online purchases is one example and paying in shops is another. In addition to apps such as Vipps, it is likely that banks will develop mobile wallets with a scroll-down menu of payment solutions. The experience of other countries and the introduction of PSD2 may indicate that international operators may also enter the Norwegian market.

Interoperability implies that payments can be made even if the payer and payee use different banks or user interfaces. It has been challenging to achieve interoperability between mobile apps. Vipps' market dominance reduces these challenges, but this assumes that all market participants will be connected to the system. This assumption may be too strict. Other payment service providers and payment solutions will also wish to enter the market on equal terms.

The alias registers are important here. An alias register links account numbers to telephone numbers and other ways that identify account holders. Today, separate registers are compiled in each solution. In my opinion, there are clear advantages to having a central register that is used by all banks and other service providers in the Norwegian payment

market. This should be part of a common infrastructure and not be part of private closed systems where ownership can change.

A common register facilitates interoperability and high register quality. The greater the level of activity is, the more up-to-date the information is. We would also then avoid contradictory information in the various registers, which can arise, for example, when customers do not update their information everywhere at the same time.

Insufficient register information may be a barrier to competition. An alias register shares similarities with a public good that should be organised as common infrastructure and be available to all service providers, for a price, if necessary. Service providers should compete on other aspects of the services they offer.

I look forward to seeing initiatives from Finance Norway and Bits in this respect. It is often most appropriate for the industry to arrive at satisfactory solutions on its own.

Cyber security

The consequences of cyberattacks can be considerable. What we are now witnessing is probably just the beginning. We must find a suitable way to mitigate risk, without making our systems needlessly expensive. Cyber-security challenges are among the most significant challenges to our payment system. Without an efficient defence system, trust in the system can be undermined over time.

For its part, Norges Bank is devoting considerable resources to securing its systems, oversight of activities and implementing measures to protect against cyber attacks. As part of oversight and supervision, we will increase our monitoring of cyber-security risks in the payment system.

This requires cooperation, both nationally and internationally, to identify and combat cyberattacks. Nationally, this takes place through, for example NorCERT, part of the Norwegian National Security Authority (NSM), and for the financial sector through the Norwegian Financial Sector Cyber Security Center (FinansCERT) under Bits. The Nordic financial sector has established Nordic Financial CERT as an extension of the Norwegian FinansCERT. The need for cooperation does not stop at a Nordic level. The challenges are international, and are shared by private financial undertakings, their service providers and subcontractors and authorities in many countries.

Measures to promote cyber security are technically complicated and require specialist expertise. But it is management and boards of directors in institutions and companies that have the final responsibility and decide strategy and resource use. This responsibility cannot be delegated or outsourced to others. Owners and managers must be aware of their ultimate responsibility. As supervisory authority, Norges Bank will follow up efforts in the area of cyber security, in collaboration with Finanstilsynet (Financial Supervisory Authority of Norway).

Here, the interests of the authorities and the financial industry coincide. Let me once again encourage the industry to work out satisfactory solutions. A great deal has already been done and collaborative bodies have been established at a national level. However, initiatives in this area are still rather fragmented. There is a need for an even more coordinated and targeted effort to obtain overall control and reduce risks.

The system owners must ensure that critical IT providers have established robust contingency solutions and that these are tested regularly. If this is not done, the system owners are obliged to assess alternative solutions, also if they are costly.

The responsibility of the system owners is the same, irrespective of whether the entire technical operation or just parts of it are outsourced.

Offshoring is increasing. More flexibility, lower costs and a larger pool of persons with requisite skills are good arguments. At the same time, offshoring entails other forms of risk. Norwegian control is reduced. We become dependent on infrastructure and authorities outside of Norway. It would help if, in a crisis, operations can be moved back to Norway at short notice. It is still possible that in the future, critical systems will be required to be permanently operated from Norway.

Electronic central bank money

Making payments electronically involves the use of deposit money (money deposited in banks). Bank deposits refer to money that is issued by, and is a claim on private banks. Each time a bank extends credit, new money is created. Bank deposits now account for 98 percent of the broad money supply (M3). The increasing use of new payment methods, such as mobile payment solutions, suggests that this percentage will continue to rise.

We have to ask ourselves: should we allow private solutions to compete freely in developing means of payment, or must the authorities play a role? The crucial factor is whether solutions based on private money deliver the characteristics the payment system should have. The system must be able to channel payments swiftly, safely, at low cost and in a user-friendly manner. The means of payment itself – our money – must be universal, because money is only useful if it is widely used. This requires trust.

Deposit guarantee schemes and banking regulation promote trust in banks' deposit money. Trust is also underpinned by being able to convert to another secure alternative, ie cash. Norges Bank assists private operators in implementing faster and safer payments. We cooperate with other authorities to oversee and supervise the payment infrastructure to ensure robustness and efficiency. Privacy rules prevent unauthorised access to payment information.

But there are some characteristics deposit money lacks. Nor is direct and immediate settlement between two parties, without the involvement of a third party, possible without cash. The system is vulnerable to advanced attacks. Having more money on deposit than is covered by the deposit guarantee scheme involves risk.

Perhaps new private payment solutions may be able to offer some of these characteristics, but a possibility which is also being discussed is the introduction of electronic central bank money – in addition to cash. This possibility raises many questions which Norges Bank and other central banks are trying to answer. This is a long-term process and we do not yet know what the answer will be.

Conclusion

The Norwegian payment system was digitalised at an early stage and this has benefited private individuals, businesses and banks. We can be justifiably proud of our payment system. Digitalisation is now going through new phases. The deliveries of customer services and the underlying infrastructure are being separated from one another, and we are witnessing the arrival of new market entrants. Global platform providers are interested in the payment market.

We must make full use of the opportunities to improve the payment system and we have made a start. Further changes will come. Today I have emphasised some of the tasks which the industry and Norges Bank must solve in the coming years:

- Introduce instant payments and develop a better solution through the BRO project.
- Mobile instant payments and BRO.
- Agreement on a single alias register as a common infrastructure.
- A more coordinated and systematic effort to reduce cyber risk. Managers and owners must be aware of their responsibility, also when operations are outsourced.
- We must continue the work on truly reliable contingency arrangements.
- We must assess whether it is necessary for risk-mitigating measures related to offshoring.
- And we must assess whether electronic central bank money is necessary and desirable.

We all want Norway, also in the future, to have one of the most efficient and robust payment systems in the world. This will require change and willingness to invest.

We have a job to do, but we have what is required to succeed.