Committee on Payments and Market Infrastructures

Non-banks in retail payments

September 2014

BANK FOR INTERNATIONAL SETTLEMENTS

This publication is available on the BIS website (www.bis.org).

ISBN 978-92-9131-650-2 (print)

ISBN 978-92-9131-655-7 (online)

Contents

Executive summary

The safe and efficient functioning of retail payment systems and instruments is a core concern of most central banks, reflecting the key role such systems play in the financial system and the real economy. As part of its on-going work in this field, the Committee on Payments and Market Infrastructures (CPMI)[1] highlighted the growing involvement of non-banks in retail payments in its May 2012 report on *Innovations in retail payments*. In a follow-up to this report, the Working Group on Non-banks in Retail Payments was set up to conduct an analytical study on this topic, including the possible implications for central banks.

For this purpose, the Working Group has defined non-banks as entities "involved in the provision of retail payment services whose main business is not related to taking deposits from the public and using these deposits to make loans". Regarding the scope of the payment services covered, this study includes all activities in the payment chain connected with widely used retail payment instruments such as credit and debit cards, credit transfers, direct debits, cheques, e-money products and remittances.

The study of the involvement of non-banks in retail payments was supported by two fact-finding exercises conducted by the Working Group. The fact-finding revealed that non-banks participate in all stages in the payment process and across all payment instruments. The Working Group categorises non-banks into four types based mainly on the stages of the payment chain in which they engage, the type of payment service provided and also their relationship with banks: (i) front-end providers that provide services directly to end users such as consumers and businesses/corporates; (ii) back-end providers that typically provide services to banks; (iii) operators of retail payment infrastructures; and (iv) end-to-end providers that combine front-end services to end users with clearing and settlement services.

Retail payment services have a number of characteristics that may attract non-banks. Payment services may allow non-bank entities to gain economies of scale and scope and to exploit opportunities for specialisation. Specific drivers for non-bank involvement in retail payments include (i) the trend for banks to outsource payments and technology-related services; (ii) changing payment habits and customer preferences, including the emergence of new payment needs; and (iii) technical and other innovations in payment methods. In addition to these market-driven factors, the regulatory environment can also influence non-banks' involvement in retail payments.

These drivers have implications for both the efficiency of retail payment systems and the related risks. As for efficiency, non-banks can use economies of scale or scope to bring down the cost of retail payments. Non-bank providers of front-end services may compete with banks to improve end users' access to retail payments by providing a broader range of payment options including new methods such as person-to-person proximity payments in place of cash. Competition may also lead to improvements in traditional payment systems, such as faster or round-the-clock retail payment services, and to lower costs for end users. In some cases the introduction of such services has occurred with official sector encouragement, and has involved collaboration between banks and non-bank technology providers. Further, in some segments and jurisdictions, non-bank involvement in payment services has made it easier to meet financial inclusion objectives.

By providing services at various points along the payment chain, non-banks may have implications for at least some types of risk arising from retail payment systems. These implications will

[1] The Committee on Payment and Settlement Systems (CPSS) changed its name to the Committee on Payments and Market Infrastructures (CPMI) on 1 September 2014. Please note that references to reports published before that date use the Committee's old name.

vary by the type of non-bank and service provided. Back-end providers may pose operational risks either through concentration – ie, in providing a specific service that, if disrupted, could have far-reaching repercussions– or through the challenges associated with outsourcing. They may also reduce risks through specialisation in services that provide more security along the payment chain. Front-end and end-to-end providers may also impact the risk of fraud or other consumer protection-related issues. The risks posed by non-banks in retail payments probably do not differ fundamentally from those posed by banks, especially when they are providing the same type of payment services. However, even if the types of risk do not differ materially between banks or non-banks, differences in the way that they are regulated could translate into differences in risk mitigation measures (and hence in the probability that risks might materialise and the potential impact).

Although the safety and efficiency of payment systems and services is typically a prime concern of central banks, the regulatory treatment of non-banks varies greatly across CPMI jurisdictions. This is true of the regulatory framework itself, the regulatory status of non-banks (including licensing requirements), the authorities involved and the regulatory tools they use. Regulation varies across jurisdictions according to the perceived roles and risk profiles of non-banks. How far non-banks have access to national payment systems and infrastructures also varies widely depending on relevant policies or regulation.

For central banks and other authorities, a number of issues arise from the growing presence of non-banks in payment systems. Some of these relate to operational risks, level playing field issues, consumer protection aspects or the risks that might emerge if outsourcing of payment services/activities is concentrated in a single or a few non-banks.

Central banks and other authorities may wish to take note and consider the implications of the issues that are analysed in this report, including risk and level-playing-field issues, and take action as appropriate in their jurisdictions.

1. Introduction

Retail payment systems and instruments play a key role within both the financial system and the rest of the economy. In March 2003, the Committee noted that "retail payment systems and instruments are significant contributors to the broader effectiveness and stability of the financial system, in particular to consumer confidence and to the functioning of commerce. Moreover, efficient and safe use of money as a medium of exchange in retail transactions is an essential function of the currency and a foundation of the trust people have in it. For these reasons, the efficiency and safety of retail payments are of interest to central banks."[2]

In the CPMI countries, non-financial institutions handle almost 300 billion non-cash payment transactions every year (the bulk of which are retail payments). This payments volume has been growing at more than 5% annually in recent years, implying that, on average, every individual now makes more than 70 cashless payments each year. In some of these countries, indeed, this average may exceed 300 payments per year.[3] Such figures not only demonstrate the importance of retail payments for the smooth functioning of the economy, but also suggest that even fairly minor disruptions in retail payments could have potentially significant effects on public services, business activity and everyday life. By the same token, even small increases in the efficiency of retail payments could yield considerable benefits for society as a whole, as recent studies show.[4]

Reflecting the interest of central banks in the safe and efficient functioning of retail payments, the Committee has published several reports relating to retail payments, of which the most recent, published in May 2012, covered innovations in this field. This report noted that the retail payments landscape has changed significantly in recent years, in line with evolving payment needs, product, process and technical innovation, as well as structural, business and regulatory developments. One of the trends identified was the increasing role of non-banks in retail payments. Seeking to understand and assess this trend, the Committee set up a Working Group on Non-banks in Retail Payments to conduct an analytical study and assess the possible implications for central banks. This report presents the Working Group's analysis and its findings.

The report is structured as follows. Chapter 2 proposes a definition of non-banks, outlines the methodology and the main results of the fact-finding exercises, and sets out a categorisation of non-banks in retail payments. Chapter 3 reviews the main factors influencing the increasing presence of non-banks in retail payments, while Chapter 4 addresses the implications for efficiency and risk. Chapter 5 describes the various regulatory and oversight approaches towards non-banks. Chapter 6 concludes with an overview of the main issues identified and sets out the challenges posed for central banks and other authorities. To support the analysis, the report generally draws on the outcomes of fact-finding exercises that were conducted in CPMI member jurisdictions.

[2] CPSS, *Policy issues of central banks in retail payments*, March 2003.

[3] This is the case, for example, in Australia, Korea, Netherlands, Sweden and the United States; Singapore, with 644 transactions per inhabitant per year records the highest figure. In contrast, other CPMI countries such as China or India record fewer than 10 cashless payments per inhabitant per year. For the 2012 figures, see CPSS, *Statistics on payment, clearing and settlement systems in the CPSS countries*, December 2013.

[4] See ECB, "The social and private costs of retail payment instruments – A European perspective", ECB occasional paper series, September 2012; N Jonker, "Social costs of POS in the Netherlands 2002–2012: efficiency gains from increased debit card usage", *DNB Occasional Study*, no 11(2), Netherlands Bank, 2013; and ECB, "Retail payments and the real economy", *ECB Working Paper Series*, August 2013.

2. Framework for the analysis

2.1. Definition of non-banks and scope of the report

This report focuses on the role of non-banks in retail payments. Neither term – retail payments and non-banks - is easy to define precisely. Retail payments are relatively low-value payments between consumers, businesses and public authorities. Typically, they account for most of the payments made within an economy, but only a small fraction of their total value. One common way of defining retail payments is to focus on the relevant payment mechanisms and instruments – this report considers debit and credit payment cards, credit transfers, direct debits, cheques, e-money products and remittances.[5,6]

For their part, non-banks are defined by what they are not – that is to say, providers of traditional banking services. A primary function of banks is taking deposits from the public and using them to make loans. As deposit-takers, banks have historically also served depositors as a gateway to the payment system. Non-banks might in principle be defined from either a legal or from a functional perspective. But, just as the legal definition of a bank varies widely from one country to another, most CPMI jurisdictions lack a common definition of non-banks in the field of retail payments. In many jurisdictions, there is no specific legal definition of non-banks, or various definitions may apply depending on the functions that a non-bank performs. Focusing on the functional definition of a bank, as outlined above, is therefore a pragmatic way to arrive at a definition of non-banks in retail payments, ensuring that a wide range of entities is included, but without needing to reconcile cross-country legal distinctions.

Therefore, for the purposes of this report, a non-bank is defined as: **any entity involved in the provision of retail payment services whose main business is not related to taking deposits from the public and using these deposits to make loans**.

This functional definition excludes entities such as saving banks, credit cooperatives or credit unions that provide payment services but whose main activity is related to taking deposits from the public and providing loans. However, an institution whose primary business is accepting funds from customers to provide payment services, rather than using these deposits to make loans, would be considered a non-bank for the purposes of this report, even if it has a banking licence. Similarly, an institution that in the course of its business offers payment services and extends credit, but does not accept customer deposits, would be classified as a non-bank in this report, even if it has a banking licence (eg a credit card issuer).

With regard to the scope of payment services, the main retail payment instruments are considered across all activities of the payment chain. As outlined above, the payment instruments included are credit and debit cards, credit transfers, direct debits, cheques, e-money products and remittances. In relation to the different activities that encompass the payment chain, for the purposes of this report, a categorisation involving the following five stages[7] has been adopted:

5 While cash belongs to the scope of retail payments, this report focuses exclusively on non-cash retail payments.

6 For definitions, see CPSS Glossary and the CPSS-WB report, *General principles for international remittance services*, March 2006. Given the variety of mobile payment solutions, mobile payments are not characterised as a separate payment product/instrument, but are included in one of the other instruments according to the specifics of the particular mobile payments scheme.

7 This categorisation is based on that used by the ECB and the Federal Reserve Bank of Kansas City (see *Nonbanks in the payments system: European and U.S. perspectives*, no PSR WP 07-01, Payments System Research Working Paper, Federal Reserve Bank of Kansas City, 2007). For the purpose of this report, however, an additional distinction is made between the clearing and the settlement stage, which according to the Working Group's fact-finding exercise can be characterised quite differently in terms of the level and intensity of non-bank involvement.

(i) Pre-transaction stage: This stage involves creating the initial arrangements required for payment processing, including customer acquisition, infrastructure setup, the establishment of agreements (such as security standards) and other service arrangements. The pre-transaction stage is not directly linked to any specific transaction(s), but is necessary to establish the contractual and technological infrastructure that allows payment processing.

(ii) Authorisation stage: The authorisation stage involves the creation, validation and transmission of a payment. It can include activities to verify the identity of the parties involved in the transaction, validate the payment instrument used, verify that sufficient funds are available, and communicate relevant information required to complete the payment and the payment processing.

(iii) Clearing stage: The clearing stage involves the exchange of relevant payment information between the payer's and payee's accounts, and the calculation of claims that need to be settled.

(iv) Settlement stage: The settlement stage involves the final discharge of a valid claim. It involves the movement of funds from the payer's account to the payee's account.

(v) Post-transaction stage: This stage involves the provision of value-added services after payment settlement has been performed, including the production of statements and dispute resolution processes.

A more detailed list of the different activities that are included in each stage can be found in Annex 1. The report covers non-banks that provide retail payment services at any or all parts of the payment chain (ie their participation in retail payments can extend across the entire payment chain or be limited to a single or a few activities in a specific stage) and for any or all types of retail payment instruments (ie they may offer services related to a variety of instruments or concentrate on a single one).

2.2. Summary of the fact-finding exercises

For a better understanding of the breadth and depth of non-banks' involvement in retail payments in the CPMI jurisdictions, the Working Group conducted two fact-finding exercises. The first focused on how far non-banks are involved in different payment instruments and across the different stages of the payment chain. The second exercise aimed to identify the key characteristics of non-banks in retail payments, such as the activities they perform, their relationship with banks, and the regulatory status of the main non-banks or categories of non-banks. This second survey also collected information on the regulatory measures implemented in various jurisdictions relating to non-banks, including policies related to the access of non-banks to payment systems. The goal of both fact-finding exercises was to obtain a high-level view of non-banks across the CPMI member countries; it was not designed to provide data for a formal quantitative analysis. Rather, the information was used to help identify and analyse key similarities and differences across jurisdictions.

In addition to the feedback gathered from all CPMI jurisdictions, the report also surveys other global developments and trends by incorporating selected results of the latest World Bank 2012 Global Payments Survey, which contains data and information from around 150 jurisdictions.

Overall, non-banks participate in all stages in the payments process and across all payment instruments. The degree of involvement and the type of activity conducted, however, differ by payment instrument, as in some areas and activities non-banks play a very important role, while in others their role is less significant.

Figure 1 below illustrates the presence of non-banks in the payments process based on the evidence gathered in the fact-finding exercises. It shows the degree of non-bank involvement in the five main stages and 23 sub-stages of the payment chain (see Annex 1 for details of the different stages and sub-stages) and for the different payment instruments covered in the report.[8] As the figure shows, non-banks participate in all payment instruments, although their presence is strongest in credit and debit cards, e-money products and remittances. Non-banks' provision of services related to other payment instruments, such as credit transfers, direct debits and cheques is less prominent, but still quite relevant. Similarly, the involvement of non-banks in the various payment stages varies according to both the activities in each stage and the type of payment instrument. For instance, non-banks have a quite significant presence in the pre-transaction stages for credit and debit cards, e-money products and remittances, but their presence is moderate in the case of other instruments.

[8] The figure shows the presence of non-banks in different stages and instruments according to the inputs provided by the Working Group members in one of the fact-finding exercises.

Figure 1

Involvement of non-banks across the payment chain in different instruments

Stage of the payment chain		Cheques	Credit transfers	Direct debits	Credit cards	Debit cards	e-money products	Remittance transfers
Pre-transaction	1. Customer acquisition							
	2. Services for issuer's front-end customer acquisition							
	3. Provision of payment instruments/devices to front-end customers							
	4. Provision of hardware to accept payment instruments/devices							
	5. Provision of software to accept payment instruments/devices							
	6. Provision of internet security-related technology/support							
	7. Payment card industry compliance services to merchants and/or payers							
	8. Provision of data centre services to back-end customers							
	9. e-invoicing							
	10. Communication connection for merchants							
Authorisation	11. Transaction authorisation (fund verification)							
	12. Fraud and risk management services to front-end customers (payees)							
	13. Fraud and risk management services to card issuers							
	14. Initiate the debiting of the front-end customer's (payer's) account							
	15. Ex-ante compliance services							
Clearing	16. Preparation							
	17. Clearing							
Settlement	18. Settlement							
Post-transaction	19. Statement							
	20. Reconciliation, incl. collection and receivable management services							
	21. Retrieval							
	22. Reporting and data analysis services							
	23. Ex post compliance services							

Darker color indicates higher involvement/importance of non-banks, light colour indicates no involvement. Shading within a cell indicates differences across countries.

2.3. A classification framework for non-banks

The retail payments landscape is characterised by a wide diversity of payment instruments and activities along the different stages of the payment chain. Non-banks involved in retail payments also reflect this diversity, as very different entities, performing different activities in various fields, can be identified. The working group identified a series of characteristics or dimensions by which the activities of non-banks in retail payments systems can be described and analysed. These dimensions serve as the basis for the categorisation of non-banks involved in retail payments.

A first dimension can be established according to the stages of the payment chain in which the non-bank is involved (see Section 2.1). Non-banks that are present in all stages can be differentiated from those that are only involved in one or two stages of the payment chain. Within those non-banks that do not cover the entire payment chain, further differentiation is feasible by taking into account the specific stages in which they are providing services.

Secondly, non-banks can also be differentiated according to the type of payment instrument or product they offer or support. Then those that provide services across all or many payment instruments can be differentiated from those that specialise in a specific instrument or product. For instance, in some jurisdictions, non-banks that provide e-money products or remittance services tend to specialise in these instruments.

A third dimension is the type of service provided. Some non-banks provide mainly front-end services to end users of payment services, ie payers and payees, whereas others concentrate on the provision of back-end services to banks and other payment service providers.[9] The provision of front-end and back-end services is not mutually exclusive, as some non-banks offer both types of services.

A fourth dimension is based on the relationship between non-banks and banks. Some non-banks provide services to banks under outsourcing agreements or other types of cooperative arrangements. In other cases, banks and non-banks may compete with each other, or a non-bank may cooperate with other entities in some stages of the payment chain (eg for the clearing and settlement of transactions) while competing with other non-banks and banks at other stages (eg in providing payment services to end users). Competition might be more evident when the non-bank provides services similar to those offered by banks, or less apparent when the payment service supplied by the non-bank has no equivalent in the range of services offered by banks. Even in this case, the new services are usually close substitutes for more traditional ones, so that some degree of competition between new and traditional services arises, given that both serve the same purpose of transferring money.

Non-banks can also be differentiated by their ownership status. Some may be owned by a bank or a group of banks, while others have no ownership relationship with banks. This dimension can be linked to the previous one, as non-banks owned by banks may be more likely to engage in a cooperative relationship with banks. In other cases, where there is no ownership relationship, a wider range of competing or cooperating relationships may develop.

An additional dimension that can be taken into account is the regulatory status of the non-bank. The functional definition of non-banks, as described in Section 2.1, does not differentiate between non-banks on the basis of their regulatory status. Thus, some non-banks included in the scope of the report could have a banking licence and may be considered as banks from a regulatory perspective in some jurisdictions. In other instances, non-banks might be regulated entities with a special status that differs from that conferred by a banking licence. In yet other cases, non-banks might be entities which

[9] In the context of this report, front-end services are those directly offered to the final user of a retail payment, ie payers and payees, which include consumers, retailers, non-financial corporations or public entities. Back-end services are those provided to another institution (eg a bank, another non-bank service provider or financial infrastructure) that participates in the provision of the payment service.

are not subject to any specific regulation in relation to the payment services they provide (apart from the general regulatory framework applicable to non-financial institutions in the respective jurisdiction).

To support further analysis, the working group decided to focus on three main factors or dimensions that are closely interrelated: (i) the stages of the payment chain in which non-banks are involved, (ii) the type of service provided by the non-bank (front-end or back-end), and (iii) the type of relationship they maintain with banks (reflecting differing degrees of cooperation or competition). This approach helps to clarify the economic rationale for the role of non-banks and their interactions with banks, and to illustrate the diversity of non-banks in retail payments. Further, the working group believes this approach strikes a balance between a classification based on a single dimension, which would not adequately represent the full variety of non-banks that provide retail payment services, and a classification that is based on every possible dimension, which would be too complex without necessarily being more informative.

Taking into account the three dimensions indicated above (stages of the payment chain, type of service provided, and predominant type of relationship with banks), a broad classification of non-banks into four distinct types of entities can be established:

i. **Front-end providers**: These are non-banks which typically provide an interface between end users of payment services (payers and/or payees) and the traditional clearing and settlement process. They are mostly present in the pre-transaction, initiation, and post-transaction stages of a payment, but usually not in clearing and settlement. Front-end providers may compete with banks in certain dimensions, but they typically cooperate with banks for the clearing and settlement of transactions. Typical examples of this type of non-bank are mobile wallets, internet payment gateway providers, credit card acquirers or, payment institutions and e-money institutions in the EU.

ii. **Back-end providers**: These are non-banks that mostly provide specialised back-end services to banks, often related to several payment instruments, via outsourcing arrangements or in the framework of a cooperative arrangement. They do not have a direct relationship with payers or payees and they generally focus on just one or two stages of the payment chain. Examples include information technology (IT) services, providers of data centre services, trusted service managers, data security firms, or entities that provide back office operations, anti-money laundering, audit or compliance.

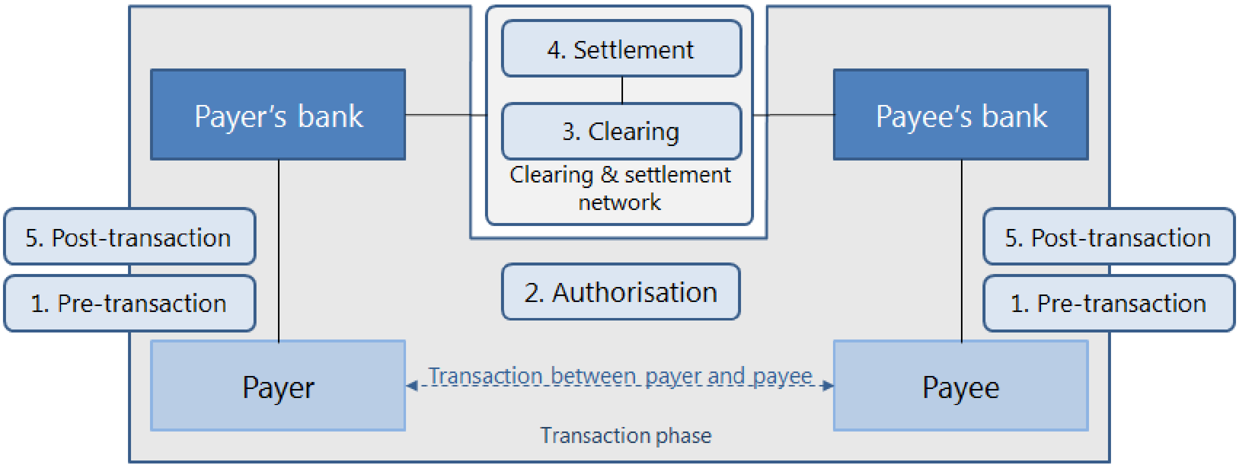
iii. **Operators of retail payment infrastructure**: These specialise in back-end clearing and settlement services, cooperating with banks and other payment service providers to whom they offer their services, usually in relation to different payment instruments. In some cases, these non-banks are owned by the banks participating in the arrangement. Examples in the card payment business would include card networks, such as Visa, MasterCard, or China Union Pay. They do not offer front-end or back-end services, but provide clearing and processing services for card transactions.

iv. **End-to-end providers**: This is essentially a combination of the foregoing categories. Payers and payees have a direct relationship with end-to-end providers, usually by maintaining an account with them. These providers are closed-loop systems in the sense that movement of funds from a payer's account to a payee's account does not necessarily require connections with banks, although banks may be used to fund or redeem end user accounts with the end-to-end provider. Some examples of this type of non-bank include operators of three-party card schemes, providers of certain e-money products, such as PayPal, and some operators of remittance services. End-to-end providers may also use other non-banks and banks as agents for the provision of some services. Notable examples are remittance service providers and e-money providers that use agents to offer cash-out and cash-in services.

The following figures[10] provide a simplified overview of the retail payment infrastructure and the four above-mentioned types of positions that non-banks may hold. Figure 2 below presents the traditional model of retail payments. Historically, when banks were the only entities providing payment services, all the steps involved in making a payment transaction were undertaken by the banks of the payer and payee. The figure below outlines this traditional retail payment environment: a range of banks provide retail payment services to end users (payers and payees) to facilitate payment transactions between them. The banks use market infrastructures to clear and settle the transactions (the settlement of the final positions might take place in a large-value payment system that is not shown in the figure for reasons of simplicity).

Figure 2

Retail payments landscape – stylised model

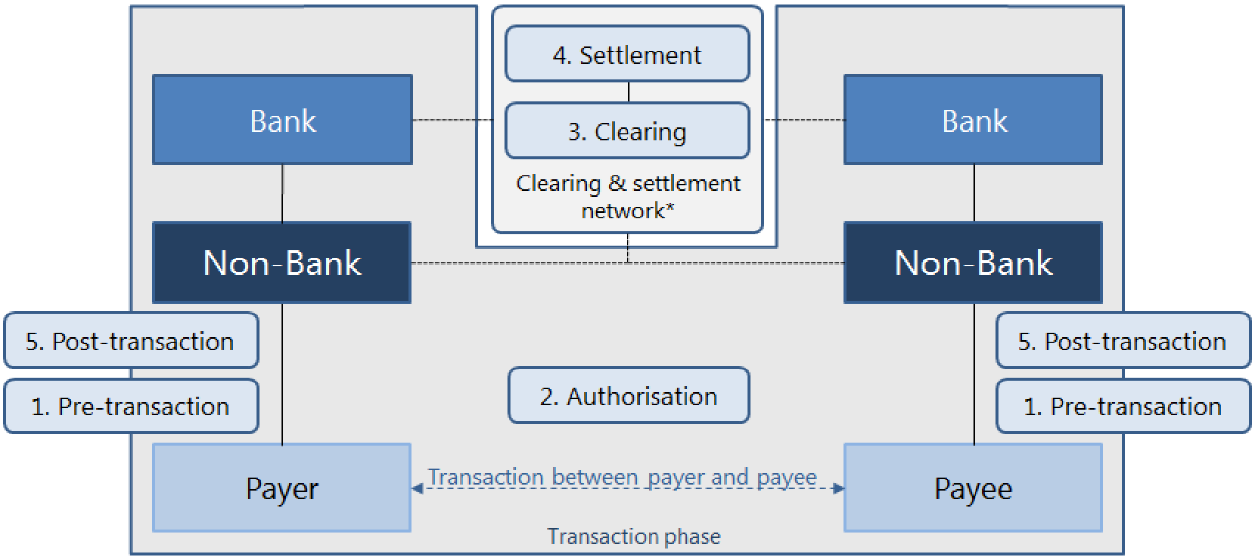


More recently, however, non-bank entities have become increasingly involved in various stages of the payment chain, depending on the type of service the non-bank is offering. The role of such non-bank entities is depicted in the figures below.

[10] In these figures, the various stages involved in a payment transaction are also depicted in the context of banks and non-banks providing payment services. Note that, depending on the position held by the non-bank (front-end provider, back-end provider etc.), activities involved in pre-transaction, authorisation, and post-transaction stages could be undertaken either by the bank or the non-bank entity – at the payer's as well as payee's end.

Figure 3

Front-end providers

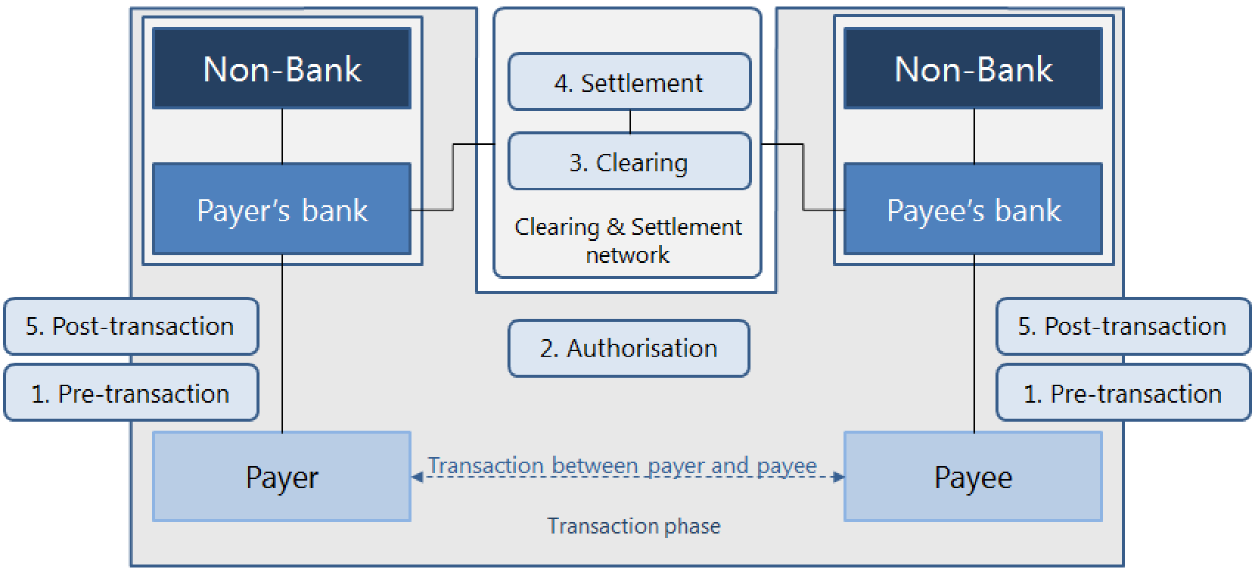


* Dashed lines reflect that access to clearing and settlement for non-banks may be direct or indirect.

Figure 3 above shows non-banks that can be categorised as front-end providers, which offer services directly to end users (payer and payee). They might provide only an interface between the users and their banks, or they might deliver payment services similar to those provided by banks. In the latter case, in order to obtain the necessary reach, non-banks need a connection to the retail payment infrastructure (for clearing and settlement services), either through a bank (indirect access) or by directly participating in the retail payment infrastructure (direct access).

Figure 4

Back-end providers



As shown in Figure 4 above, non-banks may provide specialised services that are outsourced to them by banks or by other non-banks. In such scenarios, it is the banks that have access to the clearing and settlement infrastructures. Besides providing services to banks in various stages of payments, the operator of the clearing and settlement component could also outsource some of the back-end services to a non-bank (although this is not reflected in the figure for reasons of simplicity).

Figure 5

Operators of retail payment infrastructures

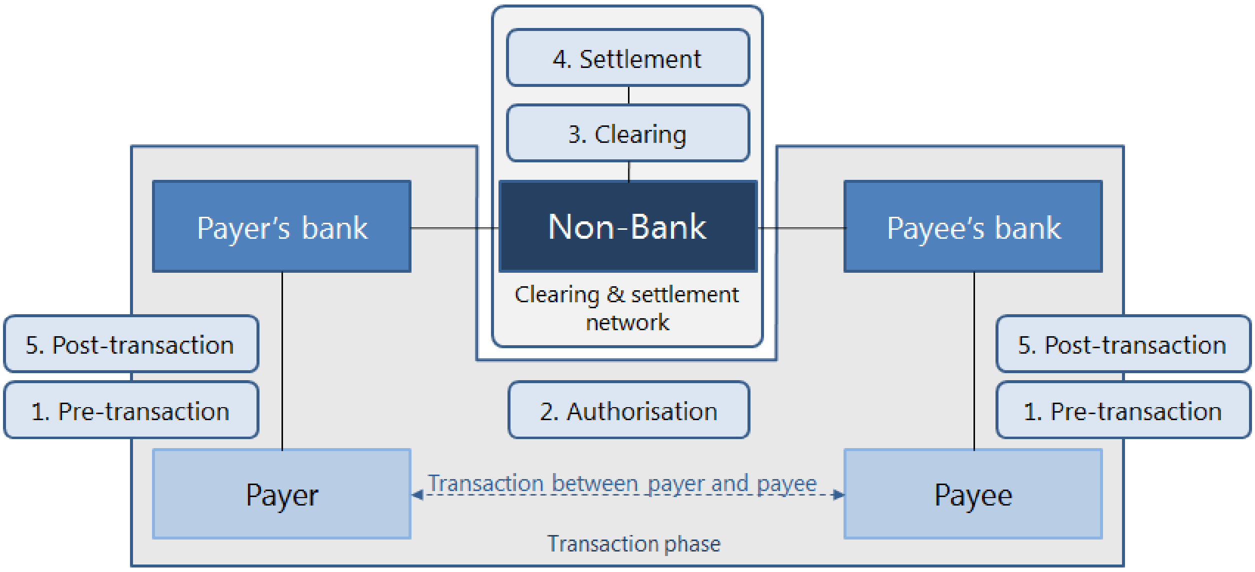
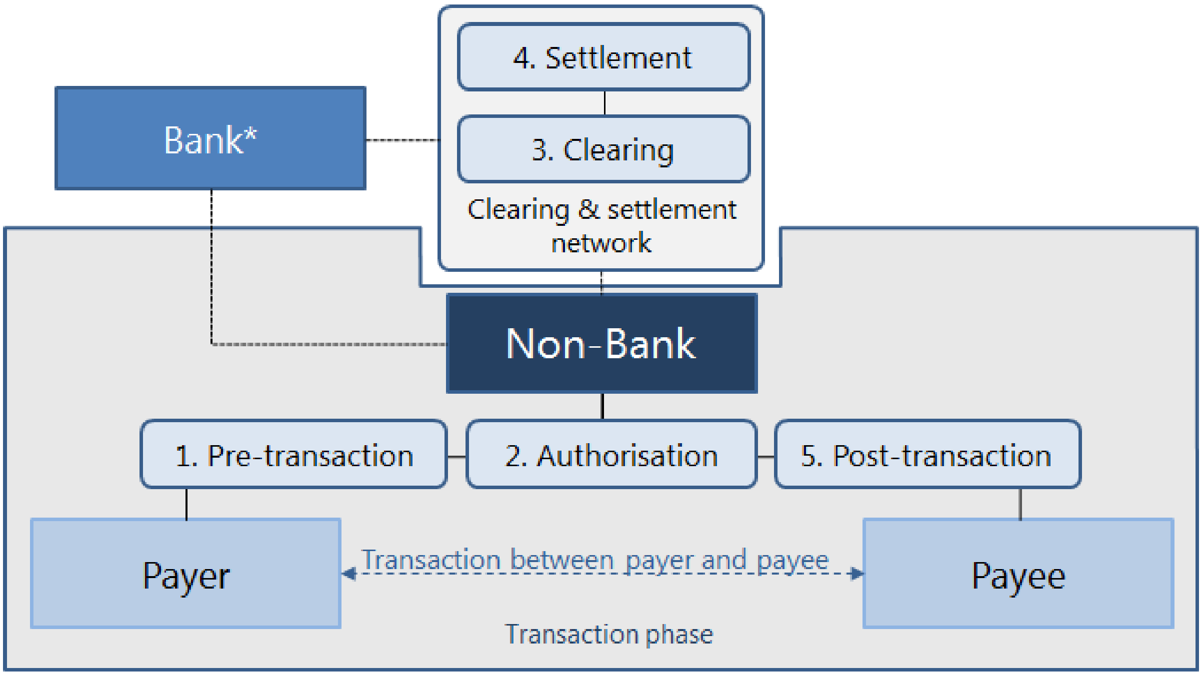


Figure 5 above shows how the clearing and settlement component of the retail payment infrastructure could be operated by a non-bank. This might occur, for example, when specialised activities in the clearing and settlement phase of the payment chain start to be undertaken by non-banks.

Figure 6

End-to-end providers



* Depending on arrangements for access to clearing and settlement, end-to-end providers may have direct access to a clearing and settlement network, or use a bank for parts of these processes.

Finally, non-banks may be classified as end-to-end providers. End-to-end providers may either offer services under a three-party model payment service (where the non-bank provides all services for transactions between its customers – both payers and payees) or they could be part of a platform in which other banks and non-banks participate. In Figure 6 above, the lower half depicts the scenario where the non-bank provides end-to-end services as a three-party service provider, thus undertaking pre-transaction, authorisation and post-transaction services. Typically, under a three-party model, there would be no need for clearing as the payment service is provided by the non-bank entity to its own customers. However, connections with end users' banks might be needed to send or retrieve funds to and from the scheme. In such cases, the end-to-end providers could be on only one side of the payment transaction (payer or payee) and will need to access the retail payment infrastructure either directly or indirectly.

This broad categorisation of non-banks is followed throughout the report, although other specific dimensions are mentioned when necessary. In any case, it should be noted that a wide variety of non-banks provide services related to retail payments, and in some cases it would be difficult to characterise a specific non-bank according to any of the categories outlined above, as its activities may span more than one category.

3. Factors influencing the increasing presence of non-banks

The presence of non-banks in retail payments is not new (eg non-banks were the earliest providers of credit and charge cards in the 1950s). However, recent years have seen a worldwide increase in the involvement of non-banks in retail payment services. This chapter briefly analyses the main economic characteristics of retail payment markets in relation to non-banks[11] and discusses the main drivers for their increased involvement in retail payments.

3.1. Economic characteristics of retail payment markets

In most cases, providers of retail payment services are motivated by the earnings potential. As documented in the CPSS report on *Innovations in retail payments*, a number of economic characteristics of the retail payment market may influence whether incumbents and new entrants provide new or improved retail payment services anywhere along the payment chain. These include both supply-side factors that deal with the "provision" of payment services and demand-side characteristics connected with the "consumption" of payments.

On the supply side, the provision of payment services can often generate economies of both scale and scope. Economies of scale arise when the average cost of producing a payment service falls as more of the service is produced. Economies of scope are generated whenever the processing of multiple products on the same infrastructure reduces unit costs or improves their quality. Thus, some non-banks may find it profitable to enter the payments market by taking advantage of economies of either scale or scope, or both.

On the demand side, the consumption of payment services often benefits from network effects, as each additional user increases the value of the network for all users. By the same token, new networks may be hard to establish because a critical mass of users is required to meet the network's start-up costs. Thus, when non-banks seek to provide payment services to new market segments, they are likely to face the challenge of finding a critical mass of new end users.

These economic characteristics can both help and hinder non-banks in their provision of retail payment services. For example, if a non-bank is able to anticipate that it can take advantage of economies of scale in a particular service over the long run, it is more likely to enter the retail payment market. Thus, economies of scale can serve as a driver. However, it may be hard for a new non-bank to establish the scale necessary to exploit cost savings in the short run, so that economies of scale may prove a barrier to market entry.

Whether a non-bank chooses to offer a new or improved retail payment service will depend on whether it can find a comparative or absolute advantage over existing banks in one or several areas. This may be the case if it can leverage an existing non-payments business into an advantage over banks, or if its payment services complement its existing business and can therefore be priced competitively vis-à-vis those offered by banks. For example, social networks, large e-commerce platforms, telecoms, and transport companies may be able to leverage existing networks of end users. Of course, banks may also be able to leverage their own account and financial services as well.

3.2. Drivers of non-bank activity in retail payments

The main drivers for the increasing presence of non-banks in retail payments emerge from both the demand and the supply sides.

[11] See CPSS, *Innovations in retail payments*, 2012, Chapter 3, for more information on the characteristics of the retail payment market.

Outsourcing of back-end services by banks to non-banks

Outsourcing involves the transfer of work to an outside third-party service provider. Although banks have outsourced specific back-end payment functions to non-banks for some time, increased competition and new technology have recently created more scope for such outsourcing.

Cost savings for the bank in providing payment services are the main motivation for the outsourcing of back-end services to non-banks, when this is possible. In such cases, a non-bank may have a comparative advantage in a particular back-end service, usually because it specialises in providing this service. This specialisation can lead to cost savings because of the particular expertise that a non-bank can offer, or because a non-bank can provide the service broadly (to many entities), taking advantage of economies of scale. For example, the provision of payment services typically requires information processing in large IT systems. Although such systems require large fixed-cost investments, once the investment is made, payment services can then be offered at competitive prices since the cost of processing each additional payment is marginal and economies of scale are fully exploited. By outsourcing some activities or by buying some services on the market, banks can avoid large fixed IT costs by sharing a platform with other providers.

For some time, banks have increasingly been outsourcing back office operations such as transaction management, reconciliation, reporting and item processing. More recently, they have also started to outsource pre-sales, customer service, information technology and human resources.

Changing payment needs and innovations in payment consumption

New opportunities for non-banks to provide both front-end and end-to-end payment services are emerging from changes in payment habits or customer preferences and the emergence of new payment needs. Some examples of these changes include a shift from paper to electronic payments, and the increased popularity of online consumer payments and mobile payments. Some of these preferences are related to workers' remittances, social benefit transfers, and efforts to expand financial inclusion.

Innovation has allowed non-banks to exploit the opportunities presented by changing payment needs, as noted in the CPSS report on *Innovations in retail payments*. Innovations let non-banks reach out to new segments of the retail payment market, meet new needs in an established segment, or supply specialised services to other payment service providers. For example, the issuance of prepaid products and the ability to use agents[12] let non-banks provide payment services that are distinct from those traditionally offered by banks and meet financial inclusion needs. As noted in *Innovations in retail payments*, about half of innovations principally in the mobile and internet payments field were owned either by non-banks or jointly by banks and non-banks. In the 2010 World Bank survey on innovations in retail payments, over one third of the innovations involved cooperation between banks and non-banks.

Some non-banks seek a comparative advantage over banks in the provision of front-end and end-to-end services. For example, non-banks with a large network of potential end users of payment services such as telecom companies, mobile network operators, internet service providers and web-based retailers can leverage network scale and economies of scope by adding payment services to their core businesses. In some cases, this tactic can also benefit a non-bank's primary business; for example, a telecom provider can improve the retention of its telecom customers by offering them mobile payment services. Such considerations could induce a non-bank to bundle payment services with its core product and offer them at a more attractive price or more quickly than a bank.

[12] The agents are typically existing businesses that provide the services using their existing business location and using their existing cash flow. They settle with the payment service provider periodically, often in real time and are paid for the service. In some countries, specialised entities (known as agent network managers) manage a network of agents and tie up with payment service providers to offer their agent network to their customers.

The growth of e-commerce has fostered the development of various new internet payment mechanisms. Although banks have extended various traditional payments products and services through the internet, this is an area where most of the innovation has come from non-banks, and banks have had to compete with such non-banks. Some non-banks have developed transaction services that reduce the amount and/or frequency of customer data-sharing, which may increase the attractiveness of such services to consumers over those of bank-provided equivalents. In such services, the non-bank acts as a "trusted intermediary" for the payment. The basic idea is that the consumer only has to provide key data to the middleman and all subsequent transactions only reference the consumers' wallet held by the middleman, so that no key information such as a credit card number is shared with the payee. Some of these entities have now enhanced their products to cover mobile payments and proximity payments too.

Social networks and online gaming have created various new payment needs, often for use within a limited ecosystem. Traditional payment products may not efficiently meet these payment needs, leading to the development of new products such as Amazon Coin, Facebook Credit (now discontinued) and the Linden Dollar. While the use of such products is currently still restricted to their respective ecosystems, it is conceivable that some of them may develop into more widely used payment services, as PayPal did. Moreover, non-proprietary forms of such alternative payment products have appeared, notably Bitcoin. Box 1 below briefly describes "virtual currencies" (deemed to be "virtual commodities" in some jurisdictions).

Box 1

Non-banks and virtual currencies

The development of virtual currencies is driven by increased internet usage and developments in cryptography as well as by enhanced processing power and the need to make virtual payments. Some are specific to a particular online community while others, in particular Bitcoin and similar concepts, may serve as an alternative means of exchange facilitating e-commerce and peer-to-peer transfers with varying degrees of anonymity. Virtual currencies may reduce transaction costs, and may expand global reach for some transactions. There is no universal definition of a virtual currency. Recent focus, however, has been on virtual currencies such as Bitcoin, which are decentralised (ie they have no central issuer) and are based on open-source protocols and cryptographic techniques.

Unlike bank money, electronic money, or prepaid/store value payment formats, virtual currency schemes are typically denominated in their own units of value rather than being tied to national currencies.

Virtual currencies may raise policy concerns, mainly related to consumer and investor protection and their potential for money laundering and criminal misuse. The public policy measures taken to date (in various CPMI and non-CPMI member jurisdictions) could be categorised as follows: (i) imposing restrictions on regulated entities for dealing with virtual currencies; (ii) adoption of legislative/regulatory measures, such as the need for exchange platforms dealing with virtual currencies to be subject to regulation as money transmitters, or the proposed regulation of virtual currency intermediaries in some jurisdictions for AML-CTF purposes; (iii) publication of statements cautioning users about risks associated with virtual currencies and/or clarifying the position of authorities with respect to virtual currencies; or (iv) monitoring and studying developments.

Virtual currency schemes, particularly decentralised ones, may operate without the involvement of traditional players in the financial system. The service providers that support their use may be non-bank entities, including exchange platforms and service providers that make the use of the virtual currencies more accessible. The conclusions of this report apply to non-banks providing services in virtual currencies in much the same way as non-banks providing services in traditional retail payments. However, specific issues related to the use of virtual currencies, such as money laundering and criminal use, are beyond the scope of this report.[13]

[13] The Financial Action Task Force (FATF) has recently published a report on these issues: *Virtual currencies, key definitions and potential AML/CFT risks,* June 2014.

Some non-banks may have a competitive advantage in providing front-end payment services in cooperation with banks. For example, a specific technological advantage could allow a non-bank to build a new access channel to an existing payment service and thereby facilitate payments. This gives the non-bank access to the bank's customers and allows the non-bank to leverage the bank's reputation while helping the bank to provide additional payment services, reach new segments of the retail payments market or provide existing payment services more effectively. This could create the conditions for a "win-win" situation for both the bank and the non-bank. Non-banks providing a technical solution that transforms a smart phone into a payment card terminal are one example of such cooperation. Payment aggregators, which provide services and infrastructure to link the systems of merchants with those of banks, are another. Business correspondents/agents also enable banks or other non-bank payment service providers to reach their customers more efficiently.

Innovation may fragment parts of the retail payment market, thus creating further opportunities for innovation and the entry of non-banks. For example, in parts of the retail payment market, the different types of new payment products created as a result of innovation have increased the complexity for payees, especially if they each have different interface requirements. This situation creates the need for payment aggregators or payment gateways, services that are typically provided by non-banks.

The complexity of payment products and services may also create the need to engage specialised firms to manage specific aspects of the payment system. While banks traditionally have a core competency in providing payment intermediation services, in some instances their expertise may not necessarily lie in developing technology to provide such an interface. This creates the need for payment intermediaries to better understand and be able to take advantage of the new payment products. In the past, a bank only needed to offer traditional payment instruments together with some basic internet payment services, whereas today consumers expect the bank to provide a wide variety of additional services, such as mobile payments, Europay MasterCard Visa (EMV) compliance, and Near Field Communication (NFC) functionality, to name but a few. This diversity may open up opportunities for specialisation and cooperation, whereby banks provide the basic payment services (building on their brand recognition and customer relationships) while non-banks (as front-end providers) provide the banks with the specialised technology that supports this increasingly diversified payments landscape. Both types of players can thus exploit their comparative advantages for mutual benefit.

Regulatory environment

A country's regulatory or legal environment can also impact a non-banks' involvement in retail payments, as the following cases illustrate.

Regulation may govern which entities may provide payment services to end users (payers and payees), thus restricting the participation of non-banks, particularly front-end providers. At one extreme, some regulatory environments may limit this activity to banks or require non-bank institutions to offer the service jointly with a bank. At the other extreme, the provision of services to end users may be completely unrestricted. According to the 2012 World Bank Global Payments Survey, non-banks such as post offices or mobile telephone companies were allowed to offer payment services in just over half of the countries surveyed.

Regulatory requirements for non-banks may reinforce public confidence in the robustness of non-bank payment providers of front-end and end-to-end services. For example, consumer protection laws that may apply to non-banks can reassure users that customer funds or consumer data are adequately protected. Also, non-banks that are subject to a licensing or supervisory regime may need to meet certain capital and/or data security requirements. In some cases, imposing an oversight regime on non-banks may establish the responsibility for ensuring that they meet minimum operational standards. Finally, in cases where non-banks may not be subject to such regulation, they may voluntarily comply with it in order to compete with banks that are regulated. However, complying with regulations can be costly for non-banks. As such, the relative benefits in public confidence versus the costs of compliance may influence how far non-banks participate in the provision of payment services.

Regulation may also (sometimes unintentionally) make it easier for non-banks to provide front-end and end-to-end payment services than it is for banks. This is particularly relevant in the provision of cross-border payment services, where banks may face higher regulatory requirements than non-banks to establish operations in another country. For example, non-bank entities such as Western Union, MoneyGram or UAE Exchange operate in a wide range of countries to cater for the migrant worker remittance market, as it is easier for them to operate than for banks to set up operations in various jurisdictions.

Whether or not non-banks can access a country's payments infrastructure, including payment card switches, ACHs, or RTGS systems, may also influence how far they participate in the provision of payment services – particularly front-end services. Non-bank access to specific payment infrastructures may be determined by regulation or as part of the rules and policies set by a system operator. Box 2 below provides an example of the rationale for allowing non-banks access to payment systems in Mexico.

Box 2

Non-bank access to large value payment systems: the case of the Mexican real-time gross settlement system (SPEI)

When SPEI started operations in 2004, only banks were eligible to participate. At that time, some non-banks, mainly broker-dealers, claimed that banks did not provide them with adequate payment services. The main complaints were: (i) restrictions on operating schedules –banks refused to receive payment instructions from some broker-dealers after 15:30, even though the banks were connected to SPEI and could still send transfers until 17:00; (ii) high fees – banks would charge fees depending on the transfer amount, especially for transfers sent by financial institutions; (iii) poor STP facilities provided by banks for their payment processes causing delays in payment processing (banks would delay sending transfers, particularly large ones). After investigating these complaints, the Bank of Mexico concluded that SPEI participants did not have sufficient incentive to offer adequate payment services to non-banks that were in competition with them. As a result, non-banks had to maintain accounts with each major bank and use manual processes that significantly increased their costs and operational risks.

In response to these findings, the Bank of Mexico's board authorised direct access to SPEI for all regulated financial entities at the end of 2005. Since then, any regulated financial institution can become a direct participant in SPEI. In 2010, Telecomm, a public telecommunication firm that provides remittance and bank-agent services mostly in remote villages, was also granted direct access to SPEI. By January 2014, some 44 non-banks participated directly in SPEI comprising 17 broker-dealers, four foreign exchange firms, seven insurance companies, 11 microfinance and financial services firms, two pension fund managers, two investment fund managers, and Telecomm. Combined, these participants represent 1.4% of SPEI's volume, and 2.6% of the value settled through the system.

In order to promote mobile payments and their interoperability, the Bank of Mexico issued new regulations at the end of 2013, and amended various provisions regarding SPEI rules so that mobile payment clearing houses were required to participate in SPEI and to receive mobile payments sent by other SPEI participants – including by other mobile payment clearing houses. By mid-2015, SPEI participants will have to process interbank mobile payments in less than 15 seconds (from initiation to funds posting), which is faster than the requirement for other SPEI transfers. In addition, participating institutions will have to gradually expand service availability for customers to a 20x7 schedule from the current 12x5 scheme. The Bank of Mexico also cut the mobile payment SPEI originating fee from USD 0.04 to less than USD 0.01. These changes are intended to promote mobile payments, helping them reach the underbanked part of the population and to increase financial inclusion.

4. Implications of non-banks for efficiency and risk

This chapter focuses on the impact that non-banks may have on the efficiency and risk of the retail payments system. In general, non-banks can improve the efficiency of the retail payments system by increasing competition, providing new or improved payment options, or reaching sectors of the population that did not previously have access to payment services. In other situations, non-banks can contribute expertise that the incumbents lack and cooperate with banks to provide innovative services such as mobile payments. At the same time, the growing involvement of non-banks could also impact risks in the system.

An in-depth analysis of these implications for efficiency and risk is amply warranted by the growing presence of non-banks in retail payments. The factors that underpin this trend include profitability pressures, as well as technical advances such as cloud computing, all of which make it likely that the trend for banks to outsource to non-banks will continue to the extent that banks can achieve cost savings through such practices. Additional supportive factors are the growth in electronic payments, the use of mobile phone and personal computing devices as transaction channels, and the rise of social networks. In particular, the interaction of social networks with retailing and advertising will drive demand for suitable payment mechanisms. Meanwhile, financial inclusion has become a key public policy objective in some countries, implying continued efforts to rapidly expand access to payment services for larger sections of the population.

4.1. Efficiency

Impact of outsourcing of back-end services by banks to non-banks

As mentioned in the previous chapter, non-banks may be able to provide back-end services at a lower cost than banks if they can take advantage of economies of scale or scope or both. Such cost reductions can be passed on to the outsourcing banks and, ultimately, to the end users of retail payment services. The cost advantages of providing these services will typically increase as the scale or degree of specialisation of the non-bank increases.

A potential consequence of these gains is that the provision of some back-end services may become concentrated in a small number of non-banks or even in a single firm. This could actually reduce efficiency if access to alternatives was so difficult that the service providers concerned were able to misuse their market power by providing their services at a lower quality or higher cost than under competitive conditions.

Competition between banks and non-banks that are front-end or end-to-end providers

As noted in the previous chapter, changing payment needs may induce non-banks to provide front-end or end-to-end payment services. In some cases, these non-banks will actually compete with banks for end users. This competition can have several implications for the efficiency of retail payments.

First, increased competition can potentially lower fees. For example, end-to-end service providers may try to undercut the processing fees that are charged in traditional forms of payment. This may put downward pressure on processing costs more generally.

Second, competition between banks and non-banks may broaden the set of alternatives open to end users. For example, competition in mobile payments has increased the range of payment methods open to consumers and merchants. Non-banks may be able to leverage economies of scope in other areas, such as location services on a phone, to lead to more targeted consumer offers that could benefit both consumers and businesses.

Third, non-banks may compete with banks in finding new markets for certain types of payments. As an example, online person-to-person card payments used to be virtually impossible because individuals could not accept a card payment without a costly card terminal and a contract with a merchant acquirer. Non-banks have found ways to fill this gap through front-end (eg PayPal) or end-to-end products that let users accept payments online without high setup costs. Some banks now offer competing services, giving end users more choices in how to make retail payments.

Finally, banks may also respond to the competition with innovations of their own, especially in front-end and end-to-end services. One example is the launch by Swedish banks of a real-time mobile payment service. Innovation often brings social benefits in the shape of more user-friendly, cost-effective and secure ways to pay for a variety of retail payments. This competition may also drive banks to improve existing payment methods. In some regions, this has led to the development of faster payments systems (in some cases allowing payment services to be provided on a 24x7 basis).

Cooperation between banks and non-banks

Banks and non-banks may also cooperate with each other, exploiting their respective competitive advantages to drive efficiency gains and generate economic benefits for both partners. For instance, banks may engage telecom providers as their business correspondents or agents for offering mobile-based payment services. Similarly, banks and non-banks may enter into co-branding agreements for payment cards whereby the bank acts as the payment service provider while the non-bank partner leverages its network for issuance and marketing. These cooperative arrangements can enhance overall efficiency in a way similar to competition, if, for example, the arrangements lead to innovations that lower costs or expand payment options for end users.

Non-banks and financial inclusion

Competition between non-banks and banks can serve financial inclusion goals. Unbanked individuals may be able to use non-bank services as an alternative to payment instruments offered by banks. Some mobile phone operators, for example, have been able to extend basic financial services to sectors of the populations that were not previously served by any financial institution.[14] Banks and non-banks can also cooperate to improve financial inclusion. Banking agents are a typical example of how the involvement of non-banks in retail payment services can have a significant impact on expanding financial and payment services to unbanked people.[15] Box 3 below outlines some case studies that illustrate the role of non-banks in financial inclusion, while Box 4 offers an overview of current CPMI work on payments and financial inclusion.

14 For example, see Consultative Group to Assist the Poor, "The role of mobile operators in expanding access to finance", brief, 2009.

For the case of Kenya see Consultative Group to Assist the Poor, "Poor people using mobile financial services: observations on customer usage and impact from M-PESA", brief, 2009.

15 For the successful case of Brazil, see Consultative Group to Assist the Poor, "Extending financial services with banking agents", brief, 2008.

Box 3

Non-banks and their role in financial inclusion: some case studies

Banking agents and mobile payments in Mexico

In 2011, financial authorities in Mexico, including the Ministry of Finance (SHCP), the National Banking and Securities Commission (CNBV) and the Bank of Mexico, issued regulations that allow banks to establish schemes that facilitate financial inclusion via cooperation with non-banks. This regulation also allows users to open low-risk banking accounts remotely (via a phone call or the internet) on the provision of basic identification information; such accounts have limits on monthly deposit amounts and may be linked to the user's mobile phone number, allowing the mobile phone to serve as a channel for payment instructions. The 2011 regulation was followed by amendments and new provisions regarding mobile payments issued by Bank of Mexico at the end of 2013:

Banking agents

Under the Credit Institutions Act, a bank may establish business relations with a banking agent (such as a retailer or store), so that the latter is authorised to offer financial services to its customers on behalf of the bank. The CNBV regulation allows banking agents to undertake activities such as receiving public utility and credit payments; cash deposits and withdrawals; issuance of payment cards; cheque deposits; balance inquiries and statements from accounts; or opening low-risk banking accounts. Since their adoption, banking agents in Mexico have increased the number of access points for financial services: the number of access points per 10,000 adults nationwide has risen to 4.76 (branches and agents) from 1.93 (branches only), a 147% increase.[16]

Mobile payment operators

Some mobile payment services in Mexico are offered by banks in cooperation with mobile phone operators, which play a fundamental role in providing the necessary communication services between account holders and their banks. Moreover, the mobile operators may also provide services such as bank account information hosting and clearing of transactions in the case that two or more banks operate a mobile payments clearing house.

Regulations issued by Bank of Mexico at year-end 2013 prescribe that legal entities that intend to operate as mobile payments clearing houses must apply for authorisation by the central bank, which will assess the fees charged to participants, entry conditions for new participants and risk management plans submitted with the application, and will ensure that the clearing house operates under competitive conditions.

Mobile payments clearing houses are required to participate in the RTGS system, SPEI, to ensure that all participants are interconnected.

Non-banks and financial inclusion in India

Although India has adopted a bank-led model towards financial inclusion, the policy approach envisages that non-bank entities can partner with banks in financial inclusion initiatives. Instead of setting up brick-and-mortar branches, banks now widely use non–bank business correspondents (BCs) or facilitators (BFs, similar to banking agents) to reach under- or unbanked segments of society in both remote and urban areas. As agents of the banks, BCs facilitate cash payments to and from bank account holders as well as non-account-holding customers. In addition, they are authorised to open information and communications technology-enabled (ICT) customer accounts. By means of these channels, BCs help to provide efficient and cost-effective access to banking services in financially excluded areas. Banks are gradually adding electronic remittance facilities to these BC outlets, thus providing customers with a link to mainstream retail payment systems.

Between March 2010 and March 2013, these policy measures have helped to increase banking outlets (including branches, business correspondents and other modes) in rural India fourfold to cover more than 268,000 villages. More than 109 million Basic Savings Bank Deposit Accounts (BSBDAs) have been opened during this period and more than 490 million ICT-based transactions have been carried out through BCs.

[16] CNBV, *Financial Inclusion Report 5*, 2013 (available in Spanish), http://www.cnbv.gob.mx/Inclusi%C3%B3n/Documents/Reportes%20de%20IF/Reporte%20de%20Inclusion%20Financiera%205.pdf.

Box 4

The CPMI World Bank task force on payments aspects of financial inclusion

Financial inclusion is increasingly becoming a key policy objective of most governments and central banks, both at the national and the international level, making it an important topic for international organisations and standard-setting bodies (such as the CPMI). At the November 2010 Seoul Summit the G20 leaders approved the "Financial Inclusion Action Plan". This plan recognises the commitments of the financial sector standard-setting bodies to "support financial inclusion" and encourages them "to further explore … complementarities between financial inclusion and their own mandates".

In this context the CPMI and the World Bank have set up a joint task force on Payments aspects of financial inclusion (PAFI). Members of the task force are senior representatives from CPMI central banks, non-CPMI central banks that are active in the area of financial inclusion and multilateral development banks. The task force started its work in early 2014 and aims to produce a report by late 2015.

The task force defines financial inclusion as the share of individuals and firms that use financial services offered by institutions that are authorised to offer these services. Typically, measures of financial inclusion consider a firm or individual "included" if they use at least one type of financial service. Non-users, or the financially "excluded", are typically defined as those that do not use any such financial service. The poor, the residents of rural or isolated communities and small businesses tend to dominate the ranks of non-users, especially, but not exclusively, in developing economies.

Payment services have drawn increasing attention since the late 2000s as a means to expand financial inclusion and measure inclusion. This reflects remarkable advances in information and communication technology, which offers the potential to greatly ease physical barriers to user access and facilitate increases in the efficiency of retail payments. The attention also reflects changes in business models, savings generated through migration from paper- and cash-based government payments, and a growing appreciation of the needs of the poor for payment services. Yet, the adoption and usage rates of payment services remain low and uneven. Even where adoption has been relatively robust, the impact on access to and usage of other financial services has been more limited than anticipated. This can be attributed, in part, to the lack of interconnectivity of predominantly proprietary innovative systems with other retail payment systems, both "traditional" and innovative, and the broader financial system.

4.2. Risk

In any retail payment system, certain risks may arise between the initiation of a transaction and its final settlement, including fraud, operational, legal, settlement and systemic risks.[17] In many cases, these risks may arise whether the services are provided by banks or non-banks. However, potential regulatory differences between banks and non-banks may lead to differences in risk mitigation measures (and hence on the likelihood that risks will materialise and their potential impact).[18] This is especially relevant because of the growing involvement of non-banks at various points along the payment chain. The implications will vary by the type of non-bank and the services that they provide. The paragraphs below outline some relevant risks.

17 See CPSS, "Clearing and settlement arrangements for retail payments in selected countries", September 2000, especially Chapter 4.

18 Regulatory approaches towards non-banks are covered in Chapter 5.

Concentration can impact operational risk

As mentioned previously, non-banks may specialise in certain services, thus generating large economies of scale or network effects. The nature of these effects could mean that the provision of such services may converge towards a small number of large providers, or in the extreme, a monopoly over the provision of a certain payment service.

If a service is localised in a particular non-bank, operational risk may also be concentrated there. For example, a (non-bank) technology service provider may offer a similar payment service to numerous banks, processing significant volumes on their behalf. Thus, an operational disruption at the non-bank provider could have a significant impact on all retail payment system participants. Or the banks could fall into a situation of regulatory non-compliance if the non-bank provides a faulty service to them or fails to carry out system changes required in time to meet current demands or new regulatory requirements.

Just because a back-end service is concentrated does not necessarily imply that there is a greater operational risk. For example, when the number of service providers is small, it may be easier for them to conclude agreements on back-ups and redundancy to make up for a disruption in one provider. Also, a small number of providers may make it easier for banks to monitor the performance of a few known entities rather than many less-established ones.

Outsourcing can impact operational risk

An important feature of non-bank involvement in payments is outsourcing. Banks and non-banks normally enter into cooperative or outsourcing arrangements with a specific objective and for mutual benefit. Outsourcing may reduce operational risk in some circumstances. For example, a non-bank that specialises in providing information technology services may be more effective in preventing operational disruptions than a bank that had to create its own information technology infrastructure.

However, an outsourcing contract cannot specify all possible contingencies that can occur. As such, there may be greater uncertainty regarding operational risks, which are potentially more challenging for a bank to manage than if the service were provided in-house. Indeed, some of these operational risks might only become clear once they materialise. Of course, because banks face reputational risk if disruptions occur, they have an incentive to anticipate possible disruptions and conclude outsourcing contracts that help to mitigate that risk.

Even with such outsourcing contracts in place, banks will need to pay more attention to incident response strategies, and to clearly define the responsibilities of the parties involved (both in normal circumstances and in case of contingencies).

Fraud and other risks related to consumer protection issues

Fraud could lead to a financial loss for one of the parties involved and may reflect inadequate security arrangements. An end user's account could be fraudulently debited, for example, if payment information or account information were stolen. Other examples of fraudulent activity include phishing for a PIN code to gain access to an e-wallet or using a false identity to obtain remote access to a front-end provider's server.

Fraud may happen on a large scale because of a data security breach at a payment provider or party that stores payment information anywhere along the payment chain.[19] While massive data security breaches can occur anywhere along the payment chain, fraudsters are likely to target the points at which data security is weakest. Inadequate data security at a non-bank service provider puts end users at risk of

[19] This includes retailers that store payment data.

fraud. Although non-banks are not more or less susceptible to a data breach than banks are, the presence of multiple providers may complicate efforts to ensure adequate security at every step of the payment chain.

Additional risks arise from consumer protection issues. For example, the ownership and use of customer data by non-banks could raise concerns about privacy. Front-end providers of mobile payment devices may have data related to a consumer's transactions patterns, locations, and other interests that could be combined with payment activity and sold to other parties, perhaps without the consumer's knowledge.

Another consumer protection issue relates to the protection of consumers' funds when these are held with a non-bank, especially in the event of the non-bank's default. End user accounts with non-banks such as end-to-end service providers may have positive balances during the time period between payment transactions. Such a non-bank, if it is not subject to appropriate capital and liquidity requirements, may not maintain sufficient liquidity to honour the timely withdrawal of those funds, with the risk that end users may not be able to access their funds. Again, it should be emphasised that these issues are similar for banks and non-banks, but differences in risk management or in applicable regulation may influence the probability of occurrence or its impact.

Increased complexity along the payment chain may introduce some legal risk

Legal risk arises if the rights and obligations of parties involved in a payment are subject to uncertainty. The presence of non-banks along the payment chain adds additional complexity to transactions that may contribute to legal uncertainty. Front-end providers may offer a new way to access traditional payment systems. For example, mobile wallets may work in such a way that transactions are split into two or more components. To an end user, these additional transactions may appear differently on an account statement as compared with a simpler transaction. Thus, end user disputes and error reports may be harder to resolve, given the uncertainty as to which parties are responsible for specific issues. Such issues may arise, for example, if there is uncertainty whether legal provisions for retail payments apply in such circumstances. Another example of potential legal uncertainty relates to the legal protection for customer funds pooled in trust accounts, which are a common feature of many e-money products and bill payment services.

Box 5 below provides a case study of how efficiency considerations can concentrate services in a single non-bank, and the implications for payment system risks.

Box 5

An example of concentration of risk: the card payments infrastructure of a country in the euro area

In the 1980s, a joint subsidiary was set up by the banking community of a country in the euro area to provide acquiring and clearing services for credit and debit card payments, and to operate the domestic debit card scheme. This company also produced hardware for card payments (in particular terminals and chip cards) and provided services to card issuers (such as a centralised blocking facility for lost and stolen cards and secure card personalisation services). The decision to create a single company was based on previous experience with the domestic card payment infrastructure, which suggested that the national market was then too small for competing players (i.e. no critical mass could be attained). As a result, this firm, which was sold by its shareholders to a pan European IT service provider in 2005 has had a dominant position in the national card payments industry from the outset. The company plays a critical part in most layers of the market, including the provision of networks for POS and interbank ATM operations (Switch), the acquiring of national and international debit and credit card payments, and the operation and management of domestic debit card and electronic money schemes.

The complete dependency on that company for the smooth functioning of nationwide card payments highlights the concentration risk that can arise from the dominant position of a single non-bank in particular sectors of the payment industry. The critical nature of that company is not related to the potential impact it might have on the financial system (it is not a systemically important institution) but to the potential impact on the economy that any disruption of its activities might have. A key consideration when assessing that risk is the fact that no competitor would be able to take over this company's business in the short run. Should this central actor suffer an outage, card payments – which are intensively used in the country – would be subject to large-scale disruption, and economic agents would then be forced to fall back on alternatives, most likely cash, for face-to-face payments. The increasing importance of card payments and the lack of suitable alternatives make the role of this firm even more crucial for the economy and the risk even more critical than previously. A default by the company would trigger a loss of confidence in crucial payment instruments and have adverse effects on the real economy.

This central card payment actor has been subject to oversight by the central bank since the mid-1990s. Initially, this oversight focused on e-money products. Reflecting the company's pivotal role and the related concentration risk, the scope of oversight was extended over time. The company has been subject to prudential supervision since 2011, when it became a Payment Institution (see Box 7).

Currently, competition in the national card payments market has already increased (eg with cross-border acquiring) and SEPA promotes even more competition for some activities relating to card payments. Consequently, it is expected that competition at the national level will intensify in the near future. In contrast, SEPA could promote increased concentration at an international level by paving the way for cross-border mergers between players seeking economies of scale, thus creating multinational infrastructure firms that would process huge volumes of transactions across Europe.

5. Regulatory framework for non-banks in retail payments

In the light of the efficiency issues and the risks outlined above, this chapter discusses the regulatory frameworks that exist to address these issues. A regulatory framework can influence the type of services non-banks can provide, the conditions under which they can provide them and the requirements they may have to fulfil.

For the purposes of this report, the regulatory framework is broadly defined, taking into account a wide range of regulations (eg including laws, regulations, directives, circulars and ordinances). Less formal measures such as market self-regulation and best practice (such as industry codes of conduct)[20] were also taken into account. Central bank oversight of payment and settlement systems[21] in relation to non-banks is also relevant in several jurisdictions, and will be highlighted throughout the chapter, as this is a specific role of central banks that can be used to gather information on the activities of non-banks, assess the safety and efficiency of the services they provide, and, ultimately, induce

[20] As an example, in the EU, self-regulation has helped shape the market, in relation to the development of both retail payment schemes and infrastructures. In particular, rulebooks for credit transfer and direct debit schemes as well as a framework for payment cards have been produced by the European Payments Council (EPC), a decision-making and coordination body for European payment service providers, and generally adopted in the market. Regarding infrastructures, the European Automated Clearing House Association (EACHA) has operated as a forum for technical cooperation between European ACHs, and has developed a framework for their interoperability.

[21] Oversight is usually defined as "a central bank function whereby the objectives of safety and efficiency are promoted by monitoring existing and planned systems, assessing them against these objectives and, where necessary, inducing change". See CPSS, *Central bank oversight of payment and settlement systems*, May 2005.

change and set requirements for the provision of these services in jurisdictions where central banks have such authority.

The broad payment system objectives of central banks – and in some cases, those of other authorities – focus on the safety and efficiency of payment systems. The specific objectives of many laws and regulations relating to payment services generally fall into these two areas, although they may be approached by different authorities from different perspectives (eg payment system oversight, prudential supervision, consumer protection or anti-money laundering). The focus of this chapter is the regulatory conditions that are specific to non-banks and the main differences in relation to the regulatory framework applicable to banks for the provision of retail payment services.

5.1. Overview of relevant authorities

As discussed in earlier chapters, non-banks are very diverse, and are often involved in a range of activities. Thus there may be more than one authority that can potentially interact with non-banks and regulate their activities. To analyse their role, it is important to distinguish between authorities responsible for issuing regulation and those charged with its implementation.

In most jurisdictions, either the government or the legislative authorities are responsible for issuing primary legislation with an impact on non-bank activities. Secondary regulation is needed in some cases to develop the details and requirements of primary legislation. In those cases in which secondary regulation has been reported, a majority of responses point to the central bank as the responsible authority.

Various types of authority are involved in implementing regulation and ensuring compliance with the regulatory framework applicable to non-banks. Implementation of different regulatory rules can be assigned to different authorities based mainly on the legal status of the non-bank (an institution-based approach) or on the activities it performs (functional approach) and the governance structure of the oversight function. Central banks are a key authority in many jurisdictions, but not in all cases or for all areas. In relation to retail payments, central banks may undertake a range of roles, including those of catalyst, overseer and system operator. These roles are developed in more detail, in view of the issues identified, in the following chapter.

In some jurisdictions, if a non-bank (according to the functional definition used throughout the report) acquires a banking licence, it will be subject to the same supervisory regime as a bank. In other cases, a licensing regime specifically tailored for institutions that provide retail payment services has been established. Sometimes, prudential supervisors or central banks (in some cases a single institution assumes both roles) are given the mandate to supervise these institutions.

Other authorities that may play a role in the regulation of non-banks are consumer protection authorities, competition authorities, telecom regulators, law enforcement agencies and/or specialised bodies within the different ministries of economy or finance (to deal with AML-related issues, for example).[22] Even though multiple authorities might potentially take an interest in non-bank activities in retail payments, the number of authorities actually involved in their regulation may frequently be quite restricted when a single authority holds several mandates, as in the case of a central bank that also has responsibility for prudential supervision of entities with banking licences. In other cases, several

22 For example, in India, the Telecom Regulatory Authority of India has issued guidelines to telecom operators on service standards that have an impact on mobile-based payment services.

authorities might be in charge of regulating and supervising the same type of non-bank, according to the geographical area in which the non-banks operate.[23]

Overall, the types of authority and their involvement vary according to the diversity of legal and institutional arrangements. This suggests that a certain degree of coordination among authorities may be necessary in order to effectively implement a regulatory framework for non-banks. In cases where more than one authority is charged with enforcing a regulation applicable to non-banks, there is usually a formal cooperative framework between the responsible authorities. In some cases, this framework might not be strictly necessary if there is a clear demarcation of responsibilities based on geographical or institutional criteria. In other cases, no formal coordination is needed if there is a clear hierarchical relation between authorities, in which one authority acts as the primary regulator and the second has delegated powers.

In contrast with the situation at the national level, there is only limited international coordination in relation to the regulation or oversight of non-banks that operate across borders, despite the fact that many non-banks offer cross-border services.

In addition to regulation, the broader involvement of stakeholders is gaining significance within the regulatory landscape. In some jurisdictions, industry associations or self-regulatory organisations representing a wide range of non-banks have been set up, or there is official encouragement for their establishment. These bodies can interact with regulators and other industry participants to represent industry views and share common interests from a non-bank perspective.

5.2. Regulatory approaches towards non-banks

In many cases, banks have been the traditional providers of payment services, especially front-end services to payers and payees. As a result, the regulatory framework for payment services may reflect the assumption that banks were the typical providers of these services, and take an institutional approach (ie regulation focused on banks). The outcome would thus be regulatory environments for these services that differ according to whether they are provided by banks or non-banks.

A basic function of a bank is to act as a financial intermediary by accepting deposits from the public and using those deposits to make loans and much of banking supervision is linked to this intermediation activity. The primary objective of such supervision is to reduce the level of risk to which depositors and other bank creditors are exposed by promoting the soundness (solvency) of individual institutions. Regulations for retail payment services have not been the main focus of the regulatory framework devised for banks, although they may play some role in that framework. Nonetheless, the requirements imposed on banks on account of their deposit-taking function may help contain the risks related to the provision of retail payment services.

Some non-banks carry out activities that are similar to those of banks in certain ways. For example, end-to-end providers may accept funds from customers and place them in accounts from which customers can make payments. Yet, these accounts may differ from traditional banking deposits in that the funds are not used to make loans but rather only to make payments. As such, these accounts may not be subject to certain types of protection, such as deposit insurance, in some jurisdictions. Non-banks that do not directly accept funds from customers usually specialise in activities that are very different from those performed by banks. Examples include front-end providers that merely interpose themselves between customers and financial institutions (eg aggregators or non-banks providing online

[23] This is the case, for example, in the United States, where certain types of non-bank may be subject to supervision from a range of different state supervisory authorities.

payment account access services[24]), as well as those that provide IT back-end services to other entities or offer clearing and settlement services.

Due to these differences in terms of services provided, the regulatory approaches to non-banks differ from those applicable to banks, and are at the same time very diverse and not necessarily mutually exclusive. Some of the situations reported include the following:

- Some non-banks have acquired a banking licence due to a regulatory requirement (or in some cases on their own initiative). Some examples are PayPal in the EU (see Box 6), or the international card schemes such as Visa or American Express in certain jurisdictions.
- Other non-banks have a specific status or licence (other than a banking licence) in relation to the payment services they provide, as is the case with payment institutions licensed under the EU Payment Services Directive (see Box 7), banking agents in Mexico, money transmitters in various states in the United States or Octopus in Hong Kong SAR.
- In some cases, a particular non-bank may be registered (with the central bank or other authorities) but not actively supervised or overseen. Examples include agents of remittance service providers in several jurisdictions. In the EU, this is also the case for payment service providers that have been exempted from licensing based on certain criteria.
- In other cases, such as Mexico's mobile payment clearing houses, Atos Worldline in Belgium and non-banks operating ACHs in many other jurisdictions, the non-bank is subject to the central bank's oversight of payment and settlement systems.
- A common approach applied to non-banks that specialise in the provision of back-end payment services through outsourcing contracts is that they are indirectly subject to the regulation that is applicable to the entity outsourcing the service. For example, in India, many banks outsource their systems for scanned image-based cheque clearing. This outsourcing activity typically does not fall under the purview of payment systems regulation or oversight, but it is subject to indirect regulation under banking supervision for outsourcing of activities by banks. Bank supervisors in the United States have statutory authority to examine non-bank service providers that enter into arrangements with their regulated financial institutions. In Saudi Arabia, the Saudi Arabia Monetary Agency (SAMA) regulates outsourcing activities, defining the areas of transaction information and activities that may be outsourced on a cross-border basis.
- Finally, some non-banks are neither specifically regulated nor are they overseen in relation to the payment services they offer.

Within jurisdictions, it may be the case that the regulatory framework for non-banks varies according to the role and type of service provided by non-banks. For instance, in India, while non-banks offering payment, clearing or settlement services in retail payments are required to be specifically authorised by the central bank under the payment system regulation, other groups of non-banks that function as aggregators or intermediaries do not require such a licence but are subject to regulation on access to participants' funds. Other types of non-bank that are pure back-end providers are not subject to any direct regulatory requirements.

A given non-bank with cross-border operations is likely to be treated differently in different countries, as regulatory approaches tend to vary widely between jurisdictions. Non-banks providing similar services in a number of countries may have a different status in each of their operating

[24] Online payment account access services can involve account information and/or payment initiation services. Both types of service require some degree of access to the user's payment account(s). The former provides account holders with (consolidated) information on their account(s). The latter consists in initiating transactions via a user's internet-enabled payment account, with or without the payee's active involvement, and with or without the payers sharing their credentials.

jurisdictions. PayPal, for instance, is not specifically regulated with respect to the payment services it provides in some jurisdictions, such as Switzerland or Canada. In other cases, including the United States, it has a specific licence or licences (distinct from a banking licence) to operate. In the EU, it has chosen to operate with a banking licence but it could, in principle, provide its services in some other form (eg as a payment institution). Taking into account the similarities of the services provided, these differences seem quite noticeable. Box 6 below provides a more detailed discussion of the different regulatory approaches in relation to PayPal, as an example of a non-bank with an international scope.

Box 6

Approaches to the regulation of an international non-bank: the case of PayPal

PayPal is subject to varying regulatory regimes around the world, with regulation generally focusing on its operations as a provider of stored value facilities for making payment for goods and services online. In most jurisdictions, its operations are limited to "electronic money" as opposed to traditional banking activities. PayPal is also typically subject to regulations such as minimum liquidity/capital requirements and anti-money laundering and counter-terrorism financing (AML/CTF) laws.

United States

PayPal is currently licensed to operate as a money transmitter in 45 US states and two territories, and as an escrow agent in one other state. While specific requirements vary from state to state, similar criteria tend to be used in defining money transmitters. Most states regulating money transmitters require a surety bond, which serves as a guarantee to the state that the money transmitter will comply with state regulations and not misuse customer funds. PayPal is also registered with the US Treasury Department as a money services business.

In 2002, the Federal Deposit Insurance Corporation (FDIC) stated that it does not consider PayPal to be a bank as it is not involved in the process of accepting deposits for the purposes of making loans under the Federal Deposit Insurance Act of 1950 (which requires a banking charter under US law). As with other US financial institutions, PayPal is subject to AML/CTF laws and consumer protection regulations such as the Electronic Fund Transfer Act 1978.

European Union

In the EU, PayPal is prudentially regulated as a bank by Luxembourg's banking authority, the Commission du Surveillance du Secteur Financier (CSSF). Formerly, from 2004 until 2007, PayPal Europe was licensed as an electronic money issuer with the UK Financial Services Authority. Under the current regime, PayPal Europe is subject to the same requirements as Luxembourg's banks. However, PayPal's main service is the issuance of "electronic money". As this does not constitute deposit-taking, the funds received in exchange of electronic money are not protected by Luxembourg's deposit guarantee system.

PayPal Europe implements its localised services in other EU countries through a "passport notification" process between the Luxembourg regulator and those of other EU member states. This process allows financial services operators legally established in one EU member state to establish or provide their services in other member states without further authorisation. In addition, PayPal is subject to the national law of each EU country, including the national implementations of the EU Payment Services Directive (PSD).

Australia

PayPal is currently prudentially regulated by the Australian Prudential Regulation Authority (APRA) as a provider of purchased payment facilities (PPFs). Under the Payment Systems (Regulation) Act 1998, holders of stored value in relation to PPFs are required to be an authorised deposit-taking institution (ADI) supervised by the Australian Prudential Regulation Authority (APRA), or authorised (or exempted) by the Reserve Bank. An additional requirement (from the Banking Act 1959 and Banking Regulations 1966) is that PPFs that are redeemable for Australian currency and available on a wide basis must be ADIs.

As an ADI, PayPal is subject to capital, liquidity and other operational requirements and must not undertake other banking business. PayPal is also the holder of an Australian financial services licence (AFSL) issued by the Australian Securities and Investments Commission (ASIC). As with other reporting entities in Australia, PayPal must comply with AML/CTF legislation enforced by the Australian Transaction Reports and Analysis Centre (AUSTRAC) and with various other consumer protection and competition regulations.

Singapore

For all markets outside the United States, the EU, Australia, Brazil, Canada, and Russia, PayPal Inc operates through its wholly owned international headquarters located in Singapore, PayPal Private Ltd.

In Singapore, PayPal Private Ltd is considered as the holder of the PayPal stored value facility (SVF) by the Monetary Authority of Singapore (MAS) under the Payment Systems (Oversight) Act 2006. PayPal is not considered to be a deposit-taker under the Banking Act 1970. PayPal does not hold a remittance licence in Singapore, and is thus unable to undertake remittance payments from Singapore. As an SVF holder, PayPal is required to comply with the Notice to Holders of Stored Value Facilities on the Prevention of Money Laundering and Countering the Financing of Terrorism.

Holders of SVFs in Singapore are also encouraged to adopt the practices set out by the MAS in their Guidelines on Stored Value Facilities, which recommends sound principles and risk-mitigating measures for the operation of an SVF. The Guidelines address issues such as transparency, disclosure, protection and redemption of stored value for users of an SVF.

Mexico

As of March 2014, PayPal in Mexico is regulated as a payment aggregator (an entity which allows merchants to accept card payments) under provisions issued by the Bank of Mexico and the National Banking and Securities Commission (CNBV) for card payment networks. However, the evolution of PayPal's role in the payments system landscape in Mexico could change its regulatory status in the near future.

Under current provisions, PayPal and other payment aggregators are required to: (i) report to the central bank and the CNBV the fees, discount rates or any other charges that apply to services related to the reception of card payments; (ii) provide account statements to their clients at least quarterly, including disaggregated information related to the number and amount of card payments processed by the aggregator, the fees charged for the services provided by the aggregator, as well as discount rates charged by the corresponding acquirer to the aggregator; and (iii) observe security measures regarding the transmission, storage and processing of sensitive information.

Russian Federation

According to the Russian Federal Law on the National Payment System, only credit institutions are allowed to hold electronic money balances and transfer electronic money. In the Russian Federation, therefore, PayPal provides payment services under a banking licence as a (non-bank) credit institution.

How freely non-banks can operate varies considerably across the CPMI jurisdictions. Different approaches are summarised below. Taking into account that non-banks are very diverse and could pose different risks for the safe and efficient functioning of payment systems, an overview based on the type of non-bank (as outlined in Chapter 2) could provide the basis for reviewing the various regulatory approaches.

Non-banks that provide front-end services

In some jurisdictions, the provision of payment services to end users is limited to supervised deposit-taking institutions (banks in a broad sense). The aim, especially when the non-bank accepts funds from its customers, is to protect the payer and payee by ensuring that, when a commitment is made to transfer monetary value, this commitment is covered by highly liquid deposits held with the regulator or central bank. Thus, front-end services that include the acceptance of funds from customers are prohibited for non-banks. The implicit assumption under this approach is that banking status and the associated regulation are necessary to address risk related to payment activities, including in the field of retail payments. In Saudi Arabia, for example, non-banks are not allowed to accept and manage customers' funds, and any non-banking entity intending to provide payment services directly to users has to seek a "no objection" from the Saudi Arabia Monetary Agency (the central bank).

In other jurisdictions, non-banks providing payment services to end users do not require a banking licence but are subject to legislation specifically tailored to retail payment services. For instance, the EU has adopted such an approach in payment services, which may only be provided to end users under a specific licensing regime. While this licensing regime currently applies only to non-banks that handle customer funds, an extension to other non-bank service providers is currently under discussion. Box 7 below details the EU regulatory approach in relation to non-banks providing front-end services.

Box 7

EU regulatory framework for retail payment services

The first step in the EU regulatory approach was taken in 2000 with the Electronic Money Directive (EMD),[25] which aimed to increase competition and innovation in retail payments without compromising security. Since then, entities other than banks – namely Electronic Money Institutions – can be authorised to issue electronic money, ie a digital equivalent of cash, stored on an electronic device or remotely at a server. In 2007 the Payment Services Directive (PSD)[26] introduced Payment Institutions as a new non-bank category of payment service providers that are entitled to provide payment services under a single licence valid throughout the EU. The EMD was reviewed in 2009[27] to bring the prudential regime for Electronic Money Institutions into line with the PSD.

Hence, non-banks are permitted to offer payment services to end users based on an ad hoc legislative framework comprising the two Directives. Electronic Money Institutions, in addition to issuing e-money, can offer the full range of services envisaged by the PSD; the new payment service providers introduced by the PSD – Payment Institutions – can offer payment services, but are not allowed to issue e-money.

Hitherto, these measures have covered only institutions with activities that involve customers' funds. Activities carried out along the payment chain without involving customers' funds are not yet regulated. After the PSD came into force, advances in technology and changes in user habits have resulted in new services (outside the PSD's scope) being offered by unregulated entities. In particular, still unregulated third-party providers have provided users with account information or payment initiation services by means of online access to their payment accounts. To the extent that their activities do not involve customers' funds at any time, such providers are so far not regulated in respect of these services. To bring such services and providers under the scope of the Directive, a proposal for review of the PSD was issued in July 2013[28] which forms part of a legislative package that includes a future regulation on interchange fees for card payments.[29]

25 Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions.

26 Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC Text with EEA relevance.

27 Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC.

28 Proposal for a Directive of the European Parliament and of the Council on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC.

29 Proposal for a Regulation of the European Parliament and of the Council on interchange fees for card-based payment transactions.

The proposal for the review of the PSD requires third-party providers to be licensed and supervised as Payment Service Providers (most likely Payment Institutions), whether or not their activities involve customers' funds at any time. Specific provisions establish the conditions and requirements on which third-party providers may access information on payment accounts, and the respective liability of third-party providers and account servicing payment service providers in the case of unauthorised transactions. The new regulatory regime should foster the development of innovative efficient e-payment solutions, while maintaining security and user protection.[30]

Overall, the aim of this harmonised EU-wide legal framework is to increase competition, innovation and security in an integrated payment service market by allowing licensed non-banks to offer payment services alongside banks, under a lighter regulatory regime that takes due account of the risks inherent in their specific business models.

In addition to the PSD and EMD regulatory approach, the Eurosystem has developed oversight standards for retail payment systems that are derived from the PFMIs as well as a "Harmonised Oversight Approach and Oversight Standards for Payment Instruments".[31] The latter takes into account that the risks in the provision of payment instruments are not considered as being of systemic concern, but the safety and efficiency of payment instruments are important for both maintaining confidence in the currency and promoting an efficient economy. It describes how the Eurosystem develops oversight standards for payment instruments, outlines five oversight standards (legal risks, information on financial risks, operational risks, governance and clearing and settlement risk) that apply to all payment instruments and establishes who is required to comply with these standards. This approach makes no differentiation between bank and non-bank service providers.

Other examples of jurisdictions in which some non-banks providing front-end services to customers are required to obtain a specific licence or authorisation to operate in the area are states in the United States that require money transmitter licences, and similar regulations for money transmission in Mexico. In India, non-bank entities must meet certain paid-up capital and net worth requirements before they can be authorised as issuers of prepaid payment instruments and, even within the same payment instrument, restrictions are placed on the extent of activities that non-bank entities may perform in comparison with banks.[32]

In some other jurisdictions, non-banks are not subject to any specific regulatory framework for these services. In the case of Switzerland, the only piece of regulation that specifically relates to payment services offered by non-banks is the Anti-Money Laundering Act. Beyond complying with the AML standards, non-banks are free to provide payment services without the need to comply with any other regulatory requirement except for certain restrictions such as on the maximum amount stored in accounts offered by non-bank prepaid services providers. The framework is complemented with a light monitoring regime that allows the central bank to obtain statistical information from non-banks that exceed a threshold in the annual value of transactions processed.

[30] In this respect, the European Forum on the Security of Retail Payments (SecuRe Pay) developed a set of recommendations to improve the security of payment account access services. The ECB, on behalf of SecuRe Pay, carried out a public consultation on the requirements in 2013, and published the relevant outcome in 2014. The SecuRe Pay Forum was set up in 2011 as a voluntary cooperative initiative between supervisors and overseers, fostering knowledge and understanding of issues related to the security of electronic retail payment services and instruments. In regard to payment account access services, the recommendations aim to reduce fraud and increase customers' trust thanks to (among other things) security and control measures, increased transparency, traceability, improved information flows, protection of sensitive payment data, customer education and communication.

[31] Harmonised oversight approach and standards for payment instruments, ECB, February 2009, www.ecb.europa.eu/pub/pdf/other/harmonisedoversightpaymentinstruments2009en.pdf.

[32] In India, while both banks and non-banks are permitted to issue e-money, only banks are allowed to issue open-system prepaid instruments that permit cash-out from the prepaid card or wallet, and non-banks are not permitted to give the cash-out facility in the prepaid cards issued by them, which are typically semi-closed systems. This situation is, however, being reviewed currently and the feasibility of allowing non-banks to do cash-out is being tested in a pilot project.

The aims of regulation directed at non-banks involved in front-end services typically centre on security, consumer protection, the maintenance of the confidence in the payment system, level playing field concerns, competition, financial inclusion or anti-money laundering. In particular, security, consumer protection and public confidence are important drivers of regulation where non-banks have a direct relationship with the end users of payment services (payers and payees). This is particularly the case when the non-bank's activities directly involve customer funds (as in the case of some e-money issuers or EU Payment Institutions), in relation to measures directed to protect or isolate the funds managed by the non-bank. However, even front-end providers that cooperate with financial institutions and merely provide an interface between the final customer and a financial institution (such as some types of e-money issuers, acquirers or agent banks) are subject to some measures aimed at protecting customers, such as data security and data privacy.

Some examples of regulations that address consumer protection as well as level playing field and competition issues in relation to the provision of retail payment services are the EU's Payment Services Directive (see Box 7 above), the US Electronic Fund Transfer Act, Singapore's Payment Systems (Oversight) Act[33] or the Transparency and Financial Services Arrangement Act in Mexico. In some cases, the rules are part of voluntary agreements or best practice, as is the case with Canada's Code of Conduct for the Credit and Debit Card Industry. This code is not enforceable in law, but debit and credit card providers do observe these guidelines and their compliance is monitored by a government agency.

As non-banks that provide front-end services have a direct relationship with end users, they are in many cases subject to AML/CTF regulation. This is the case, for example in Switzerland (as explained above), the United States, Australia, EU, Russian Federation or India.[34]

In many cases, non-banks that provide front-end services are not subject to central bank oversight, as they are individual participants in the retail payment system or cooperate with other participants.

The increasing reliance on banking agents as front-end service providers raises the policy question of how these entities may be overseen and supervised. In general, the payment service provider (bank or non-bank) engaging the agent is made responsible for the agent's compliance with regulatory requirements for AML/CFT, consumer protection and other payments-related rules. However, some significant variations in such arrangements can exist between jurisdictions, which affect (i) the services that can be provided by agents; (ii) the types of entity that can become agents; (iii) registration versus licensing procedures for authorising agents; (iv) organisation of sub-agents and tiered arrangements; and (v) operating restrictions on interoperability requirements or on whether agents can charge fees.

Non-banks that provide back-end services

In general, non-bank entities providing back-end services to banks or non-banks, usually in the context of an outsourcing arrangement, may be subject to regulatory measures on data security, data privacy or operational reliability. Examples of such regulation include India's Information Technology Act 2000, which applies to both banks and non-banks, and the Monetary Authority of Singapore's Technology Risk Management Notice, which sets out mandatory technology risk management requirements for regulated entities including non-banks.

[33] The Payment Systems (Oversight) Act requires holders of widely accepted stored value facilities to appoint a bank to be fully liable for all stored value collected from users.

[34] The following regulatory measures can be mentioned as examples: in Switzerland, the Anti-Money Laundering Act (AMLA), which applies to most non-banks providing front-end services; in the United States, the Bank Secrecy Act; in Australia, the Anti-Money Laundering and Counter-Terrorism Financing Act of 2006; in the EU, the third Anti-Money Laundering Directive (currently under revision); in the Russian Federation, the Federal Law on Anti-money Laundering and Terrorism Financing. Payment system operators have also been specifically brought within the scope of the Prevention of Money Laundering Act in India.

In most CPMI jurisdictions, back-end service providers are not directly regulated, but some may be indirectly subject to regulation as the outsourcing entities are subject to regulatory requirements for the services provided by the non-bank. In this case, the outsourcing contract will determine how far the outsourcing entity can require the back-end provider's compliance with applicable regulation. In the United States, bank supervisors have statutory authority to examine non-bank service providers that enter into arrangements with their regulated financial institutions under the Bank Services Company Act. In Italy, back-end service providers are under the control of the central bank as the supervisory authority. Supervisory circulars and regulations set out the rules that banks must comply with when outsourcing.

Back-end providers are normally not overseen by the central bank, as they usually cooperate with individual payment system participants and carry out functions that are not directly infrastructure-related (ie they are not involved in the provision of clearing and settlement services for other participants).

Operators of retail payment infrastructures

Non-banks that specialise in clearing and settlement activities are mainly operators of retail payment systems or of payment card networks. In many countries, these non-banks are key components of the retail payments infrastructure and usually operate well established infrastructure that is under the purview of a supervisory authority. In some CPMI jurisdictions, this type of non-bank may be licensed and/or overseen by the central bank. Some examples are Sweden's Bankgirocentralen BGC, Singapore's BCS and NETS payment, clearing and settlement systems, the National Payments Corporation of India (NPCI), or the operators of ACHs and card schemes in some CPMI jurisdictions.

As is the case for payment infrastructure in general, these entities are usually subject to regulation that addresses the related financial or operational risks. Some examples of this type of regulation are Mexico's regulations on card payments and mobile payments clearing houses or Singapore's Payment Systems (Oversight) Act, which governs the operators of designated payment systems such as NETS and BCS.

In a few cases, retail payment infrastructures are designated as systemically important and could thus be fully subject to the CPSS-IOSCO Principles for Financial Market Infrastructures. One example is Sweden's Bankgirocentralen; in other instances, the infrastructure in question is designated as of "prominent" rather than systemic importance, as in the case of South Africa's BankServAfrica.

In a minority of CPMI jurisdictions, this type of non-bank is not subject to any specific regulatory framework.[35] Alternatively, it may be overseen by an authority other than the central bank (eg as in Canada with respect to retail payment infrastructures).

End-to-end service providers

This type of non-bank shares the characteristics of the front-end providers and operators of retail payment infrastructures described above. As such, the regulation applied to the former categories of provider may also apply to end-to-end service providers. Thus, they may be subject to regulatory measures designed to foster competition, ensure security and consumer protection or increase financial inclusion.

The distinctive feature here, however, is the provision of services from end to end: payers and payees have a direct relationship with the non-bank provider and transactions are cleared and settled in-house by the non-bank. This creates some unique characteristics for this type of non-bank:

[35] Switzerland could be an example, although a regular reporting of statistical information is in place and minimum requirements would apply if the infrastructure were to be designated as systemically important.

- Similar to operators of retail infrastructures, this type of non-bank provides clearing and settlement services, and functions in many ways as infrastructures. As a result, these non-banks could come within the scope of central bank oversight of payment and settlement systems or relevant regulation. As an example, providers of remittance services are covered by the EU's PSD. However, in certain cases, these providers may be small institutions with a limited customer base and specialising in the provision of innovative services. Therefore, central banks with oversight responsibilities geared to institutions of systemic significance might not conduct oversight of such end-to-end providers, or they might be exempted from relevant regulation (eg many small e-money issuers are exempted from licensing in the EU, although they are registered and known to the regulator). Authorities may in some cases have little awareness of this type of provider if they are small and their products are highly innovative.
- As the services they provide to end users are sometimes part of a closed loop, access to payment systems for settlement (eg ACH or LVPS) is usually less pressing for this type of non-bank than for pure front-end providers. In some cases, however, even though access to a payment infrastructure is not essential for processing transactions, a linkage with one, usually through the banks of end users, is necessary to fund and redeem the balances of the end user accounts in the system.

6. Implications for central banks and other authorities

The aim of this final chapter is to identify the main issues and challenges for central banks and other authorities with respect to non-banks and discuss how the main roles of central banks in retail payments relate to these issues. While the role of non-banks in retail payments is increasing, it is noteworthy that for funds settlement most non-banks ultimately rely on the credit/debit transfer services provided by banks. Moreover, competition from non-banks is also driving banks to offer more efficient or faster payment services, which suggests that properly managed cooperation and competition between banks and non-banks could enhance the security and efficiency of retail payments to the benefit of end users.

6.1. Issues for central banks and other authorities

Based on the foregoing analysis (especially Chapter 4 on efficiency and risk and Chapter 5 on regulation), the main issues in relation to non-bank activities in retail payments can be summarised as follows:

- **Concentration issues**: This is an issue that is especially relevant to outsourcing. If services are offered only by one or a small number of non-banks, their operational failure can have widespread implications. Whereas issues related to concentration are not specific to non-banks (a similar concentration in a single bank might have similar effects), regulatory differences could make such concentration risks less visible for authorities in the case of non-banks where these are not licensed, overseen or actively monitored. This could especially be the case for non-banks that provide specialised back-end services via outsourcing arrangements.
- **Outsourcing issues**: Outsourcing to a non-bank can improve the efficiency of the payment system, but the responsibilities (of respective entities) for the process being outsourced need to be clearly defined. In some cases, the institution outsourcing the service will remain responsible for complying with regulation or oversight requirements, but the service is effectively provided by another entity (usually a non-bank). Whether the overseer or regulator can directly access the non-bank, and whether the outsourcing institution can effectively enforce these requirements depends on the regulatory framework and on the contractual relationship

between the outsourcing entity and the non-bank. This might be problematic if responsibilities are not clear. Cross-border outsourcing may also enhance the likelihood of such problems, as clear delimitation of responsibilities across different jurisdictions and authorities may be difficult to achieve. Additionally, in the case of smaller banks outsourcing to a large non-bank (with a concentration of activities as indicated above), their powers to negotiate and enforce changes with the non-bank may be weakened. Situations could arise where problems in the non-bank could disrupt service to a large number of outsourcing institutions that have no alternative mechanisms in place to ensure business continuity.

- **Operational complexity issues**: The presence of some non-banks may add complexity to retail payments by adding more players and layers to the payment chain. This increases the number of nodes at which security breaches or other operational problems could take place. In principle, the presence of non-banks does not by itself increase operational risk or security issues, as similar problems would appear if the new layers and the increased complexity were originated by banks providing similar services. In contrast to banks, however, non-banks may not follow regulatory or oversight standards in jurisdictions where, because they are non-banks, they are not required to do so or there is ambiguity in whether or not they are required to do so.

- **Consumer protection issues**: In addition to the security breaches mentioned above, non-banks may impact consumer protection in additional ways. For example, the ownership and use of consumer data by non-banks could raise concerns about privacy and data protection. Additionally, end-to-end service providers may hold positive account balances for end users. Such a non-bank, if it is not subject to appropriate capital and liquidity requirements, may not maintain sufficient liquidity to honour the withdrawal of those funds in a timely manner, and there may be a risk that end users may not be able to access their funds. Again, it should be emphasised that these issues are similar for banks and non-banks, but differences in risk management or in applicable regulation may influence the probability of occurrence or its impact.

- **Level playing field issues**: Regulation, official policy and market self-regulation or best practices can have a direct impact on the type and terms of services that non-banks can offer. Regulation is likely to have evolved from the historical fact that banks are the typical providers of payment services, and this might disadvantage non-banks vis-à-vis banks (or vice versa) in offering a given service. Banks could be advantaged if, for instance, a banking licence is required for certain services to be offered. Or non-banks could be favoured if, for instance, they are subject to less stringent requirements than banks (or none at all).

  Level playing field issues arise not only between banks and non-banks in a given jurisdiction, but also between non-banks offering cross-border services from different jurisdictions. As noted above, regulatory frameworks for non-banks differ widely between jurisdictions, and such discrepancies are likely to become more significant in future as new technologies facilitate the provision of cross-border services.

- **Stakeholder involvement**: Non-banks, especially front-end and end-to-end providers, are often relatively new providers of retail payment services, and the most innovative may be very small firms, especially in their start-up phase. Additionally, newcomers may follow very different business models, resulting in a high degree of fragmentation. On the other hand, banks usually have a predominant role in the industry bodies that influence the way in which retail payment services are provided and represent the providers to the authorities. As a result, industry agreements, the development of standards and other arrangements may not adequately include input from non-banks, possibly limiting the usefulness or effectiveness of standards and other arrangements. Defining appropriate channels for a dialogue with the new actors, taking into account their degree of fragmentation, is likely to present a challenge to both the authorities and the industry.

All the issues outlined above are interconnected. For example, concentration might greatly increase the impact of an operational failure or a security breach if it affects the non-bank in which the services are concentrated. Also, level playing field and stakeholder involvement issues reflect a similar type of problem.

Not all these issues will be relevant in all jurisdictions. The topics of relevance will depend on the types of non-bank that are present, on the regulatory and institutional framework and on the authorities' mandates and actions in relation to non-banks. Even if the risk and efficiency issues posed by non-banks in retail payments are no different from those affecting banks, differences in way that banks and non-banks are regulated may increase the likelihood that risk or efficiency issues will materialise and impact the payment system as a whole.

Finally, there are circumstances that may affect the importance of the issues above or the way they can be addressed by central banks or other authorities. These factors include:

- **Diversity of authorities at the national level**: The retail payments system may involve a number of different authorities at the national level. For example, there may be bank supervisors, consumer protection agencies and central banks responsible for oversight of systems. New non-bank entrants may not immediately fit neatly into the jurisdiction of any particular authority, or there may be ambiguity as to which authority is responsible for the non-bank.
- **Cross-border factors**: The above issues are magnified in the international context. Some non-banks provide similar services in different countries, and this tendency may intensify as new technologies enable innovative cross-border services. The diversity of regulatory approaches may result in the different treatment of the same non-banks in different jurisdictions (see Box 6 on PayPal). At the same time, the diversity of authorities, and any lack of international coordination could leave gaps or inconsistencies in oversight and supervision. Additionally, few detailed arrangements for cooperation exist between authorities at the international level in relation to non-banks providing retail payment services. As a result, the potential for regulatory arbitrage may be created.

These factors point to the importance of cooperation among central banks and between central banks and other authorities, both nationally and internationally. The aim should be to ensure a consistent approach, where appropriate, to the treatment of non-banks with similar risk profiles, preventing level playing field issues and opportunities for regulatory arbitrage.

6.2. The role of central banks

The degree of involvement and the mandates of central banks in relation to retail payment services differ widely, as highlighted in previous Committee reports.[36] The role of non-banks in retail payments is equally diverse. Differences in central bank responses to issues raised by non-banks may depend on the central bank's mandate, on applicable regulation, on the systemic significance of the non-banks and on the degree of cooperation with other authorities, both nationally and internationally.

As a result, the issues highlighted in the previous section are not necessarily under the direct control of central banks in all cases. These issues have been outlined irrespective of the relevant authority addressing the specific problem, and some of the issues, such as those related to consumer

[36] CPSS, *Policy issues for central banks in retail payments*, March 2003.

protection, were not within the mandate of many of the CPMI central banks represented in the working group.

However, the safety and efficiency of retail payment services is an area of general interest for central banks, and several traditional roles of central banks in relation to retail payment systems might also be relevant to the case of non-banks providing retail payment services.

- **Catalyst for change**: As catalysts for change, central banks cooperate with public bodies and private sector firms, and use their influence and analytical capabilities (eg undertaking research or monitoring trends) to facilitate the industry's movement towards desired outcomes. This function is more indirect than oversight, and can thus be exercised to some extent even when the central bank lacks formal oversight powers. Most often, however, this function is not an alternative to oversight, but complements it as a way of reinforcing the policy stance.

  Due to the diversity of their activities and sectors of origin, non-banks may not be well represented by industry associations or share sufficient common interests for collaborative industry actions. This may be in contrast to banks, which have typically found sufficient common interest to participate in payments industry forums. Where potential benefits could accrue from such collaboration, either to reduce risks or increase efficiency, scope may exist for central banks to engage with non-banks to encourage their participation in industry or stakeholder bodies and create conducive market conditions for non-banks to effectively contribute to the development of retail payments market. The central bank may fulfil its catalyst role by promoting constant interaction between the authorities, financial institutions and banking and payment associations. The resultant discussions can help to establish whether issues related to security or stakeholder involvement could arise from the participation of non-banks in retail payments, and to suggest possible solutions. Central banks could also act as catalysts when supporting financial inclusion initiatives or providing guidance to new participants in the payments system, such as innovative non-banks.

- **Oversight role**: Payment system oversight focuses on the safety and efficiency of payment and settlement systems, as opposed to the efficiency and safety of individual participants in those systems. In some jurisdictions, oversight can extend over the entire national payment system (encompassing infrastructure, participating institutions and instruments). Traditionally, oversight has focused on systemically important payment and settlement systems. However, in many jurisdictions retail payment systems fall within the oversight of the central bank even if they lack systemic importance, and in some jurisdictions the scope of oversight is even broader, including particular types of payment instruments and efficiency-related aspects of the retail payment market. How far the activities of certain types of non-bank might fall within the scope of this oversight depends on the central bank's mandate.

- **Operator**: Central banks are typically operators of RTGS systems and they may also operate retail payment systems. Vis-à-vis non-banks, central banks face similar challenges as other operators, such as possible issues related to level playing field between banks and non-banks, including requests for access to settlement accounts and payment services by non-banks, issues related to interoperability with other systems or requests to improve the system (such as to integrate new services provided by non-banks or to allow banks to compete more effectively with them). When responding to these issues, central banks need to adequately balance level playing field and efficiency considerations against risk implications and potential operational issues.

Some central banks may have additional functions that relate closely to non-bank activities. These responsibilities could include regulatory or supervisory powers or roles related to financial stability, consumer protection or financial education.

In summary, the degree to which non-banks are involved in retail payments varies widely within the CPMI jurisdictions, especially in relation to (i) the relative importance of non-banks in different segments; (ii) their implications for risk and efficiency; (iii) the potential role they might play (eg in relation to financial inclusion); (iv) the regulatory framework they are subject to; and (v) the relevant mandates of central banks and other authorities.

As a result, the working group has not identified any single preferred approach central banks may take in relation to non-banks in retail payments. Instead, the approach should ideally be adapted to the different variables highlighted above and is therefore likely to differ across jurisdictions. However, given the interest of central banks in retail payments and the growing importance of non-banks in the provision of retail payment services, it seems appropriate to seek a better understanding of the changing role of non-banks and its implications. Accordingly, central banks and other authorities may wish to take note and consider the implications of the issues that are analysed in this report, including risk and level-playing-field issues, and take action as appropriate in their jurisdictions.

Annex A: Retail payments process, examples of activities per stage

Non-banks as defined in this report may offer their services at all stages of the retail payments process. To highlight the range of their payment activities and their involvement across the entire payment process, the working group adapted the approach used by the ECB and the Federal Reserve Bank of Kansas City[37] and assessed the presence of non-banks in the various stages of the payment process. For the purpose of this report, the payment process is broken down into the following five stages:[38]

- **Stage 1: Pre-transaction** – this stage consists of all activities involved in creating the initial infrastructure required for payments; it includes processes and activities related to customer acquisition (enrolment of front-end consumers and merchants, related credit evaluation tools), provision of actual payment instrument (card issuance including personalisation, delivery and activation, e-money wallet, cheque manufacturing), provision of related hardware, software and network infrastructure (ATM and POS terminals, cheque and card readers, application processing and web-hosting services, shopping cart software, cheque verification software, connection to payment gateway and related services), provision of security-related technology support (digital signature services, online transaction security systems), other value added services such as provision of data centre services, e-invoicing etc.
- **Stage 2: Authorisation** – this stage includes the processes and activities that enable a payment transaction to be authorised and approved before it can be completed. It includes provision of various back-end services (connection between networks and payment instrument issuers, software and related services to issuers to enable pay-or-no-pay decision and fraud screening, checking funds availability and actual debit of payer's account etc), fraud and risk management services to customers and issuers of payment instruments (PIN verification and other identity authentication services, transaction monitoring, sending of alerts to customers), ex ante compliance services (database and application services for identifying and reporting of suspicious transactions).
- **Stage 3: Clearing** – This stage consists mainly of activities which enable the submission of claims by members in the payment system against each other and, calculation and dissemination of information relating to payment/receipt obligations of respective members. It includes provision of services to merchants to sort their sales information and submit claims to respective networks; calculation of net positions of members by networks, ACH operators, transmission of clearing orders, distribution of advices etc.
- **Stage 4: Settlement** – This stage consists of activities directly related to the posting of credits and debits in the account of the bank/financial institution with the settlement bank (central bank or any other bank) as well as in the accounts of the final payer (customer) and beneficiary (merchant or individual). It also includes activities related to (reversal) accounting for return of transactions/payments.
- **Stage 5: Post-transaction** – This stage includes mainly the processes and activities related to provision of various types of value added services for statement generation (preparation, dispatch and notification of statements to consumers and merchants), reconciliation (matching

[37] Federal Reserve Bank of Kansas City, *Nonbanks in the payments system: European and U.S. perspectives*, no PSR WP 07-01, Payments System Research Working Paper, 2007.

[38] This categorisation differs slightly from the categorisation used by the ECB and Kansas Fed in that we make an additional separation between the clearing and the settlement stage, which according to our fact-finding exercise can be characterised very differently in terms of the level and intensity of non-bank involvement. In addition, the separation between clearing and settlement activities is consistent with the stages analysed in CPSS, *Clearing and settlement arrangements for retail payments in selected countries*, September 2000.

invoices and payments), dispute resolution (chargeback and dispute processing services), reporting and data analysis, and ex post compliance services (reporting to authorities for AML and terrorist financing, back-feeding to ex ante databases).

A more detailed list of these sub-activities, including examples, is shown in the table below.

Retail payments process, examples of activities per stage

Table 1

1. Pre-transaction	Examples
1. Customer acquisition	Registration and enrolment of consumers and merchants or deployments of ATMs and other access points (eg self-service kiosks) used for non-cash payment services
2. Services for issuer's front-end customer (payer) acquisition	Provision of credit evaluation/credit risk assessment tools, application processing services
3. Provision of payment instruments/devices to the front-end customer (payee or payer)	Activities performed by Trusted Service Managers, card issuance, card personalisation, delivery and activation; hardware and software provision (such as card readers) for usage with a consumer's online device (PC, mobile, hand-held); provision of e-money wallet/access code to e-money values
4. Provision of hardware to accept payment instruments/devices	Provision of ATM terminals and other access points (eg self-service kiosks) used for non-cash payment services, POS terminals, cheque readers/cheque POS terminals
5. Provision of software to accept payment instruments/devices	Web-hosting services, provision of shopping cart software, cheque verification software or software to connect payment gateway service providers
6. Provision of internet security-related technology/support	Certificate-authority services (such as PKI-based secure environments), provision of digital identity services for consumer authentication, provision of online transaction security systems to front-end customers (payees, merchants), and back-end customers (such as 3D-secured card transactions via internet), provision of e-signatures and other e-authorisations for payment authorisation purposes
7. Payment card industry (PCI) compliance services to merchants and/or payers	
8. Provision of data centre services to back-end customers	Outsourcing complete data centre functions/secured, supervised floor space/multi-site backup storage for disaster recovery
9. e-invoicing	Creation and delivery of electronic invoices to front-end customers (payer)
10. Communication connection for merchants	Provision of gateway to acquirer/payment processors, provision of gateway to various networks/check or ACH authorisation vendors
2. Authorisation	
11. Transaction authorisation (fund verification)	Provision of network switch services; a back-end service, provision of communication connection between networks and payment instrument issuers, provision of decision management/fraud screening/neural network scoring system to card issuers for authorisation, process to verify and confirm if payer has sufficient funds (or credit lines) available to cover the transaction amount
12. Fraud and risk management services to front-end customers (payees)	Verification services (address, IP address, card verification number, other data), payment instrument authentication and authorisation services, identity authentication, decision management/fraud screening/neural network scoring system (hosted at third-party service providers)

13. Fraud and risk management services to card issuers	Monitoring transactions and notifying cardholders of potential fraud, enabling them to take immediate action
14. Initiate the debiting of the front-end customer's (payer's) account	Debiting the front-end customer's (payer's) account/e-money purse
15. Ex ante compliance services	Anti money laundering and terrorist financing regulation such as controls to identify suspicious transactions (database, software etc)
3. Clearing	
16. Preparation	Sorting merchant's sales information by payment instrument/network for clearing, submission of sales information to each payment instrument network, calculation of each network member's net position and transmission of net position information to each member, provision of transformation services into other payment instrument formats (such as MICR to ACH), provision of sorting transactions by destination groups to financial institutions
17. Clearing	Transmission of clearing orders to a financial institution, transmission of clearing orders to ACH operator, distribution of advices showing the amounts and settlement dates, clearing (different from an ACH)
4. Settlement	
18. Settlement	Posting credit and debit at each financial institution's central bank account, posting credit and debit at each financial institution's commercial bank account, posting debit (credit in case of a return) to front-end payer account, posting credit (debit in case of a return) to merchant (payee) account, check settlement
5. Post-transaction	
19. Statement	Provide statement preparation/delivery services for payers (such as mobile credit advice; online bank/card account statements)
20. Reconciliation, incl collection and receivable	Matching invoices and payments
21. Retrieval	Provision of chargeback and dispute processing services
22. Reporting and data analysis services	Reporting and data analysis services to merchants (such as support services for treasury and accounting), to consumers and to financial institutions
23. Ex post compliance services	Compliance with anti-money laundering and terrorist financing regulation, such as reporting to authorities, back-feeding to ex ante databases

Annex B: Members of the working group on non-banks in retail payments

Chairman	Gopalaraman Padmanabhan Reserve Bank of India
Members	
Reserve Bank of Australia	David Emery
National Bank of Belgium	Pierre Gourdin
Bank of Canada	Ben Fung
European Central Bank	Tom Kokkola (until June 2013)
	Francisco Tur Hartmann (since June 2013)
Bank of France	Geoffroy Goffinet
Deutsche Bundesbank	Marcus Härtel
Hong Kong Monetary Authority	Clarence Hui
Reserve Bank of India	Charulatha Kar
Bank of Italy	Nives Coppari
Bank of Japan	Yuushi Endo (until August 2013)
	Takaaki Kurebayashi (since August 2013)
Bank of Mexico	Alberto Mendoza Hernández
Netherlands Bank	Anneke Kosse
Central Bank of the Russian Federation	Olga Lapkina (until January 2014)
Saudi Arabian Monetary Agency	Abdulaziz Aldahmash
Monetary Authority of Singapore	Chek-Tchung Foo
South African Reserve Bank	Shaun Rayfield
Sveriges Riksbank	Björn Segendorf
Swiss National Bank	David Maurer
Central Bank of the Republic of Turkey	Erdem Oz (until March 2013)
	Canan Özcan (from March 2013 until July 2013)
	Betül Üzer (since July 2013)
Board of Governors of the Federal Reserve System	David Mills
World Bank	Harish Natarajan
Secretariat	
CPMI Secretariat	Carlos Conesa

Significant contributions were also made by Emanuela Cerrato (European Central Bank), Emanuel Freire (CPMI Secretariat) and Marc Hollanders (BIS).