# Central Bank Oversight and the Changing Retail Payments Landscape

Ron J. Berndsen and Bouke H.J. Buitenkamp

## I. What is Payment Systems Oversight?

Supervision of payment and settlement systems, known as oversight, is among a central bank's responsibilities. For the Netherlands, the legal basis for oversight lies in the Banking Act of 1998 and in the EU Treaty. Oversight is a form of supervision aimed at promoting the security and efficiency of payment and securities clearing and settlement systems. De Nederlandsche Bank (DNB) considers that this includes all payment systems, payment products and securities settlement systems of relevance for the Netherlands. The supervision consists of monitoring these systems and products, assessing them in the light of international standards and—where necessary—insisting on changes.

Oversight has dual objectives. The first objective is to help prevent systemic risks in systemically important payment systems. To assess systemically important payment systems, standards are used which are intended to prevent one party's problems (e.g., liquidity problems) from spreading to the other payment system participants and beyond. The second objective of oversight is to control risks which may affect the smooth operation of the payment system. One example is fraud via electronic means of payment, such as the skimming of bank cards. These risks may endanger the smooth operation of payment systems, even if there is no systemic risk. Nevertheless, the poor functioning of one or more payment products may have significant economic and social implications, and may ultimately damage public confidence in the payment and currency system. This approach to the objectives of oversight is in line with the general definition put forward by the BIS.[1]

## II. How We Do Oversight

In this section we introduce the way oversight is conducted at De Nederlandsche Bank (DNB). The focus here will be on oversight in the retail payments area.

DNB, as a Eurosystem central bank, conducts oversight in line with the Eurosystem's oversight policy.[2]

## A. Scope of oversight

In line with the two goals of oversight of mitigating systemic risk and promoting the safety and efficiency of the payments, the scope of the oversight is rather broad. In our case all payment systems, payment instruments and securities systems that are relevant to the Netherlands are in scope. In 2008 there were 22 oversight objects for the Netherlands (see Table 1) of which half belong to the retail space. A central role in the retail payments area is played by the automated clearing house (ACH) called Equens. The ACH clears more than 95% of all interbank retail transactions. Furthermore, there is a payment scheme owner—named Currence—carrying the following main payment instruments: debit card PIN, direct debit, e-purse, an Internet payment instrument and a paper-based instrument.

There is an important distinction between on the one hand the wholesale and securities systems and on the other hand the retail payments area. In wholesale and securities systems, the process of internationalization in Europe, kick-started by the introduction of the euro, is far more advanced than in the retail payments area. The physical IT infrastructure supporting the real time gross settlement (RTGS), central securities depository (CSD) and central counterparties (CCPs) that are relevant for the Netherlands is located abroad. In the European retail space the Single Euro Payments Area (SEPA) project is setting the stage, but it will take some more years before SEPA-wide payment instruments have reached a critical mass. The different degrees of internationalization are reflected in the way oversight is conducted. For wholesale payment systems, such as TARGET2 and CLS, and for securities systems, such as those offered by Euroclear, LCH.Clearnet and European Multilateral Clearing Facility (EMCF), cooperative forms of oversight are standard, while for retail systems and products oversight is still largely organized along national lines or cooperative oversight is in an initial phase. It is widely expected that the corresponding national instruments will be replaced by their SEPA variants of the credit transfer and the direct debit.

In cooperative oversight there is more than one overseer that has an interest in the well-functioning of a system or payment instrument (and often there are quite a lot of overseers and other supervisors) because the system is of importance in more than one country; the system may be multi-currency or operate cross-border. In such cases one overseer takes primary responsibility for overseeing the system, the so-called lead overseer. The role of the lead overseer is to coordinate oversight tasks and to ensure to the extent (legally) possible that the other authorities agree on a common, consistent approach. The other overseers with an interest in the system then usually enter into a memorandum of understanding with the lead-overseer that describes the agreement between the parties on how to conduct oversight.

**Table 1**
**OVERSIGHT OBJECTS AND ARRANGEMENTS (2008)**

| System | Lead overseer/regulator | Other overseers/regulators |
|---|---|---|
| **Interbank large-value payments** | | |
| Target2 | ECB | Eurosystem NCBs |
| Target2.nl | DNB | |
| EURO1 | ECB | Eurosystem NCBs |
| CLS | Federal Reserve System | G10 central banks and other central banks of the 17 currencies involved |
| SWIFT | National Bank of Belgium (NBB) | Other G10 central banks |
| **Securities clearing and settlement** | | |
| LCH.Clearnet SA | Rotating chairmanship for regulators Euronext countries | Other regulators from Belgium, France, Netherlands and Portugal |
| LCH.Clearnet Group Ltd | Commission Bancaire (France) | AFM, DNB and the regulators from Belgium, France, Portugal and the United Kingdom |
| EMCF | AFM and DNB | |
| Euroclear SA | NBB and CBFA (Belgium) | AFM, DNB and regulators from France and the United Kingdom |
| Euroclear NL | AFM and DNB | |
| ECC | Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) | AFM, DNB and Bundesbank |
| **Retail payments** | | |
| Equens | DNB | |
| Paysquare | DNB | |
| VISA Europe | ECB | DNB and NCBs from Belgium, Germany, France, Italy, Austria and the United Kingdom |
| MasterCard Europe | NBB | DNB, ECB and NCBs from Germany, France, Italy and Austria |
| Currence (Chipknip, Acceptgiro, PIN, Incasso, iDEAL) | DNB | |
| NVB (Spoedopdracht) | DNB | |
| UPSS | DNB | |

A second distinction between on the one hand wholesale/securities and on the other hand retail is the number of different parties involved in the respective payment chain. On the retail side, there are many parties involved that provide different services to consumers and merchants. Many of these parties may be non-banks, which in itself poses some challenges for central banks. This was in fact the topic of the previous Kansas City Fed Payments Conference in 2007.[3]

Determining the precise scope of retail oversight is therefore sometimes challenging. A recent example can be found in the so-called overlay payment service. This service was introduced in the beginning of 2009 in the Netherlands and also in some other countries. An overlay payment service is a service where, from the perspective of the consumer, a third party intervenes between the consumer and the Internet banking application of the consumer's bank when the consumer pays for a good he or she ordered at the website of an online-merchant. By doing so, the overlay service provider is able to provide real-time information to the merchant whether the payment was sent or not. The merchant then receives the payment amount in due time following normal interbank settlement. However, in the process, the overlay service provider obtains authentication data from the consumer that, under most terms and conditions of Internet banking in the Netherlands, are to remain secret at all times. Although the overlay service may be an innovation allowing consumers to pay for online goods and services, it is also interrupting the end-to-end secure connection between the consumer's computer and the bank's server, raising serious objections.[4] It is therefore very important and at the same time difficult to determine whether an overlay service is in or out of scope as it doesn't fit in any of the usual categories of a payment instrument, a payment system, a credit institution or a payment institution. It is therefore not easily brought within the scope of oversight.

## B. Prioritizing the work

The oversight department of any central bank will presumably have limited resources for conducting the oversight. Prioritization is therefore a necessary annual exercise. Having determined the scope which could be seen as the "width" of oversight, prioritizing could be termed the "depth" of oversight: determining the amount of resources to be spent on each object. For the systemically important (retail) payment systems prioritizing is fairly straightforward as —given their systemic importance—a considerable portion of the available oversight capacity should be used to assess such systems. Those assessments can be comprehensive when a new system is planned or when an existing system undergoes a major change that implies a potentially large change in its risk profile. In any case, at De Nederlandsche Bank, assessments are updated annually in order to have at least once a year an overview of how well the system complies with the relevant standards.

For retail payment products and other non-system roles performed by parties in the payments infrastructure, determining the priority is less trivial. Typically, systemic importance of retail payment products is low. For payment instruments a triennial cycle is used for planning the assessments. The order in which the instruments are assessed within the triennial period depends on the perceived level of risk. Important drivers are the amount of fraud, whether there are any known complaints by the general public or substantive negative media attention, the amount of time elapsed since the last full assessment and any proposed joint cooperative oversight assessments. The triennial cycle ensures that each payment instrument

is at least periodically assessed. The assessment and its follow up are refreshed on an annual basis.

It is good to have a plan but sometimes deviating from the plan is necessary. Suppose everything is neatly prioritized and planned, resources are allocated and the assessments have had their kick-off meetings. Then a financial crisis or a major operational disruption hits the payment system or its participants. The traditional view assumes that the overseer would not be involved during the crisis itself as oversight is a form of *ex ante* supervision. The overseer is therefore involved pre-crisis (in normal oversight mode) and post crisis (to conduct a post mortem and see to it that the lessons learned are indeed implemented). The global financial crisis that started in August 2007 and especially the weeks following the Lehman Brothers default on 15 September 2008 showed that there is a role for the overseer to play. Not in managing the crisis or the disruption itself—that remains the responsibility of the system operator—but in gathering in a timely fashion the status of other systems and critical participants so this can be used to assemble an up-to-date picture of the whole relevant infrastructure.

## C. Reporting the outcomes of oversight

The reporting phase of an assessment is an important step to improve the degree of compliance with the relevant oversight standards. We distinguish between internal and external reporting. With internal reporting we share the assessment with the oversight object. The result of the assessment against the appropriate oversight standards is usually a report listing the major findings, the degree of compliance with each standard and the requested follow up (if any). After internal validation within the central bank it is essential to discuss the results of the assessment with the management of the oversight object and to reach agreement on the follow-up. The follow-up is a list of issues that need to be resolved by the system under oversight in order to improve the degree of compliance. This internal report and the follow-up remain confidential.

External reporting is vital from a transparency viewpoint. The oversight function of the central bank needs to be transparent about its goals and oversight policy methods.[5] This is widely recognized and is a responsibility that central banks have subscribed to in the report "Central bank oversight of payment and settlement systems" issued in May 2005.[6] Some central banks pursue a higher level of transparency than the minimum responsibility just mentioned through also publishing the outcome of the oversight (Bank of England annually since 2005, the Banque de France in 2006 and 2009). As of 2006, DNB also publishes an oversight chapter in its annual report.[7] In that chapter a summarized version of the assessment results of the oversight objects is shown, of course without disclosing classified information. The content of the publication is sent for consultation to the overseen systems and —in the case of cooperative oversight—the other competent overseers. In doing so, external reporting can be viewed as a powerful way of promoting the oversight goals as experience shows that the oversight policy of publishing assessment results

in itself has a disciplinary effect on the overseen entities.

## III. The rationale of oversight

The decisions of a (sufficiently large) payment system provider may have far-reaching consequences throughout society. Both during the design phase and in the day-to-day management of a payment system (or payment product), decisions are made that may affect the ability to conduct payments in a society. The ability to conduct payments in a timely and secure manner is crucial for the smooth functioning of an economy. For the large real time gross settlement (RTGS) systems, this dependency is widely acknowledged. But it also holds true for large *retail* payment systems.

A case in point is the use of the debit scheme "PIN" in the Netherlands. In the Netherlands, debit card use is very widespread. PIN payments can be made at 184,000 points-of-sale, including the vast majority of retail stores. In 2008, a total of 1.75 billion points of sale transactions have been conducted using PIN. With a population of 13.5 million (aged 15 or older), this comes down to almost 130 transactions per person. Balance verification takes place online with each transaction, and the associated payment account is debited typically the next day. Especially when a payment product is so widely used as PIN, it reaches a point where it becomes impossible to swiftly substitute away from it in case of an operational calamity. The public simply does not carry enough cash anymore. Checks, which might provide a flexible alternative in some other countries, have been fully phased out in the Netherlands. Not only have the cash balances of the general public fallen, it is also unfeasible for the public to quickly obtain sufficient cash in case of an operational calamity with PIN. Banks have reduced the number of physical branches and ATMs use the same online PIN verification[8] as PIN transactions. Clearly, should a major operational failure in the online PIN verification process occur, this will have far-reaching repercussions throughout Dutch society.

Decisions by the scheme owner of a significant payment instrument, such as PIN in the Netherlands, have implications that go beyond the normal influence of a private company. As a result, the well-functioning of significant payment systems and instruments is of interest to society at large. Oversight is the way for society to guard its interests regarding the activities of a payment system or a payment product. As is clear from the PIN example, our main focus is on those payment products that are sufficiently widespread (or are likely to be used widespread in the foreseeable future) to impact society at large.

Establishing that decisions of payment systems have implications for society is a required, but not a sufficient condition to establish the need of an oversight function. After all, if society can be fully assured that payment systems will always make correct choices in the absence of oversight intervention, there will be no need for active oversight. In the rest of this section, we conjecture that a payment system can be expected to often make decisions that are in line with society's preferences,

but may also fail to do so. In order to explore the question in more detail, we first note that the decisions that are of most importance are the ones that affect the safety of the payment function and/or its efficiency.

## A. Safety

The perceived safety of a payment instrument is one of the most important factors that determines whether consumers will use it. If a payment instrument is perceived to be unsafe, consumers are likely to shy away and use an alternative payment method. Hence, it is of great importance for the firm that exploits the payment instrument to ensure that a payment instrument is considered to be sufficiently safe by its potential customers. Given the importance that customers typically attach to the safety issue, firms that exploit a payment instrument are likely to attach a high weight to ensuring that their payment instrument is considered to be sufficiently safe. However, the firm also incurs the costs of safety measures. A profit-maximizing firm will weigh the total costs of safety measures against its benefits.

Will the level of safety that a payment service provider chooses[9] be optimal from society's point of view? There are several causes to doubt that this will always be the case. First, a firm may under-invest in safety because of a lack of resources. If, for instance in case of hefty competition, payment fees come under downward pressure, necessary security measures may be postponed or cancelled. Second, note that a firm is not only concerned about the actual safety of their product, but also by the safety of its product *as perceived by the public*. If the firm considers that it can create a positive (and persistent) gap between the perceived and actual safety of the product, it may choose to attempt to influence the perception of safety rather than the actual safety of the instrument. This situation may be most likely to occur if the risks consist of low-probability/high-impact calamities that are very costly to prevent. Especially in these situations the firm may decide to accept the risk that the calamity occurs rather than actively trying to mitigate that risk.

A case in point is the direct debit scheme as it was implemented in the Netherlands up until a couple of years ago. Direct debit is a very common payment method in the Netherlands. In 2008, 1.23 billion direct debit transactions took place for a total value of EUR 300 billion. To put this number into perspective, it is slightly above 50% of total Dutch GDP in 2008. In general, with a direct debit, the recipient debits the account of the payer after receiving a mandate to that effect. If a direct debit transaction is done while the necessary mandate is not present, the payer has the right to have the payment reversed. In the Netherlands, the administration of the mandates was (and is) done solely by the recipient. With mandate verification being done only in case of a complaint/payment reversal, a recipient that faces a pending bankruptcy could turn rogue and misuse the direct debit scheme to collect money from all of its customers. Up until several years ago, few measures were in place to prevent such rogue payments from being processed. The safety net was far from perfect. For instance, the recipient's "normal" payment behavior was unknown to the processor that processes the direct debit payments.

This implied that the plausibility of a batch of direct debit transactions could not be verified by the processor. Since the delivery of a batch of direct debits often took place on an unencrypted data carrier (a tape or floppy disk), manipulation of the batch could even take place in transit. Overall, these risks have not materialized, but that could arguably be merely attributed to the fact that only a small group of people was aware of the security caveats. Hence, although a large fraud would have severely damaged the reputation of the direct debit and would have resulted in a large financial loss, the underlying security risks existed for a prolonged period. Apparently, the chance of such a large impact fraud was considered to be too small to warrant corrective measures. Following critical oversight assessments and a lot of media attention a couple of years ago, such risks concerning the direct debit were addressed.

Generally, the negative effects of a failing payment instrument will go beyond the scope of the payment service provider, especially if the payment instrument is widely used. Conversely, the measures it takes to mitigate those risks will create benefits for society at large. Differently put, the safety of the payment instrument is a quasi-public good. A private, profit-maximizing firm that only partially benefits from positive effects of its actions, but at the same time incurs the full costs of those actions, cannot be expected to fully internalize its positive external effects. A well-known result from public good theory is that in this situation the firm will "produce" less safety than would be optimal from the point of view of society.

## B. Efficiency

Markets for payment instruments are two-sided, requiring that two separate, identifiable groups of customers together use the payment product. Both groups are needed for the successful use of the product.[10] In the case of a payment instrument, one group of customers consists of the holders of the payment instrument (the issuing side) and the other group of customers accepts the instrument as a means of payment (the acquiring side). This two-sided setup complicates the network effects that exist in these markets. Basically, for each customer group, the value of being "connected" to the payment product is a positive function of the size of the other group of customers. So, for a holder of e.g. a credit card, the value of possessing the credit card positively depends on the number of shops where that credit card is accepted. Vice versa, for a store, the value of accepting a certain credit card depends on the number of holders of that credit card. Although these network effects are thus rather complex, it is straightforward that they are a positive function of the overall size of the combined user group. The more people use and accept a payment instrument, the better it can function as a means of payment. Markets with significant positive network effects generally also exhibit strong economies of scale. That is, as the number of users of the product increases, the average costs of operating the payment product falls because of the existence of sizable fixed costs. Furthermore, with marginal costs of an extra payment generally being very small, a payment product may prove to be an uncontestable monopoly.

We will not focus on the difficult pricing issues that arise in two-sided markets with strong network and participation externalities.[11] Rather, our aim is to infer whether a private firm running a payment product is likely to produce an overall level of efficiency that is optimal from society's point of view. For this, we note that in markets with strong positive network effects and economies of scale, the value to the customers of the payment product may outweigh the marginal costs of a transaction by a large margin. If, furthermore, the payment product is a *de facto* uncontestable monopoly, monopoly profits are likely. Although optimal from the firm's point of view, monopoly pricing will generally not deliver optimal results for society as a whole. This is because the extra revenues that the firm generates are likely to shift the focus away from cost effectiveness (static efficiency). Furthermore, product innovation (dynamic efficiency) may be suboptimal due to the lack of competitive pressures. This is not to say that the converse situation, with fierce competition, will automatically result in better efficiency. In highly competitive markets, fees may be driven down to marginal costs, making total cost recovery difficult. On the one hand, this will naturally increase the focus on static cost efficiency, but on the other hand, dynamic efficiency is likely to suffer because of the lack of resources. In all, due to network effects and economies of scale, payment firms may not deliver the level of static and dynamic efficiency that are optimal for society.

In conclusion, both the level of safety and efficiency that a payment firm produces may not be optimal from society's point of view. The oversight function of a central bank is a means to incorporate the external effects that a payment firm exerts, in effect promoting the socially optimal levels of safety and efficiency. It has to be noted that the extent to which oversight is an effective tool depends on the efficacy of the oversight function. There is a risk that market failures are merely replaced by a government failure. This happens if oversight turns out to be ineffective or when it introduces new, and possibly larger, problems that did not exist prior to intervention. Of course from our perspective we assume that oversight, on balance, is effective in increasing social welfare.

## IV. Challenges to oversight from the changing retail payments landscape

### A. Identifying new initiatives

New retail payment initiatives emerge almost on a monthly basis. A part of the initiatives stem from companies that are already within, or at least close to, the payment sector. Quite often, companies that offer new payment instruments come from outside the traditional banking and payment community, e.g. the telecommunication sector. Especially this group of "outsider" start-ups may be relatively unfamiliar with the oversight function of the central bank and unaware that they might be subjected to oversight. For oversight, this implies that it might be challenging to ensure that we are aware of all relevant initiatives. Furthermore, we need to be ready to start active oversight as soon as we feel that new entrants turn into

relevant players.

For all ends and purposes, the identification of new potential oversight objects is not a major practical issue. In the past months, DNB has performed a stock-taking exercise that showed that a large number of nonbanks are active in the payment sector, together covering virtually all sections of the payment chain. Considering only the nonbanks that offer services to a significant number of banks, we find that most of these service providers are already subjected to oversight or other forms of supervision. Generally, once start-ups have become aware of the oversight function, in most cases they are willing to be subjected to oversight. This may at first sound counterintuitive. After all, being subjected to a supervisory body places an extra burden on these start-ups as it takes time and effort to comply with oversight standards. The reason for this counterintuitive outcome is that these companies often feel that being subjected to oversight may be a valuable asset in their relationships with potential partners and customers. A payment product firm needs to gain the trust of potential customers as consumers will need assurance that the product is sufficiently safe. Being subjected to oversight helps these companies to signal to the public that they can be considered to be trustworthy. De Nederlandsche Bank also publishes the results of oversight in its annual report, which implies that there is a two-sided risk for the firm: We could also assess the start-up to significantly fail the oversight standards.

After the identification of new relevant players in the payment market, a practical question arises regarding the scope and the optimal intensity of oversight. As was illustrated in section IIA, those questions can sometimes be challenging as new and emerging nonbanks don't always fit in any of the typical categories.

## B. Increased competition

Many of the new entrants in retail payments markets direct their attention on the beginning and the end of the payment chain, offering consumers and merchants new and innovative means of conducting retail payments. Often, alternative payment instruments will be available and the introduction of a new payment method will not increase the total number of transactions. However, in some cases, a new payment instrument enables trade that had not been taking place before, for instance because consumers or merchants previously felt that there used to be no safe payment method available. In these instances, the total number of transactions will increase. A case in point is PayPal, which has served, among other things, as an enabler for international consumer-to-consumer trade that had previously been infeasible due to the prohibitively high costs of conducting consumer-to-consumer cross-border payments. However, we feel that the PayPal example does not constitute the typical case. Rather, in most markets, alternative payment methods *are* available and the introduction of a new payment instrument is unlikely to significantly affect the total number of products sold. In these situations, a new payment instrument will be a substitute (often a close one), for existing payment methods. If we abstract from the cases where a new payment instrument is responsible for

a significant increase of the total number of transactions, it is clear that we can normally expect new retail payment products to increase competition in the retail payments market.

If we consider the (theoretical) case with only one, uncontestable, payment instrument, it is clear that the entity that governs will be able to charge monopolistic usage fees from its users. In reality, several competing retail payment instruments exist that may be each others' imperfect substitutes, and each may also offer a unique set of characteristics that sets it apart from alternatives. Generally, we expect that payment firms facing competition will not be able to charge total usage fees that are as high as in the monopoly case, although the resulting market structure or the specific characteristics of the payment instrument may still allow for usage fees that remain significantly above marginal costs. This is for instance shown by Bolt and Soramäki[12], who compare a market with two competing payment instruments (with Bertrand-type competition) to the monopoly case and unequivocally conclude that overall fees are lower in the duopoly case.

A Dutch example that shows, according to the Dutch competition authority NMa, excess revenues in the presence of market power, is the PIN scheme in the Netherlands as it operated until some years ago. For a long time, the PIN scheme has been the only domestic debit card scheme in the Netherlands, thereby competing with alternatives such as cash and credit cards. The company Interpay, founded by a consortium of eight banks, provided the network services for PIN transactions. It was also the sole provider of PIN acquiring services, offering these services directly to merchants. In 2004, the Dutch competition authority concluded that Interpay had been abusing its position of power through overcharging merchants.[13] Its fee structure allowed Interpay to earn significantly more than the NMa considers as a normal return on equity. In response to the NMa ruling, a more competitive structure was formed, in which banks (as opposed to Interpay) offer PIN acquiring services to merchants, thereby competing amongst each other. In effect, the monopolistic structure was broken up. This change in the competitive structure was one of the main factors that led the NMa to partly remit the fines one year later.

Overall, we expect that the fee revenues of all payment firms will fall as a consequence of increased competition. Both the usage (volume) and the fee (price) are likely to be adversely affected. The usage falls because the total number of retail payments have to be split among more competitors. Fees fall because in a more competitive environment, the value of the payment instrument to customers is reduced, because of reduced network effects. Furthermore, increased competition from substitutes implies that the usage of each payment instrument is reduced, resulting in lower network effects and therefore a reduction in consumers' willingness to pay for the payment instrument.

How does increased competition impact the oversight function? From the

point of view of oversight, the reduction in total fee revenue itself is not of primary interest. However, the reduction of total revenues may affect payment firms' decisions in fields that *are* of primary interest to oversight: safety and efficiency.

Regarding the effects of more competition on efficiency, on the one hand, the existence of more payment networks that compete for the same number of payment transactions implies that (positive) network externalities will decrease. Hence, it is likely that static efficiency deteriorates. On the other hand, competitive pressures may incite firms to focus more on product innovation in an attempt to reduce costs or create added value for customers. This may improve dynamic efficiency. Overall, the effect of more competition on the efficiency of retail payments is ambiguous.

Increased competition has two, opposing, effects on safety. On the one hand, as established in section IIIA, payment firms may, related to their external effects, "produce" less safety than would be optimal from the point of view of society. If total revenues fall as a result of increased competition, this may prompt payment firms to postpone or cancel costly safety measures that might be crucial to prevent low-probability/high-impact risks, thus increasing the chances that a payment instrument fails. On the other hand, however, with more alternatives methods of payment available, large-scale operational calamities that hit only one of the payment instruments will have a less severe impact on society. After all, consumers and merchants would in such an event find it easier to switch to alternative payment methods. Overall, even if the "production" of safety is adversely affected, this may or may not be problematic for society.

Oversight needs to ensure that the minimum safety and efficiency standards remain observed. Although the effects of higher competition on both variables are ambiguous, heightened competition may change the assessments of the safety and the efficiency of retail payment products, both existing and new.

## C. Emergence of common payment infrastructure

As indicated above, new entrants to the retail payment markets often seem to sprout very near to final consumers. With payment product innovations, such as mobile payments, aimed at changing the interaction between merchants and their customers, most of the new entrants want to position themselves at the endpoints of the payment chain. They may, however, find it difficult to position themselves, not only because of competition of existing payment instruments, but also because they need to find a way to connect to existing payment infrastructures. Some initiatives sprung from banks, which clearly are in the best position to ensure a connection to existing payment infrastructures. Truly new entrants to retail payment markets, however, are likely to face difficulties in connecting to current payment infrastructures. Operators of those payment structures may need to be forced by law to open up and grant competitors access to their networks. In light of the experiences in other sectors, including networks for cable TV, mobile telecommunication

and electricity, this is likely to be a jerky process that may take significant time. The overlay services that have been referred to above are a telling example. The "product" that these companies want to sell, is the guarantee that a customer has indeed executed a payment to the benefit of the merchant. For this, they use a method (authenticating and conducting payments on behalf of the consumer, using their credentials) that clearly cannot be endorsed as a safe and prudent way of conducting payments. However, it appears that safer methods would crucially depend on the cooperation of the consumer's bank, which would be in a position to provide a guarantee that the consumer has made an outgoing payment.

We expect that in the longer run, developments such as this one will lead to a situation where a wide range of retail payment instruments exists, but that those products connect to a limited number of payment infrastructures. "Payment infrastructure" should in this respect be understood to include a wide range of elements that are used for conducting payments. It not only pertains to clearing and settlement (which in most countries already is very concentrated), but also to payment terminals in merchants' shops, to communication networks used for financial transactions and even to the physical carrier of the payment instrument. Technically, cards can combine debit and credit payment products and, for instance, an e-purse. In fact, cards that combine a debit product with an e-purse have been in use in the Netherlands for roughly a decade. In a similar fashion, payment terminals are or can be made flexible so as to accept multiple products that are within a previously defined specification.

A move towards a situation where payment infrastructures are used for several payment instruments changes the risk profiles of these products. A (possibly significant) part of the operational risks originate at the physical infrastructure, and if that infrastructure is not dedicated for a specific payment product, a failure will simultaneously impact all products that use that infrastructure. Differently put, the safety and efficiency of several payment instruments crucially depend on the safety of the common infrastructure.

The concentration of operational risks may also give rise to legal governance risks. After all, who is primarily responsible for the functions that the shared infrastructure performs? The conventional view is that the governance authorities of the payment products involved is, as they have outsourced to the common infrastructure. Furthermore, outsourcing should never imply that responsibilities are transferred. Hence, from this point of view, the governance authorities of all products that make use of the common infrastructure each are responsible for the functions that the common infrastructure performs for their product.

There are, however, two drawbacks to this conventional view. The first one regards the efficiency of the oversight function itself. There are costs involved in the conduct of the oversight function; costs that are ultimately borne by society. The

efficiency of oversight may not be optimal if, for operational issues related to the common infrastructure, we would address all individual governance authorities. We would be putting the same requirements, pertaining to a single infrastructure, on a range of governance authorities. Rather, it will in certain situations be more efficient (i.e., lowers costs to society) to direct the oversight attention regarding these operational issues directly towards the operator of the common infrastructure itself.

The second drawback relates to the overall risk profile of the common infrastructure. With the use of a common infrastructure, operational risks of several retail payment products are concentrated. Individual governance authorities only carry a responsibility for the risks that the infrastructure implies for their own payment instrument. However, as a failure of the common infrastructure impacts a whole range of payment instruments simultaneously, the risks to society may be larger than the sum of the individual risks that it poses to the governance authorities. After all, the ability to conduct retail payments may be severely impaired if several payment instruments fail simultaneously.[14]

An example that illustrates this issue is the Dutch Interbank Authorization Network Switch (IAN-Switch, or Switch), which is operated by Equens. The Switch plays a central role in the authorization of retail payment transactions that require the use of a PIN code. It performs this function for a wide range of products, including point of sale transactions with credit and debit cards, the authorization of cash withdrawals and recharging e-purses. It receives requests for authorizing PIN codes and acts as a switchboard, routing the requests to the respective bank or payment institution. The response (authorization) from the bank is also routed through the Switch back to the payment terminal, ATM or e-purse recharge station. Furthermore, several additional functions have been added, such as a stand-in function which allows payment transactions to be conducted even if the bank of the holder of the payment instrument is temporary offline. If the Switch should fail, this would instantly halt all point-of-sale transactions that require PIN verification (including the debit card scheme "PIN" that is so widely used in the Netherlands) and all ATMs, halting retail payments.

A wide range of products use the Switch, including all major credit cards and debit card schemes. In order to cover the full extent of the risks that the Switch poses to Dutch retail payments, DNB Oversight is currently in the process of placing the Switch directly under our oversight. This does not imply that the governance authorities of the affected retail products may now ignore the operational risks that are associated with its function. What they can do is reduce their effort to monitor the Switch as they may now take into account that it is a function directly under oversight.

## V. Conclusion

It may not always be obvious which new entrants to the retail payment market need to be subjected to oversight. There is a risk that oversight fails to identify relevant new entrants, although this risk is probably limited for two reasons. First, as the oversight function only deals with parties that in themselves are large enough to impact society, they will normally be identified before they reach that threshold. Second, new entrants often seek out overseers, hoping to obtain a sign of recognition from a trustworthy party.

New entrants can normally be expected to increase competition in the retail payment market rather than open up new markets. As the number of transactions will need to be split among a larger number of companies, the average usage of each competing retail payment product will fall. Furthermore, because of increased competition, the fee per transaction is expected to fall. Overall, with lower volumes and lower prices, fee revenues for each competing product, both new and existing, are expected to fall. With less fee revenues, risks increase that necessary safety measures are not undertaken, especially those aimed at preventing low-probability/high-impact events. This may warrant increased oversight attention. On the other hand, it may be less dramatic if such operational calamities occur as more alternative payment methods are available and the impact on society of one failing payment instrument may be less severe. Overall, even if the "production" of safety is adversely affected, this may or may not be problematic for society. An increase in the fierceness of competition in these network industries implies that (positive) network externalities will decrease, possibly reducing static efficiency. On the other hand, competitive pressures may turn the focus towards product innovation and improve dynamic efficiency. Overall, the effect of more competition on the efficiency of retail payments is ambiguous.

Probably the most significant impact of the changing retail payments landscape on the oversight function is the emergence of common payment infrastructures. We expect that the payment infrastructure will evolve as several other network industries have done in the recent past, turning from competition of networks to competition on the networks. Such an evolution changes and concentrates operational risks. In order to guard that the oversight process remains efficient and ensures that risks that surpass individual payment instruments are well-contained, oversight is being focused on common payment structures rather than only the payment instruments' governance authorities.

---

Authors' Note: The views expressed are those of the individual authors and do not necessarily reflect official positions of De Nederlandsche Bank.

## ENDNOTES

[1]BIS, "Central bank oversight of payment and settlement systems," May 2005.

[2]See *https://www.ecb.int/pub/pdf/other/eurosystemoversightpolicyframework2009en.pdf.*

[3]The conference proceedings can be found at: *http://www.kansascityfed.org/home/subwebnav.cfm?level=3&theID=11323&SubWeb=10683*

[4]DNB's position on overlay payment services can be found at: *http://www.dnb.nl/en/news-and-publications/news-and-archive/persberichten-2009/dnb223392.jsp* (in Dutch).

[5]This paper is doing exactly that.

[6]BIS, "Central bank oversight of payment and settlement systems," May 2005.

[7]DNB Annual Report 2006, 2007 and 2008.

[8]Furthermore, ATMs need to be filled with cash. In case of a run on ATMs, the short-term capacity to restock is likely to fall short as well.

[9]In the absence of oversight.

[10]For a general treatment of two-sided markets, see Armstrong (2006) "Competition in two-sided markets," *RAND Journal of Economics*, Vol. 37, No. 3, Autumn.

[11]The two distinct groups of customers (holders of the payment instrument and merchants that accept it) are likely to face wildly different fee structures. It is even quite conceivable that one customer group actually pays a negative fee (that is, receives a fee) for using the product. For the current purpose, we can limit ourselves to the sum of the fees that are charged to merchants and consumers together.

[12]Bolt and Soramäki, "Competition, bargaining power and pricing in two-sided markets," DNB Working Paper 181 (September 2008).

[13]*http://www.nmanet.nl/nederlands/home/Actueel/Nieuws_Persberichten/NMa_Persberichten/2004/04_10.asp* (in Dutch).

[14]If the risks associated with the concentration of the infrastructure are considered to be too big, oversight may also require governance authorities to diversify and use multiple, distinct infrastructures.