Nonbanks in the Payments System: European and U.S. Perspectives

By:

Members of European Central Bank Oversight Division[1]
Members of Federal Reserve Bank of Kansas City Payments System Research Department[2]

Prepared for Conference Sponsored by the Federal Reserve Bank of Kansas City
"Nonbanks in the Payments System: Innovation, Competition, and Risk"
Santa Fe, New Mexico USA
May 2-4, 2007

---

[1] Dieter Reichwein and Simonetta Rosati. The authors acknowledge Ann Borestam, Giacomo Caviglia, Niall Merriman, and Remco Bruins for useful comments; Monica Hartmann, Elin Amundsen, Johannes Priesemann, and the central bank Experts for their contributions to the EU survey concept and methodology; and Chantal Brion for excellent research assistance. The views expressed in this paper are those of the authors and do not necessarily reflect the views of the ECB or the Eurosystem.

[2] Terri Bradford, Nathan Halmrast, Fumiko Hayashi, Richard Sullivan, Zhu Wang, and Stuart E. Weiner. The views expressed in this paper are those of the authors and do not necessarily reflect the views of the Federal Reserve Bank of Kansas City or the Federal Reserve System.

Contents

Figures and Tables

1. Introduction

A smoothly-functioning payments system is critical to the health of a financial and economic system. That payments system, in turn, is comprised of many critical components, both bank and nonbank. In recent years, nonbanks have become increasingly prominent in payments systems around the world, reflecting in part the growing dominance of electronic forms of payment.

In addition to its impact on the payments industry itself, the increased prevalence of nonbanks raises potential implications for central bank oversight. Central banks are almost uniformly charged with ensuring that payments systems are safe and efficient. With nonbanks growing in importance, a reevaluation of oversight activities appears warranted.

This paper presents the initial results of a joint study undertaken by staff at the European Central Bank (ECB) and the Federal Reserve Bank of Kansas City to document and analyze nonbanks in the payments system. The focus is on electronic (non-paper) retail payment services in the European Union (EU) and the United States. The paper adopts a common set of definitions and a uniform analytical framework.

The study has three general objectives: (i) to document the various activities performed by nonbanks in the provision of retail payments services; (ii) to evaluate the role of nonbanks relative to the role of banks; and (iii) to present a preliminary assessment of the implications of the growing role of nonbanks. More specifically, the following key questions are addressed:

1. What payment activities do nonbanks perform in specific payment types?
2. What is nonbanks' importance, relative to banks, in performing different payment activities?
3. What are some examples of specific nonbank companies that are active in payments?
4. What benefits and risks are potentially associated with rising nonbank participation?
5. Does the current regulatory environment adequately address potential risks?
6. What are some of the differences and similarities between EU and U.S. nonbank prevalence, and between EU and U.S. regulatory approaches?

The paper is organized as follows. The next section introduces fundamental conceptual considerations. The definition of "nonbank," the difference between front-end and back-end payment services, and the distinction between payment types and payment activities are first discussed. The section then presents the seven primary payment types and the twenty-three primary payment activities that are used in the analysis to follow. The third section presents the principal results, documenting and analyzing the role played by nonbanks in the EU and U.S. retail payment systems. The information presented in this section draws on several sources, including a recently-completed survey of EU central banks. The fourth section of the paper describes the regulatory environment surrounding nonbank provision of payment services in the European Union and the United States. The fifth section explores central bank oversight issues, including

discussions of risk and efficiency. Finally, the paper closes with a brief summary and suggestions for future research.

2. Conceptual considerations

Nonbanks can perform functions at all stages of the payments process. For all forms of payment (credit cards, debit cards, electronic cheques, credit and debit transfers, e-money, and stored-value transactions) and for all points on the payments chain (hardware and software provision, consumer and merchant interaction, backroom processing, clearing and settlement, and post-transaction accounting) nonbanks can play a major role. This section provides a framework for documenting and analyzing these roles.

2.1. Definitions

A nonbank payment service provider is defined in this study as any enterprise that is not a bank and which provides, primarily by way of electronic means, payment services to its customers. In the European context, nonbanks include all entities that are not authorized as a credit institution; hence, electronic money institutions (ELMIs) are considered to be nonbanks. In the U.S. context, nonbanks include all entities that do not accept demand deposits. A nonbank payment service provider may be either bank-controlled or nonbank-controlled.[3]

A nonbank payment system provider's customers may be either: (i) end-users of retail payment services, in which case the nonbank is providing front-end services; (ii) banks or other nonbank payment service providers, in which case the nonbank is providing back-end services; or (iii) both types of customers. Examples of front-end services include money-transfer services provided to households and acquiring services provided to merchants. Examples of back-end services include back-office data processing, authentication and authorization, and hosting of payments-enabled web sites. An example of a firm with both types of customers is a company that is leasing point-of-sale (POS) devices to merchants and at the same time performing processing and routing services on the data captured on those devices for the banks issuing the associated payment cards. Such a firm would be considered to be providing front-end services to the merchants and back-end services to the issuing banks.

2.2. Payment types and payment activities

There are two ways to think about the payments process. One is to think about payment types—the means and instruments through which a transaction is undertaken. Examples are credit card transactions, debit card transactions, credit and debit transfers, and person-to-person Internet payments. The second way is to think about payment activities—the various steps and services that are provided as a given transaction takes

[3] Examples of bank-controlled nonbank payment service providers include subsidiaries of banks, for example, TSYS, a large U.S. processor owned by Synovus Bank, and bank associations, for example, Visa Europe, the large European credit and debit card network. Nonbank-controlled service providers are firms without a governing bank affiliation, for example, First Data Corporation, PayPal, Hypercom, Vodafone, etc.

place. These two concepts—payment types and payment activities—are clearly very closely related.

Table 1 (see p. 53) shows the broad payment types that are used in this study. Categories include electronic cheques; credit transfers; direct debits; payment (credit and debit) cards; money remittance and transfer transactions; e-money and other prefunded or stored-value instruments, including Internet person-to-person (P2P) payments; and other payment instruments. The first category, electronic cheques, are those payment types that begin with a paper cheque, or information from a paper cheque, but are converted to an electronic payment at some point in the process; end-to-end, traditional paper cheques are excluded. The second and third categories, credit transfers and direct debits, utilize agreements that credit or, with preauthorization, debit accounts. The fourth category, payment (credit/debit) cards, relies on networks to access either a line of credit or a demand deposit account to enable a payment. The fifth category, money remittance/transfer, involves currency transfers transmitted by nonfinancial third-party operators. The sixth category, e-money and other pre-funded/stored-value instruments, uses an electronic store of monetary value, which may not necessarily involve a bank account, to make a payment. Finally, the remaining category, other payment instruments, includes payment types that are not easily classified elsewhere.

Table 2 (see p. 54) shows the wide range of variants that occur within the broad payment types. The broad payment types are listed again in column 1, with European and U.S. "versions" listed in columns 2 and 4, respectively. Credit transfers and direct debits can often be viewed as distinct categories in Europe, for example, while in the United States, they are usefully subsumed under the general automated clearing house (ACH) payment category. Similarly, e-money schemes function differently in the European Union as compared to the United States. In Europe, e-money schemes are either prepaid schemes subject to specific issuer regulation, where the prepaid value is embedded in a physical device like a card (e-purse), or memorized in accounts held on a server and accepted by parties other than the issuer. In the latter instance, when the user transfers funds to cover e-money payments, he/she is in fact purchasing e-money issued by the service provider, and the deposit balances are transferred to the provider's bank, which holds them in the provider's bank account. Consequently, what is transferred for payment by the user is not the bank balances, but the e-money that was purchased from the provider; the settlement asset among the users is thus e-money, not bank money. In the United States, while prepaid products like stored-value cards and e-wallets function similarly to the European Union, proprietary balances do not. Rather, users of proprietary-balance transfers determine how to fund each balance transfer on a transaction-by-transaction basis. The service provider does not become the owner of the funds, nor does it hold the funds in custody. Mobile phone payments, although in their infancy in both the European Union and United States, are another payment device that may function as e-money depending on the service provider's payment model.

Columns 3 and 5 of Table 2 list the various physical environments in which a transaction can take place. These include POS, mail, telephone, and Internet. For example, a customer wanting to purchase a book, say by using a credit card, can visit a local book store (POS), order through the mail, order by phone, or order over the Internet. Each represents a different physical environment and, consequently, potentially involves

a different set of payment service providers. The range of options shown in Table 2 thus constitutes the full group of payment types that are available to end-users.

Payment innovations challenge the traditional way of looking at payment types. In most cases, innovative payment services build on existing, traditional payment types. In some cases, though, they present elements of novelty that may lead to considering them as an innovative and independent payment service. Box 1 provides an example of different m-payment models currently available in Europe, and a possible classification among the existing payment types included in Table 2. Although volumes are still extremely limited, there are expectations in Europe about their growth potential, also in light of the forthcoming regulatory opening to nonbank payment institutions (see Section 4.2.2) which may contribute to a significant development of m-payment services.

Box 1: M-payments in Europe

In Europe there are a number of initiatives undertaken by telecommunication companies to facilitate payments initiated by their customers using mobile phones. These are sometimes referred to, in general, as m-payments, but the underlying payment schemes may vary significantly. M-payments are a relatively new payment service, and their use is still reported to be negligible compared to other payment instruments (volumes for 2001 were estimated to be about 70.8 million transactions in 2002 in Europe.[4] This compares with an overall noncash payment market of more than 50 billion transactions in the EU). However, they have attracted significant attention in the industry and among European policy makers as their growth potential is considered huge, given the high penetration rate of mobile phones in Europe (much higher than the Internet penetration rate in some countries).[5] The following main models are in place:

1. Mobile phones just provide access to Internet banking, allowing the user to initiate a payment from the Internet payment application of its own bank (or, mobile phones are used to transmit transfer orders to the user's e-money issuer). In this case the telephone company is just acting as a communication service provider. In Table 2, they fall under row 2 (credit transfer, initiated by telephone & Internet);
2. The scheme is used to pay for digital goods or services which are directly related to the use of the mobile phone (and not separable from it). For example, mobile phones are used to download digital content or telephone related digital products (ring tones, games, other information services), and the phone prepaid airtime is debited of the price of these digital goods and services (prepaid version), or the amount due is included in the telephone bill, and settled using the direct debit relation between the telephone company and the user and their banks (post-paid version). Even if the digital goods/services are provided by third parties (thus the telephone company will pass part of the revenues to them), since the digital goods can only be distributed and used through the phone, these kind of m-payments are not usually considered as a payment service independent from the payment of the telephone bill, and therefore they are not included in the table, although the prepaid version usually relies on

[4] "Mobile Data 2004", Credit Suisse First Boston, European Wireless Telecommunications Services (15 September 2003), quoted by Vodafone in its comments to the Communication from the Commission to the Council and the European Parliament concerning a New Legal Framework for Payments in the Internal Market COM (2003) 718, 13 February 2004

[5] In 2005, almost half of all EU households had Internet access. At the end of 2004, the rate of subscriptions per 100 inhabitants to mobile phones stood close to 100 (and in some countries like the Czech Republic, Luxembourg and Sweden even surpassed this (as one person may have more than one subscription, privately or for professional use (Eurostat, 2007).

telephone cards, and therefore it may fall under row 6, sub-case "limited purpose prepaid cards");

3. Prepaid mobile phone airtime, stored in a telephone card, in the telephone chip, or on a server (and activated via a telephone message) is used to pay third parties for goods and services which are unrelated to the telephone service (e.g. a drink at an automated machine, cinema tickets, parking, and so on). This scheme has features in common with e-money schemes and in some countries telephone companies have been requested by the authorities to apply for a proper license (in some cases they benefited from a waiver due to the small amounts involved, limitation in acceptance circuits, or other qualifying features). In Table 2, this case would be covered by row 6, e-purse or e-money;

4. Schemes similar to number 3 above (payments made in favor of third-parties, for goods/services unrelated to the use of the telephone), but using a post-paid billing scheme (similar to the second version in number 2 above). Given the post-paid billing procedure the payment service is clearly outside the definition of e-money, but it can be considered a payment service (or a payment service provided by the telephone company independently from the telecommunication services provided to the same user). In Table 2, these schemes would be covered by row 7 (other bank-based (post-billed) payment services initiated by telephone).

One important distinction between prepaid and post-paid models is that in the former case the user is exposed to credit risk versus the telephone company (or e-money issuer, but if e-money is involved risks would be minimized by the application of the relevant regulation), while in the latter the telephone company is exposed to credit risk versus its customer until the bill is successfully settled (for this reason, post-billed services are usually available only for payments of very limited amounts, like the micro-payments for digital goods and services described under number 2 above, or to pay for goods/services of very small value as in the case described under 4).

As noted earlier, a second way of thinking about the payments process is to examine payment activities, that is, the various steps and services that are undertaken as a transaction moves from beginning to end. Figure 1 (see p. 51) shows the broad payment activities that are used in this study. The payments process can be thought of as a chain of events in which four principal categories of services are performed: pre-transaction activities encompassing customer acquisition and the provision of front-end infrastructure; during-transaction Stage 1 activities encompassing connection, communication, authorization, and fraud detection activities; during-transaction Stage 2 activities encompassing clearing and settlement activities; and post-transaction activities encompassing statement provision and reconciliation activities. All in all, one can identify twenty-three primary payment activities that underlie, to varying degrees, all payment transactions. Within these twenty-three primary activities, there are, in turn, a host of subactivities, numbering over fifty. The full list of primary activities and subactivities is shown in Table 3 (see p. 55).

By way of example, continuing with the case of a credit card purchase, the pre-transaction section of Table 3 lists the activities that must occur before a credit card transaction can begin. From a customer perspective, a card issuer first must enroll the customer, evaluate their credit worthiness, and provide them with a payment instrument. From a merchant perspective, a service provider must "qualify" the merchant to be able

to accept card payments, provide them with the necessary hardware and software to read the card, as well as provide services that ensure the security of any data required to conduct the transaction. The during-transaction Stage 1 activities associated with the credit card purchase include providing the merchant with a gateway to the various networks that process card transactions, providing the merchant with the means to authenticate the card user, and authorizing the customer's transaction for processing. During-transaction activities Stage 2 might entail sorting the merchant's sales information by network for clearing, calculating each network member's net position and transmitting net posting information to each member, transmitting clearing orders to the appropriate parties, and settling the transactions by posting credit and debit information to the appropriate accounts. Finally, post-transaction activities for the credit card purchase might include providing both the customer and merchant with activity statements, reconciling invoices and payments for the merchant, as well as providing the merchant with dispute and chargeback resolution services.

2.3. Nonbank role

The preceding subsection highlighted the distinction between payment types and payment activities. But clearly the two are related. Indeed, as evident in the credit card example above, any given payment type is the combination and interaction of any number of payment activities. And, importantly, nonbanks can, and do, play a role in a majority of these activities.

Figure 2 (see p. 52) illustrates this point by showing the payment activities associated with a credit-card transaction over the MasterCard or Visa network that is initiated by a mobile telephone. The figure has four panels corresponding to the four principal categories of payments activities: pre-transaction, during-transaction Stage 1, during-transaction Stage 2, and post-transaction. Each of the panels, in turn, shows the various steps involved in that part of the payments chain. The coloured blocks in a given panel show activities in which nonbanks may be participating (the colours correspond to those in Figure 1; the numbers show the sequencing of steps in the during-transaction stages). The grey blocks in a given panel show activities that are not performed in that part of the payments process but that may be performed by nonbanks in one of the other three parts (panels). White blocks show customer, bank, merchant, and central bank activities. An important observation is the large number of coloured and grey blocks in Figure 2, underscoring the importance of nonbanks in the payments process. The next section of the paper takes up this issue in greater detail.

3. Nonbank payment activities for various payment types

The previous section stressed that a payment transaction can be initiated in several ways, and that the related payment information and instructions can be captured and transmitted using several methods. Nonbanks can be involved at many points along the processing chain, as well as in the direct provision of payment services to end customers.

Nonbanks have long had a presence in core payments processing, as banks and other financial institutions have sought to outsource such activities as data processing, file

transmission, and related tasks. Other during-transaction activities in which nonbanks have been heavily involved include network services, such as gateway provision and switching services, authorization services, and fraud and risk management services. All of these activities are important elements of the retail payments process and are of key importance in maintaining public confidence in the safety of payment instruments.

Additionally, nonbanks have been active in the range of activities that take place before and after the execution of a given payment transaction. As noted above, examples of such pre-transaction activities include the development and provision of hardware for electronic payments (for example, card production and POS devices) and the establishment of contractual relations with cardholders and merchants. In the case of emerging payments, in many cases these pre-transaction services involve new ways of providing access to traditional payment types, for example, credit transfers initiated via the Internet or via mobile phones, or web portals that consolidate billing and facilitate payment initiation. Moreover, nonbanks have also been important in many post-transaction services, including statement provision, reconciliation, and retrieval.

This section of the paper documents and discusses in greater detail the role played by nonbanks in the EU and U.S. retail payment systems. The basic tool of analysis is a table—for each country—showing, for each of the various payment subactivities and each of the various payment types, the importance of nonbanks relative to banks. Thus, each table is a matrix, in which the rows are payment activities, the columns are payment types, and the entry in an individual cell is the authors' assessment of whether nonbank presence is prevalent (blue), high (green), medium (yellow), low (orange), or nonexistent (pink) for that particular payment activity-payment type combination. Cells in grey are not applicable, while cells in white indicate insufficient information to judge. The assessments are based on survey results, industry data, and other sources. Also indicated in each cell is the survey participants' or authors' view of the quality of the data (high, medium, or low) on which the "importance" assessment is based.

3.1. European Union

The role of nonbanks in payments in Europe was analyzed by carrying out a survey among Payment Experts of the National Central Banks (NCBs). The results presented include 13 countries, eight from the euro area (Austria, Germany, Finland, France, Greece, Italy, Portugal and Slovenia) and five from EU Member States that have not yet adopted the euro (Bulgaria, Cyprus, Czech Republic, Latvia and Lithuania). These countries together process about 58 percent of the number of payment transactions in the European Union. However, as the NCBs of the largest non-euro area Member States did not participate in the survey, the focus of the analysis is mainly on the euro area (the above mentioned eight euro area countries in the survey together process about 79 percent of the total euro area payment transactions, and 57 percent of the total EU payment transactions).[6] All in all, these eight countries represent 59 percent of the EU GDP (77 percent of the euro area), and 56 percent of the EU population (76 percent of the euro area).

[6] The survey was based on 2003 data and includes the countries that joined the EU in 2004 (i.e., the survey excludes Bulgaria and Romania who joined in 2007).

The survey was carried out using a common methodology.[7] The results are reported in Tables 4, 5, and 6. Rows are the various payment activities and subactivities, and columns are the principal payment types used in Europe (electronically processed cheques, credit transfers, direct debits, payment cards, e-money and other payment instruments).

Before moving into each table, a first observation is that information on the role of nonbanks is not equally available across countries and across payment instruments, as shown by the large white areas in most of the countries, particularly for cheques, money transfers, and other payment instruments. Information on entities involved in retail payments processing may be more easily available for those payment instruments that are more popular in the country: national preferences in the use of payment instruments are very marked in Europe, reflecting cultural preferences,[8] traditions, historical development of the industry, or different stages of maturity in the payment services industry. For instance, cheques are rarely used in Austria and Finland, and their use is very limited, compared to other payment solutions, in Germany, while they are still common in France (where more than 55 percent of all EU cheques transactions take place), Italy, Cyprus, and Portugal (although their use is, in general, declining)[9]. Italy and Finland can be considered "credit transfers countries," while direct debits have been introduced relatively recently in several countries and are becoming increasingly popular. In contrast, card payments are common and popular in most countries. Thus, respondents were able to assess the importance of nonbanks for almost all the relevant payment activities with a relatively high confidence for payment cards.

A second observation is nonbank presence varies significantly by country. Based on the limited information available, countries are divided in three groups. The first group, shown in Table 4 (see p. 56), consists of Austria, Germany, and Italy. In these countries, nonbanks play a larger role compared to other countries in the activities of most payment types. Finland, France, Latvia and Slovenia are in the second group (Table 5, see p. 59), where nonbanks seem to play a more limited role. The last group (Table 6, see p. 63) includes the remaining countries: Bulgaria, Cyprus, Czech Republic, Greece, Lithuania and Portugal. Nonbank presence in these countries can be considered somewhere in between.

---

[7] Some respondents stressed that they faced data limitations that did not allow considering the results as a comprehensive and exhaustive description of the role of nonbanks in their respective countries. Thus, the survey shows some of the activities that nonbanks perform, but it does not imply that these are the only activities that nonbanks perform in payment processing or that all payment solutions offered to customers in the surveyed countries are covered. Nevertheless, the survey provides a useful overview of the role of nonbanks in payments, shedding some light on an aspect of the European payment industry that was not thoroughly investigated previously.

[8] The impact of preferences in terms of cultural similarities, geographical proximities, and language was shown by Rosati and Secola (2006) for large-value cross-border payments in euro. It is likely that in the retail markets cultural preferences may also play a role.

[9] This explains why France is the country where cheques processing is highly automated also in the initial stages of the processing chain (pre-transaction and during-transaction Stage 1, e.g. provision of cheques readers/POS, provision of cheques verification software and of cheques verification services) and more information is available on nonbanks' roles in cheques processing, while in other countries the cheques column contains a good deal of white and grey cells.

A third observation is that in the majority of the 13 countries, the role of nonbanks for payment cards is high or prevalent in many of the activities considered. This is probably due to the high automation of the pre-transaction and during-transaction Stage 1 activities (e.g., switch routing, authentication, and real-time authorization of the transaction) and, also, to the international dimension of cards-processing standards. It should be noted that in Europe there are a number of national card schemes that are usually co-branded with the international schemes like Visa and MasterCard to allow customers to use the card abroad. In addition to co-branding, there are in Europe also a few examples of (bilateral) interoperability agreements between national (mainly debit cards) schemes, particularly to allow use in the EU cross-border context. As a result, cards processing is largely organized around a common model, except for the settlement phase, which may be carried out differently in the various countries.[10]

The growth of the use of cards and the development of national card schemes has gone hand-in-hand with the growth of the market for card transaction processing, which was often characterized by "national champions" concentrating most of the transactions and allowing the exploitation of scale economies at the individual country level.[11] This market now seems to be undergoing a very dynamic phase in Europe, driven by the recent development of SEPA instruments and SEPA infrastructure. In particular, a consolidation process has just started, through a wave of alliances and joint ventures, with the objective to achieve a sufficient scale to allow repositioning of national players as European players serving the common euro payment area.[12] For instance, in September 2006 the Dutch company Interpay and the German company Transaktioninstitut agreed to merge to form Equens, a company aiming at serving the European market. Similarly, the cards payments processor SiNSYS is jointly owned by SBB (an Italian firm), Banksys (a Belgian processor), and Interpay (a Dutch ACH). An example of a global firm operating in Europe is First Data, which is present in Austria, Germany, France, Greece, Latvia and Lithuania.

Finally, irrespective of the role played in pre-transaction and other during-transaction activities, the settlement phase remains a prerogative of the banking sector in Europe, and this is true for all payment instruments, not only for cards. In the case of traditional payment instruments, this may be explained by the fact that banks are normally those entities that have access to the retail payment systems (and, in many cases, national banking associations actually have set up or own the national clearing and settlement companies) or those to whom the legislation in place reserves settlement accounts provision and management. For e-money and other innovative payment solutions, settlement also remains largely dominated by banks, which is consistent with two observations on the development of new payment methods in Europe. First, that innovation seems to have focused on means (using mobile, Internet technology) to access traditional banking funds transfers services (i.e. the so-called "access products"), rather

[10] In some countries, national card transactions are settled in the ACH or other national retail payment system. In others, they may be settled by banks bilaterally. Furthermore, as it relates to international cards transactions, the correspondent banking channel normally is used for settling interbank positions.
[11] For example, SBB in Italy or Banksys in Belgium.
[12] Cordone (2004) and Moeller (2006) provide different examples of such cooperative ventures.

than payment instruments alternative to those offered by banks.[13] Second, e-money as an alternative to instruments transferring bank deposits has remained somewhat underdeveloped compared to initial expectations and most e-money schemes in Europe are actually bank ventures with some notable exceptions (e.g., PayPal).[14]

Table 7 (see p. 69) provides (a non-exhaustive) example of some nonbank companies that play a role in the various payment activities in Europe.

3.2. United States

To assess the role of nonbanks in payments in the United States, staff at the Federal Reserve Bank of Kansas City completed the same survey as that distributed to EU survey respondents. Information utilized included industry directories and news articles, interviews with nonbanks and industry observers, and other sources more anecdotal in nature.

Table 8 (see p. 72) presents the results for the United States. Rows are the various payments activities and subactivities previously explained. Columns are the principal payment types found in the United States. These include: e-cheques;[15] credit transfers; three types of direct debits (automatic, one-time, and those completed under, for example, the Tempo and PayByTouch schemes); three types of payment card transactions (four-party credit and signature debit (e.g., MasterCard and Visa), PIN-debit, and three-party credit (e.g., American Express, Discover, and private-label); money remittance; four types of e-money and other pre-funded or stored-value instruments (open-loop prepaid card, closed-loop prepaid card, PayCash, and PayPal transactions); and other instruments (the Bill Me Later scheme).

The most striking general observation is the high degree of blue and low degree of orange and pink in the table, indicating that where nonbanks can play a role in the payments process, that role is almost always an integral one. Looking across the payment type columns, almost all payment types show a significant nonbank presence in almost all facets of the payments process, with two exceptions. The first are those activities, shown in grey, that are not applicable, either because (i) they are inherently bank functions involving demand deposits, for example, some pre-transaction activities for credit transfers and automatic and one-time direct debits, or (ii) they are activities that are not

---

[13] See ECB (2005b), where reporting the results of a survey on payment innovation (with a scope wider than e-money products only), it is concluded that "two-thirds of the (surveyed) companies are related to the banking sector, either by license or by ownership and, as a consequence, most of the e-products include a link to settlement." This is also consistent with what was reported by Masi (2004), who notes that "the greatest part of the new payment initiatives does not modify the clearing and settlement phases of the payment cycle which are managed and regulated by banks".

[14] In 2003, e-money accounted for only 0.5 percent of payment transactions in Europe. EC (2006) reports evidence that "the e-money market has developed more slowly than expected, and is far from reaching its full potential", and that as of late 2005 there were "only four ELMIs", although the number was expected to increase as at least five-to-eight applications were either in process or expected shortly " (however, about 72 companies were operating at national level in seven Member States under a waiver)" noting also that, two-thirds of the e-money in circulation was issued by banks, and only one-third by ELMIs" (p.6).

[15] A physically written cheque is either truncated and becomes an ACH payment at some point of cheque processing (ARC and lockbox) or is used as a device to capture information to create an ACH payment at the point of transaction (POP, TEL, and WEB).

applicable to that payment type, be it bank or nonbank, for example, post-transaction activities for money remittance transactions. The second exception to significant nonbank presence are settlement activities that involve posting credits and debits to financial institutions' commercial and central bank accounts—here banks dominate.[16] Virtually everywhere else, nonbank presence relative to banks is high, and, indeed, prevalent.

A more specific observation is that four-party payment cards and open-loop prepaid cards have the largest number of blue and green cells. This is because these payment types require more during-transaction Stage 1 activities—namely network switching and transaction routing through card-issuer processors—than other payment types. A complementary observation is that credit transfers have the smallest number of blue and green cells. This does not imply nonbanks' importance in the credit transfer payment activities is relatively low; rather it implies this type of payment does not require as many activities as the other types of payment do.

The message from Table 8 is clear—nonbanks are a force in the U.S. retail payments system, dominating a large number of payments activities for a large number of payment types.

Table 9 (see p. 73) provides examples of some nonbank firms that play a role in the various payment activities in the United States.

3.3. EU – U.S. comparison

As noted above, nonbanks are very important throughout the retail payments industry in the United States. In Europe, nonbanks are very important for card payments and, in certain countries (e.g., Germany and Italy), other payment types as well. For other payment types, however, the role of nonbanks in Europe appears more limited.

While in the United States the role of nonbanks in payments activities is fully established and visible, in Europe this role is still growing. However, it is expected to increase further in years to come. Contributing factors will be, first, the increasing use of cashless payments; second, the ongoing (albeit gradual) substitution of mature/declining products, such as cheques, with other instruments that allow for easier electronic processing (as direct debits and cards payments); and third, industry restructuring due to the SEPA project, with a redesign of payment instruments, infrastructures and processes, and the start of a consolidation process among national payment processing providers.

As nonbank presence and influence continue to grow on both continents, it becomes increasingly important to have a solid understanding of risks involved in the various stages of the payments processing chain and of the regulatory structures in place in various countries. The next section examines the regulatory environment.

4. Regulatory environment

4.1. Objectives

[16] This also is a principal finding of Bradford, Davies, and Weiner (2003).

The payments industry usually operates in a largely regulated environment. Payments are an integral part of the functioning of the whole economy. Thus, maintaining a safe and efficient environment for the transfer of funds between economic actors and preserving public confidence in the systems and instruments used for such funds transfers are key public interests.

The regulatory approaches usually combine hard law provisions (issuance of legislation and binding regulations by competent authorities) and soft law (standards setting and market self-regulation). Some authorities like central banks, which traditionally have specific competences in this field, sometimes resort to moral suasion and co-operative interaction with market players instead of or together with using their power to issue binding regulation. While the relevant regulatory environment may vary significantly in the different jurisdictions in terms of detailed provisions and authorities involved, the main objectives pursued by regulation in the field of retail payments are generally the same and may be summarized as follows:

(1) Maintaining public confidence in payment instruments and systems used to transfer funds. This objective is, inter alia, addressed:

- By maintaining a sound and transparent regulatory environment for the provision of payment services that sets adequate (institutional, financial, operational etc.) requirements on the payment service providers and ensures legal certainty in the interaction of all parties involved. An example of such legal provisions could be those that protect the settlement finality in clearing and settlement systems from the application of some bankruptcy measures to payments entered into a system.

- By entrusting a public authority with the responsibility to carry out oversight of payment systems. Usually this task is assigned to the central bank. In some cases, oversight competences of central banks cover also explicitly the review of payment schemes and instruments. The general objective of the oversight function is to ensure safety and efficiency of payment systems. Safety means that the funds will be transferred from the sender to the receiver with finality when expected and that the system or payment arrangement is sufficiently robust to neither create nor transmit financial shocks. Efficiency means that the speed of the transfer and the allocation of its end-to-end costs are acceptable to the sender and the receiver of the transaction and, where applicable, to their customers. Thus, payment systems oversight contributes to maintaining financial stability. In the field of retail payments, where systemic risk is not particularly relevant (although there are some exceptions whereby retail settlement systems are considered systemically important and subject to the same requirements of large-value payment systems) efficiency is often the focus of oversight. Central banks may be allowed also to engage in an operational role by providing themselves payment infrastructures or services, where necessary to ensure the achievement of the safety or efficiency objectives.[17] (Oversight issues are discussed in Section 5.)

[17] The operational role of central banks in the field of large-value payment systems is related to the need to reduce systemic risk by providing settlement in central bank money and preserve the vehicle for the execution of monetary policy. In the case of retail payment systems, it may be justified by the need to serve

(2) Ensuring an adequate level of customer protection, which in the case of retail payments, assumes two dimensions:

- First, individual customers should be protected against undue financial losses. Depending on the payment instrument, such losses may arise in the event of failing payment service providers, criminal acts etc. Also, in order to ensure an orderly functioning of payment schemes, in many countries there are laws or regulation concerning the proper execution of payment orders. Where they exist, such regulation would typically deal with issues such as transparency of terms and conditions, fees, maximum execution time, rights and obligations of customers and payment services providers, and dispute resolution bodies.
- Second, maintaining confidence in payment instruments. A crisis of confidence may degenerate involving more widely the financial system and, ultimately, the trust in the currency. For instance, in the case of certain payment instruments which can be economically assimilated to deposits (e.g. e-money), holders may not be able to properly assess the creditworthiness of issuers due to asymmetric availability of information, with the consequent financial stability risks of overreaction to crisis of confidence. For this reason, in some cases even if not involved in other banking activities, issuers of e-money may be subject to various requirements aimed at preserving their financial soundness and financial equilibrium (imposition of sound investment policy and limitation of liquidity risk) as well as to a prudential supervision regime (this is the case in Europe).

(3) Avoiding the misuse of the financial services for criminal purposes: the illegal part of the economy tries to transfer funds for criminal purposes, and it is a public objective on the one hand to protect the financial system and on the other hand to fight illegal activities. Typical regulations in this field, which are relevant from a retail payments perspective, are anti money-laundering and terrorist financing regulations, and anti-fraud regulation.

(4) Like other industries, the payment industry may be subject to competition law. Like other network industries, payments processing efficiency benefits from consolidation and concentration which ensure an adequate critical mass. However, the possibility for new players to enter the industry, and a level playing field among actors needs to be ensured to maintain an adequate level of innovation and efficiency.

(5) Other objectives

- Sometimes the nature of certain payment instruments deserves special regulatory requirements. For instance, payment instruments that represent a monetary value which is convertible on demand at par with cash (and are therefore a close substitute for money), due to their intrinsic link to money and its properties, may need to be subject to a set of regulations aiming at preserving the effectiveness of

---

the banking community by providing efficient settlement services, for example in the absence of adequate market solutions.

the monetary policy framework (e.g. statistical reporting for the purpose of inclusion in monetary aggregates, or imposition of reserve requirements).[18]

- Other regulatory provisions may be introduced to achieve public objectives that depend on the specific regional context. For example, in the European Union, two reasons to review the regulatory framework for the provision of payment services were first, to achieve an internal market for payments across the 27 Member States and second, to harmonize the regulatory treatment of payment service providers.

4.2. Europe

This section describes, first, the payment systems oversight responsibilities of the ECB and Eurosystem; second, the regulatory environment surrounding payments, including provisions that apply to banks and to nonbanks; third, the industry self-regulatory initiatives aiming at achieving a Single Euro Payments Area (SEPA), a project that is contributing to a reshaping of the payments industry in Europe; and fourth, the proposed Payment Service Directive, a legislative innovation that will facilitate the SEPA project implementation and that is expected to open up the market for payment services in Europe to nonbanks, with the introduction of the new category of nonbank "payment institutions."

4.2.1. Oversight responsibilities in the field of payment and settlement systems

According with the Treaty on European Union, the ECB and the European System of Central Banks (ESCB) were established in 1998. The ESCB comprises the ECB and the national central banks (NCBs) of all EU Member States (Article 107.1 of the Treaty) whether they have adopted the euro or not. The Eurosystem comprises the ECB and the NCBs of those countries that have adopted the euro. The Eurosystem and the ESCB will co-exist as long as there are EU Member States outside the euro area.

One of the basic tasks[19] of the Eurosystem is to promote the smooth functioning of payment systems (Article 105 (2) of the Treaty (reiterated in Article 3.1 of the Statute of the ESCB, which is an annex thereof)). In this field the ECB enjoys significant regulatory powers: Article 22 of the Statute of the ESCB states that the ECB and NCBs may provide facilities and the ECB may make regulations[20] to ensure efficient and sound clearing and payment systems within the Community and with other countries. Such ECB regulations are directly applicable in the Member States which have adopted the euro. So far, the

[18] See ECB (1998) for a detailed discussion of the various policy issues related to e-money. The report recognizes (p. 1) that "the issuance of electronic money is likely to have significant implications for monetary policy in the future. Above all, it must be ensured that price stability and the unit of account function of money are not endangered. A significant development of electronic money also could have implications for the monetary policy strategy and the control of the operational target."

[19] The other three basic tasks are: the definition and implementation of monetary policy for the euro area; the conduct of foreign exchange operations; and the holding and management of the official foreign reserves of the euro area countries (portfolio management).

[20] The Treaty assigns to the ECB the regulatory powers to adopt any legal acts which are necessary to implement the basic tasks assigned to the Eurosystem. Among the legal acts addressed to third parties (other than the NCBs of the Eurosystem) there are ECB Regulations, Decisions, Recommendations and Opinions.

ECB has not yet issued a regulation on the basis of Article 22. Finally, in accordance with Article 105 (4) of the Treaty and Article 4 of the ESCB Statute, the ECB is consulted on any proposed Community act in its fields of competence. The ECB may submit opinions to the appropriate Community institutions on matters in its fields of competence.

The Eurosystem fulfils its tasks in the field of payment systems by: (1) providing payment and securities settlement facilities like TARGET, and some national central banks manage retail payment systems or other payment mechanisms; (2) overseeing the euro payment and settlement systems by setting standards to ensure the soundness and efficiency of systems handling euro transactions; it also assesses the continuous compliance of euro payment and settlement systems with these standards; and (3) acting as a catalyst for change, by promoting efficiency in payment systems and the adaptation of the infrastructure to the needs of the single euro payments area (SEPA, see section 4.2.3).[21]

4.2.2. Payments regulatory provisions applicable to banks and nonbanks

In general the regulatory coverage of payments is the result of the combination of various legal and regulatory provisions, which take different approaches: some are institutional-based and are applicable only to certain categories of players (for example, issuers of e-money need to be licensed and are subject to a prudential regime modeled on that of credit institutions). Others are applied to systems used to clear payments, and only indirectly involve participants in these systems. Other provisions are specific to certain instruments (e.g. the legislation implementing the international convention on cheques). A detailed analysis of all the main EU legal provisions in the field of payments is outside the scope of this paper.[22] This section describes the main relevant directives and regulations in the field of payment and settlement and the undergoing initiatives to review or amend them, by looking at the treatment of banks and nonbanks. The proposed Payment Services Directive deserves a more detailed discussion given its far reaching impact on the provision of payment services (including by nonbanks), and therefore is discussed in more detail in Section 4.2.4.

4.2.2.1 Systemically important payment systems

Two main legal provisions are relevant for the containment of systemic risk in retail payment systems: the Directive 1998/26/EC on settlement finality in payment and securities systems (which is aimed at reducing the systemic risk associated with participation in payment and securities settlement systems, and in particular the risk linked to the insolvency of a participant in such a system) and the Directive 2002/47/EC on financial collateral arrangement (which provides for rapid and non-formalistic

[21] In the field of securities settlement, similar tasks are carried out by providing a mechanism for the cross-border use of collateral (CCBM); setting standards for securities clearing and settlement systems (e.g. the User standards for use of securities settlement systems in monetary policy operations and for collateralization of central bank credit operations); ensuring an integrated regulatory and oversight framework for securities settlement systems (e.g. in the framework of the cooperation between the European System of Central Banks and the Committee of European Securities Regulators (ESCB-CESR)); and promoting an efficient securities market by encouraging the removal of barriers towards integration.

[22] For an overview of the European regulatory environment and institutional framework for payments see also ECB (2007), Eurosystem Chapter.

enforcement procedures in order to safeguard financial stability and limit contagion effects in case of a default of a party to a financial collateral arrangement). Among the systems designated by Member States under the Settlement Finality Directive and which therefore benefit from its protection, are several retail payment systems and Automated Clearing Houses (for example, the ACHs CEC in Belgium, SIT in France, and BI-COMP in Italy and the Retail Electronic Clearing Co. Ltd in Ireland). Furthermore, as mentioned in the previous paragraph, the Eurosystem has oversight competence on all payment systems, including retail ones. In June 2003 the Governing Council of the ECB adopted an oversight framework for retail payment systems operating in euro (ECB, 2003b) which takes the form of ACH-type systems and multilateral arrangements (15 such systems were identified as falling into the oversight framework, and six systems were classified as systemically important: SIT in France, IRECC and IPCC in Ireland, LIPSNet in Luxembourg, CSS in the Netherlands and PMJ in Finland).

As for other Eurosystem oversight policies, the enforcement can be ensured by ECB regulations in accordance with Article 22 of the Statute (which have not been issued so far), or guidelines (the latter are addressed to the NCBs). Where applicable, enforcement can be effected by legal instruments available to an NCB. More traditional, informal tools (e.g. moral suasion) can also be used. In line with the principle of decentralization, the enforcement of the policy stance is, as a rule, entrusted to the NCB of the country where the system is legally incorporated.[23]

Finally, other infrastructures used by payment systems which have been recognized as critical by payment systems overseers have been made subject to oversight on the basis of their systemic relevance (as in the case of the SWIFT interbank communication network, which is subject to co-operative oversight by the central banks of the Group of 10 Countries). In several Eurosystem countries the National Central Bank oversees the national infrastructure provider serving the national payment system, often drawing on an explicit legal basis, setting information and reporting requirements, and carrying out a formal assessment, while in other cases oversight is based on moral suasion.

4.2.2.2 Customer protection

Two main legal texts are relevant from this perspective. First, the Directive 1997/5/EC on Cross-border credit transfers, which established minimum information and performance requirements for cross-border credit transfers, and, second, the Regulation 2560/2001 of the European Commission on equality of fees for domestic and cross-border transfers in euro, which lays down rules on cross-border payments in euro in order to ensure that charges for those payments are the same as those for payments in euro within a Member State. The Regulation applies to cross-border payments in euro up to EUR 50,000 within the Community (the regulation covers payment card transactions and

[23] In view of the increasing cross-border participation in payment systems within the euro area, the Eurosystem favors a cooperative approach towards the enforcement of the oversight policy stance, with the local NCB acting as lead overseer, and being responsible for liaising with other relevant NCBs whenever required. For systems which have no clear domestic anchorage, the body entrusted with oversight responsibility is the NCB where the system is legally incorporated unless the Governing Council decides otherwise on the basis of the features of the system and entrusts oversight responsibilities to the ECB. This was the case for the large value payments systems (LVPS) Euro System of the EBA Clearing Company (Euro 1) and, as far as the euro is concerned, the Continuous Linked Settlement Bank (CLS Bank).

withdrawals from cash machines since 1 July 2002 and credit transfers since 1 July 2003). Customer protection and execution rules for payment services are included under the scope of the proposed Directive on Payment Services, which, once adopted, will repeal Directive 1997/5/EC (while Regulation 2560/2001 will remain in force).

Furthermore, in order to maintain the confidence of the users, based on its statutory responsibilities in the field of payment systems, the Eurosystem may also formulate policies concerning the security of payment instruments. The Eurosystem developed a policy line for e-money schemes with the Report on electronic money, published in August 1998, and established E-Money Systems Security Objectives (ECB, 2003a), which are used by several NCBs to perform their statutory tasks in relation to oversight of e-money schemes.

Oversight of payment instruments is done in some cases on a national basis (e.g. France, Greece, and Italy). In some cases, national legislation also gives to the NCB some supervisory tasks vis-à-vis the institutions providing payment services (for instance, the competence of the Bank of Greece includes also licensing, regulation, and supervision of money remittance undertakings).

4.2.2.3 Provision of payment services by banks and nonbanks

In the EU, payment services can be provided by credit institutions, by e-money licensed institutions and by other nonbank providers. This paragraph reviews the regulatory coverage of these three categories.

- **Payment services provided by credit institutions**

The regulatory coverage of payments services largely depends on the bank versus nonbank status of the payment service provider, and its affiliation to a banking group.

Banking regulation applies to all activities carried out by credit institutions, including those related to the provision of payment services. The relevant pieces of legislation in the EU are first, the banking directives (directive 2006/48/EC and directive 2006/49/EC),[24] which have introduced amendments to previous legislation on the same subject (including some provisions needed to implement the Basle II Accord), and second, the Directive 2000/46/EC on the taking up, pursuit of and prudential supervision of the business of electronic money institutions. The banking directives lay down the rules concerning the taking up and pursuit of the business of credit institutions, their prudential supervision and their capital adequacy. It should be noted that in Europe a credit institution is defined, for the purpose of these directives as:

- an undertaking whose business is to receive deposits or other repayable funds from the public and to grant credits for its own account; or

[24] Directive 2006/48/EC of the European Parliament and of the Council of 14 June 2006 relating to the taking up and pursuit of the business of credit institutions (recast) and Directive 2006/49/EC of the European Parliament and of the Council of 14 June 2006 on the capital adequacy of investment firms and credit institutions (recast). The 2006 directives recast the directives on the same subject 2000/12/EC and Council Directive 93/6/EEC. As new amendments were to be made to the 2000 and 1993 Directives, and they had already undergone significant changes over the years, it was deemed desirable to recast them to provide clarity.

- an electronic money institution (ELMI) within the meaning of Directive 2000/46/EC (but ELMIs are subject to the capital requirements and prudential supervision regime described in the e-Money Directive).

Banking regulation encompasses the bank as a whole, covering also the risks faced by banks arising from all their business lines, and the settlement business line is explicitly considered in the framework of operational risk management and subject to coverage in the form of capital requirements.[25]

Finally, as other nonbank undertakings which belong to a group including a credit institution, nonbank providers of payment services which belong to a banking group fall within the scope of supervision of the credit institution on a consolidated basis, following specific criteria of consolidation. Prudential supervision authorities may obtain from all undertakings within a group the information necessary to achieve their objective to assess the financial situation of the credit institution within the group.

- **E-money and E-money Licensed Institutions (ELMIs)**

According to Directive 2000/46/EC e-money shall mean monetary value as represented by a claim on the issuer which is: (i) stored on an electronic device, such as a chip card or computer memory; (ii) issued on receipt of funds of an amount not less in value than the monetary value issued; (iii) accepted as means of payment by undertakings other than the issuer. The directive restricts the range of business activities that the ELMI may carry out, and excludes the granting of any form of credit. Relatively soon after the adoption of the directive, some doubts were raised on whether prepaid mobile phone cards were likely to be a form of electronic money when they are used to buy and pay third-party products or services and therefore whether and how some provisions of the directives should be applied to mobile operators. Currently, the directive is under review, (EC, 2006). It is foreseen that the work to modify the directive will take place after the adoption of the proposed Payment Services Directive.

- **Other nonbank providers of payment services**

Payment services may currently be provided under very different conditions within the European Union, as shown in EC (2003),[26] which summarizes the licensing rules and possible supervisory regime in place at end of 2002 in 13 EU countries and Norway with reference to the a wide range of payment services, including:

- payment services based on money received in advance on an account, be it traditional/current deposit account, for specific and limited purpose payment instruments (e.g. loyalty schemes run by merchants) and payment services based on virtual accounts (e.g. PayPal, etc.),
- issuing of (general purpose) credit cards, specific or limited purpose credit cards,

[25] The revised (BASEL II) solvency requirements for credit institutions, envisages an 18 percent capital charge for payment and settlement services provided by credit institutions under the "standardized approach."

[26] Comparative tables of the national regimes in place in the various Member States are available at http://ec.europa.eu/internal_market/payments/framework/comparison_en.htm.

- payment services based on ex-post billing like phone accounts used for non-phone payments (payment instruments for premium rate services or a SMS where the rate is higher than the standard rate, and part of the revenues is passed to a third party, and those where the payment services are not directly related to the main invoicing purpose),
- requirements for Money Transmitters and Money Transfer institutions, and
- e-money, multi-merchant loyalty schemes based on money received on electronic device such as smart cards, servers or networks and similar electronic device-based services where a higher rate is applied to Premium Rate Services or SMS than the standard price, and part of the revenue is passed to a third party. (As noted above, mobile operators or issuers of hybrid instruments may be brought by the relevant authorities of the Member States under the regime of the e-money, depending on the specific features of the scheme and service provided (see EC, 2004), on a case by case basis and thus following criteria that may be more or less strict depending on the interpretation given in the various Member States).

Overall, the regulatory provisions for the different types of payment services vary significantly across the Member States, ranging, from no license requirement in one country to the restriction of the activity only to banks or other licensed financial institution in another country. For example, for money transmitters, in Denmark no license is required, in Spain there is a special license regime for this type of activity, while in France the law requires a credit institution license with fully-fledged prudential regime. The harmonization of the regulatory regime for all entities other than banks and ELMIs that provide payment services is one of the main objectives of the proposed Payment Services Directive, with the introduction of the new figure of the "payment institution".

4.2.2.4 Outsourcing by payments service providers to third parties

For the provision of payment services to their customers, front-end providers may often resort to outsourcing of certain activities (typically IT functions or data processing) to third entities. In case of banks and ELMIs, outsourcing is covered by the relevant regulatory regime. According to banking supervisory practices, outsourcing remains the responsibility of the outsourcer and in some cases it is subject prior to approval by or information to supervisors.[27] In case of ELMIs, it is specified that the "sound and prudent management, administrative and accounting procedures and adequate internal control mechanisms" they are required to put in place should respond to the financial and non-financial risks to which the institutions are exposed including technical and procedural risks as well as risks connected to its cooperation with any undertaking performing operational or other ancillary functions related to its business activities (Art. 7 of Directive 2000/46/EC).

[27] BIS (2003).

Regulatory safeguards regarding outsourcing by other nonbank providers of payment services is not harmonized at EU level, but it will be once the proposed Payment Services Directive will come into force (see 4.2.4 below).

In some cases, national provisions on oversight by the National Central Bank may also regard nonbank back-end providers. A notable example is that of the French National Central Bank, whose legal mandate in the field of payment instruments extends "to all non-cash means of payments and applies to all payment service providers that issue or administer these means of payments, as well as their potential outsourced entities." The Banque de France can also carry out on-site inspections to verify if the security objectives it sets are met. The Banque de France "can obtain from the issuer or any other party involved the relevant information concerning the means of payment and the terminals or other technical devises associated therewith."[28] However, national approaches differ significantly across the Member States, and in some countries payment systems overseers are not entitled to approach or request information from these service providers (and for this reason, some NCBs did not participate in the survey mentioned in this paper).

4.2.2.5 Preventing and combating the use of the financial system for criminal purposes and anti-fraud

Preventing and combating criminal use of the financial system is a subject that has received strong attention by EU policy makers and legislators. From the perspective of anti money laundering and terrorist financing, the Third Anti-Money Laundering Directive (Directive 2005/60/EC) widened the definition of criminal activity giving rise to money laundering to include all serious crimes, including offences related to terrorism.

To complement the Directive, the Regulation (EC) No 1781/2006 of the European Parliament and of the Council on information on the payer accompanying transfers of funds was adopted in December 2006 to transpose Special Recommendation VII (SRVII) of the Financial Action Task Force (FATF) into EU law, further facilitating traceability of money transfers.[29]

4.2.2.6 Competition

[28] ECB (2007).

[29] The Regulation requires that the name, address, and account number of the sender of the transfer must always be transmitted together with the funds. It introduces obligations not only for the "payment service provider" ("a natural or legal person whose business includes the provision of payment services to payment service users"), but also for the "intermediary payment service provider" i.e. "a payment service provider which is neither that of the payer nor that of the payee and which participates in the execution of transfers of funds". It does not apply to transfers of funds which flow from a commercial transaction carried out using a credit or debit card or any other similar payment instrument, provided that a unique identifier, allowing the transaction to be traced back to the payer, accompanies all transfers of funds flowing from that commercial transaction. It does also not apply to certain prepaid or post-paid funds transfers carried out by means of a mobile telephone or any other digital or IT device, provided certain specific conditions are met.

Competition regulation[30] regards all economic sectors, thus it applies also to retail payments, irrespective of the bank or nonbank status of the service providers. In Europe, the competition authorities are the European Commission and the national competition authorities. The Treaty prohibits first (art 81), agreements between two or more firms which restrict competition (e.g. a cartel between competitors for price-fixing or market sharing) and second (Art 82), abuse of dominant position (for example predatory pricing policies to eliminate competitors from the market).

As regards antitrust enforcement, the Commission has done substantial case work in the field of payment cards systems, in particular addressing interchange fees. One example is case COMP 29.373 Visa International, which, in 2002, was concluded with the Commission granting exemption under Art.83 (3) of the Treaty to Visa International on multilateral interchange fees (MIF) for cross-border card payments after the card organization agreed to make significant changes to the system (EC, 2002). Other individual cases have regarded the MasterCard Network (COMP 34579) and the 'MERFA' in the French card network 'Groupement de Cartes Bancaires'(COMP 38626).

In the field of financial services, the Commission has carried out a Sector Enquiry into retail banking (see EC, 2007), looking, among others, at the area of payment systems and card payment systems in particular[31] and finding evidence of competitive concerns that require follow-up action by the Commission and national competition authorities (for instance, a great variation in cards fees which may suggest market fragmentation). The Commission recognized that current regulatory and self-regulatory initiatives underway (the proposed Payment Services Directive, and the development of SEPA payment instruments such as the SEPA card schemes) will contribute to remedy the situation (for instance, respectively, in terms of access rights to payment systems, and by opening up the currently highly concentrated market for card merchant acquiring). Nevertheless, it concluded that there is a need to monitor the SEPA framework, in order to ensure that its implementation will remain pro-competitive.

4.2.3. Payments industry self-regulation: SEPA

Following the launch of the euro in 1999 and the changeover of cash in the Euro area countries in 2002, an important area that lagged behind in terms of European integration was that of cashless transfers. European consumers and merchants were faced with a situation of efficient and relatively cheap domestic payments but inefficient and costly cross-border payments. This was due to a number of reasons, including legal and technical restrictions to the safe use of domestic payment instruments in a cross-border context (like in the example of the direct debit, an instrument which has proved very efficient domestically, but whose legal design cannot be easily used across-borders due to existing diverging legal and/or practice regimes) and the lack (at that time) of a pan-European infrastructure or of technical standards. Such a situation was not compatible with the internal market, which is in fact the domestic market of the EU.

---

[30] The EC policies to protect competition also include other aspects that are not relevant for the scope of this paper (e.g. prohibition of State aid, liberalization). For a complete overview of the EU competition policies and the EC responsibilities and actions, see http://ec.europa.eu/competition, on which this paragraph draws.

[31] The other areas are credit registers, cooperation between banks, and setting of prices and policies.

The need to overcome these limitations resulted in the launch of a far reaching project by the Eurosystem and the European Commission to support the banking community in creating a SEPA, i.e. an area where citizens, companies and other economic actors will be able to make and receive payments in euro, within Europe, whether between or within national boundaries under the same basic conditions, rights and obligations, regardless of their location.[32]

SEPA is a project carried out primarily by the European banking industry, involving a variety of stakeholders and players (see ECB 2006b for an introduction to SEPA and a description of the role of all entities involved) not only in the euro area, but also in other countries of the European Union and in Iceland, Liechtenstein, Norway and Switzerland. Thus the reach of the project is wider than the euro or EU countries.

For the purpose of SEPA, the European banking industry has set up a specific body, the European Payment Council (EPC), which is defining the new rules and procedures for euro payments. Its purpose is to support and promote the creation of a Single Euro Payments Area (SEPA) through industry self-regulation.[33] The EPC has already developed standards for three SEPA payment instruments (credit transfers, direct debits, and cards) which will be introduced in 2008, and until 2010 they will operate alongside existing national processes, with full migration achieved from the end of 2010 onwards. After the full implementation of SEPA purely national solutions for core credit transfers and direct debits, and purely national card schemes will no longer exist.

Progress has been made not only by banks but also by nonblank infrastructure providers, such as the card processors, the European Automated Clearing House Association (EACHA) and the Euro Banking Association (EBA), which are actively participating in this work. EACHA is developing a set of procedures to secure interoperability between infrastructures (ACHs), while the EBA has developed STEP2, the first pan-European ACH, or PEACH, for clearing cross-border as well as domestic retail payments in euro.

4.2.4. Proposed Payment Directive of the EU Council and Parliament

Given the legal restrictions that prevent the cross-border use of some payment instruments and make it difficult for the cross-border provision of several payment services, the EC has developed a strategy designed to remove barriers in the internal market and to simplify its rules, in particular by proposing the Payment Services Directive (PSD), in December 2005.

The proposed Directive has three main objectives: first, to bring down legal barriers by establishing a comprehensive and harmonized legal framework for payment services; second, to open up the payments markets to competition by allowing actors other than banks and e-money institutions to provide payment services (the so called “payment

[32] Given its direct interest and responsibilities in the safe and smooth operation of payment systems in the euro area, the Eurosystem is involved in the project from its very beginning in close cooperation with the European Commission, and it acts as a catalyst for change supporting the industry by making clear its expectations vis-à-vis the project. It also closely monitors progress and developments in relation to SEPA publishing results in regular Progress Reports.

[33] A complete and detailed overview of the SEPA project and activities of the EPC is available on the EPC web site, http://www.europeanpaymentscouncil.eu/index.cfm.

institutions"[34]); and third, to provide a set of standardized consumer protection rules (rights and obligation of the parties, and information requirements for both payment providers and users).

Besides fostering harmonized rules in the place of the current different national regimes and operating a significant legal simplification the main element of novelty is represented by the introduction of the payment institutions. These would be entitled to carry out the following activities:

- provision of payment services;[35]
- provision of operational and related services (such as guaranteeing the execution of payment transactions, foreign exchange services, etc.);
- operation of payment systems.

Furthermore, authorization as a payment institution (which would be subject to certain information requirements[36]) would be valid in all Member States and recorded in a Community register which will be regularly updated and accessible online. The proposed Directive also requires Member States to designate the competent authorities responsible for monitoring payment institutions. These must be public authorities, or bodies recognized by national law or by public authorities expressly empowered for that purpose. Complaints procedures and the penalties laid down by the Member States are to be administered by the above authorities.

In April 2006, the ECB issued an Opinion on the proposed directive (ECB, 2006a), where it welcomed the initiative and gave a generally positive assessment. However, the ECB underlined that on the one hand some concepts introduced by the directive would need further clarification (e.g. the scope of the activities of the payment institutions), and, on the other hand, there was the need to ensure that where the provision of payment services gave rise to risks similar to those faced when the same services are provided by banks or e-money institutions, i.e. using balances of "payment accounts" of similar economic characteristics to deposits or e-money, or funds anticipated in the form of credit provided by the payment institution, then also the level of safeguards in place should be the same. To protect the customers' balances from the event of failure of the payment institution holding such balances, and thus preserve public confidence, the ECB suggested that payment institutions should not be allowed to use customers' funds during the limited time period that the funds are being transferred form payer to the payee. Finally, in the ECB opinion the proposed directive should make it clear that the provision

[34] More specifically, the proposed Directive envisages four categories of payment service provider:(1) credit institutions; (2) post office giro institutions (within the meaning of the Banking Directive), which provide payment services; (3) electronic money institutions; and the new category of (4) payment institutions (natural or legal persons who have been granted authorisation in accordance with the provisions of the proposed Directive, when it comes into force), which are entities providing payment services listed in Annex to the Directive.

[35]The list is wide enough to include traditional funds transfer solutions (money remittance, credit and debit transfers, card payments) and innovative payment solutions (for example some of those using Internet and mobile telephone technology).

[36] Authorization would require a written application along with a detailed list of information (program of operations, business plan, a description of the applicant's administrative and accounting procedures, internal control mechanisms, risk management procedures and structural organization, etc.).

of clearing and settlement services is subject to oversight standards established by the Eurosystem, in accordance with Article 105(2) of the Treaty. In this respect, the Eurosystem will, in connection with its task of promoting the smooth operation of euro area payment systems, consider whether the participation of payment institutions (which are given by the directive access rights under certain conditions) in payment systems is sufficiently safe and does not imply undue risks for the stability of the financial system.

The proposed directive has triggered a lively debate on the opportunities and risks of opening up the market for payment services to nonbanks and, in particular, to non-financial institutions as retailers, mobile telecommunication providers and other parties.

On March 27, 2007, the EU Council reached an agreement on a general approach involving a compromise on the following main issues:

- capital requirements for payment institutions;
- activities that payment institutions may undertake, in particular the granting of credit;
- the possibility of waiving application of certain provisions for smaller payment institutions or for certain instruments used primarily for the payment of small amounts (low-value payments).

The adoption of this directive will have a strong impact on the whole regulatory regime applicable to front-end nonbank payment service providers.[37]

As far as back-end providers are concerned, it is envisaged that the proposed directive would not apply to back-end service providers (it explicitly excludes from its scope of application "services provided by technical service providers, which support the provision of payment services, without them entering at any time into possession of the funds to be transferred, including processing and storage of data, trust and privacy protection services, data and entity authentication, IT and communication network provision, provision and maintenance of terminals and devices used for payment services"), nor to "services by providers to withdraw cash by means of automated teller machines (ATM) acting on behalf of one or more card issuers, which are not a party to the framework contract with the customer withdrawing money from a payment account, on condition that these providers do not conduct other payment services as listed in the Annex" to the Directive (Art.3). However, the use of agents, or entities to whom activities are outsourced would fall under the discipline of Art 11, which in its latest available version includes information requirements to the competent authorities and conditions and limits for outsourcing of "important operational activities,"[38] thus strengthening the applicable provisions compared to the original Commission' proposal (which foresaw only a general information requirement). The proposed Directive

[37] Compared to the EC's proposal, the EU Council has, i.a., amended and simplified the list of payment services that can be provided under Article 4 by payment institutions, as detailed in Annex to the Proposed Directive.

[38] "An operational function shall be regarded as important if a defect or failure in its performance would materially impair the continuing compliance of a payment institution with the requirements of its authorization or its other obligations under this Directive, or its financial performance, or the soundness or the continuity of its payment services" (EU Council version, 27.03.2007).

specifies that the authorities supervising the payment institutions would be entitled, i.a., to carry out on-site inspections also with any entity to whom payment services activities are outsourced (Art 16). It should be noted, however, that as far as the specific enforcement powers of the supervisory authorities are concerned, the actual degree of harmonization will probably depend on how the Member States will implement the Directive in the national legislation.

Much of the debate concerning the proposed directive concerns, however, the front-end providers of payment services, and in particular the activities that the new category of payment institutions will be allowed to carry out. From the recent developments in the EU Council, it would appear that will be allowed indeed to set up "payment accounts" in the name of users, but the use of such accounts would be subject to limits (they could be used only for payment transactions; the balance of an account should not be commingled with those of other users accounts, nor with the own funds of the payment service provider). Contrary to ELMIs, these new entities will be allowed to carry out other business activities (but authorities may require them to establish a separate entity). The proposed directive specifies that they may not conduct the business activity of taking deposits within the meaning of banking legislation, but they may provide credit if certain requirements are met (e.g. credit can be granted exclusively in connection with the execution of a transaction, short term, it cannot be granted from the funds received or held for payment transactions, and subject to the payment institution having an appropriate level of own funds).

Until a final text has been adopted by the EU Council and the European Parliament, it is not possible to assess in detail the scope of the innovations introduced. Given the controversial debate around a number of points touched upon by the reform, the EU Council agreement on a general approach can be considered an important step for the adoption of the proposed directive, which has now been submitted to the European Parliament.

4.3. United States

4.3.1. Oversight responsibility and enforcement

Responsibility for oversight of retail payments in the United States is spread over a number of federal and state authorities. Areas of oversight include systemically important payment systems, competition, consumer protection, prudential supervision, privacy and data security, and law enforcement. There is also significant effort by private industry to self-regulate.

4.3.1.1 Systemically important payment systems

The Federal Reserve System's Policy on Payments System Risk addresses risk mitigation in systemically important payment systems. The policy specifies principles and minimum standards for controlling risk in payments and settlement systems. The policy is consistent with international standards and is applicable to both public and private systems.[39] Portions of the policy apply specifically to the Federal Reserve's

[39] Federal Reserve Board (2007), pp. 3-16.

clearing and settlement system.[40] The policy specifies requirements upon holders of reserve accounts and procedures for managing daylight overdrafts in order to limit liquidity and credit risk.

The Federal Reserve policy statement provides guidance to both managers and regulators of payment systems. The Federal Reserve will apply the guidance where it has explicit supervisory authority or where it operates a payments system. Where it does not have authority, the Federal Reserve encourages relevant authorities to consider the guidance when evaluating payments system participants.

4.3.1.2 Competition

The U.S. Department of Justice has the authority under U.S. antitrust statutes to review competitive implications of merger and acquisitions and this type of review applies to the payments industry. If a merger or acquisition is deemed to have significant anticompetitive effects, the Department of Justice can file a lawsuit to block it. In a recent significant case, the Department of Justice blocked a merger that would have combined the Star and NYCE EFT networks.[41] The Department of Justice has not intervened in most recent merger and acquisition activity in the payments industry, presumably because the activity has not raised competitive issues.

4.3.1.3 Consumer protections

Consumer protections in electronic payments are specified in the 1978 Electronic Funds Transfer Act. The law gave the Federal Reserve Board authority to issue regulations regarding liabilities and responsibilities of all participants in electronic funds transfers. The Board's Regulation E specifies disclosure, payments authorization, and dispute resolution requirements.

Federal agencies enforce Regulation E for the institutions in their jurisdiction. This includes federal financial institution supervisory agencies for banks, thrifts and credit unions, the Securities and Exchange Commission (SEC) for brokers and dealers, with the Federal Trade Commission (FTC) for retailers and others payment participants not covered by other agencies. Enforcement may include examination of covered institutions for compliance as well as help in resolving disputes.

4.3.1.4 Prudential supervision

Banks and thrifts are under the supervisory authority of federal and state agencies. Enforcement includes regular examination as well as ongoing monitoring of the financial health and operation of the institution. Examination may include a number of payments related areas such as FedLine (an Internet based service that allows financial institutions to order and manage Federal Reserve financial services), retail payments (cheques, card-based electronic payments, and ACH), and wholesale payments (Federal Reserve wire services, CHIPS, and securities settlement).

---

[40] Federal Reserve Board (2007), pp. 17-28.

[41] "FDC-Concord Settlement," (2003).

Table 9 above lists some of the nonbank payments providers in the United States. Whether these organizations are subject to prudential supervision depends on whether they are affiliated with banks, or if not affiliated with a bank, are in an outsourcing relationship with a bank.

Some nonbank processors of payments in the United States are affiliated with banks, either as subsidiaries of the bank or as separate entities in a bank holding company. Some of the largest payments processing operations in the United States are affiliated with banking organizations such as Fifth Third Bancorp, Marshal and Isley Corporation, U.S. Bancorp, and JP Morgan Chase, or are bank associations, such as Visa U.S.A. The payment services provided by these organizations include merchant processing, electronic funds transfer (EFT) network services, and credit card processing.

Many nonbank organizations that provide or process payments in the United States have no relationship to a banking company. Among the larger organizations with these characteristics are First Data Corporation, MasterCard, and PayPal.

The authority to supervise many nonbank payments processor depends on bank affiliation. If a nonbank payments processor is affiliated with a bank, then federal laws authorizing bank supervision provides federal agencies with the authority to examine the activities of the nonbank processor. If a nonbank payment processor is not affiliated with a bank, then it may or may not be subject to federal supervision depending on whether it has an outsourcing relationship with a bank.[42]

The Bank Service Company Act of 1962 gave authority of bank supervisory agencies to examine nonbank service companies to whom banks outsource specified financial services, and payments are among those services specified. At the time the law was passed, payments services that qualified were processing cheques and deposit account management, but as the technology of payments advanced (such as ATMs, ACH, electronic payments, and online banking) so has the types of activities that qualify a service company for supervision. Details of the supervisory process for nonbank payments processors are described below

Money service businesses in the United States provide services such as money transmission, foreign exchange, or issuing traveler's cheque or money orders. Many (but not all) state governments license these businesses. Providers of services for Internet payments can be deemed money transmitters and be required to obtain licenses for any state in which its customers does business. A prominent example is PayPal, a nonbank payment provider which has obtained money transmitter licenses for locations in which it does business.

The extent of regulation and examination of money service businesses has historically been determined by state law.[43] Recently, federal regulations related to money laundering activity and gambling have been applied to money transmitters. For example, money

[42] Sullivan (2006). The names of supervised nonbank payments processors are not publicly available due to confidentiality.

[43] States are engaged in efforts to unify standards for regulation of money transmitters; see the website of the Money Transmitters Regulators Association (http://www.mtraweb.org).

service businesses must register with the federal government, obtain independent audits of their anti money-laundering program, and file federal suspicious activity reports.[44]

4.3.1.5 Privacy and data security

The Gramm-Leach-Bliley Act of 1999 contains provisions regarding the safeguarding of sensitive financial information. It reiterated and clarified the responsibility that financial institutions have in safeguarding and disclosing to customers the use of sensitive nonpublic customer information. The Act authorized enforcement by the federal financial institution supervisory agencies, the SEC, the FTC, and state government authorities according to the extent of their jurisdictions over financial institutions.

4.3.1.6 Law enforcement

Trends in payments and data security involving data breaches, identity theft, and money laundering in payments have led federal law enforcement authorities to add resources that specialize in payments crime. The Federal Bureau of Investigation now has a Cyber Operations group that investigates computer crimes such as hacking, data breaches, and release of malicious code.[45] Authorized by the USA Patriot Act in 2001, the Secret Service has established an Electronic Crimes Task Force.[46] One purpose of the Task Force is the prevention and investigation of attacks on the financial infrastructure of the United States. Finally, the Financial Crimes Enforcement Network (FinCEN) of the U.S. Department of the Treasury was established in 1990 to assist law enforcement in combating money laundering.[47] The Bank Secrecy Act requires financial institutions to report certain activities that might indicate money laundering to FinCEN. FinCEN has developed expertise that allows it to identify patterns of money laundering in reported information. It also assists prosecution of money laundering by documenting audit trails for assets tied to illegal activities.

4.3.2. Enforcement and supervisory processes for nonbank payments processors

Regulations and their enforcement of systemically important payment systems, antitrust laws, consumer protections, and law enforcement apply equally for banks and nonbanks. For example, in 1998 the FTC required the Internet service providers AOL and Prodigy to adhere to requirements of Regulation E, such as obtaining written permission from consumers before initiating ACH debits from the consumer's bank account. But there are some important differences in regulation of banks and nonbank payment providers, particularly in the areas of data security and prudential supervision.

4.3.2.1 Data security

---

[44] This website (http://www.msb.gov/guidance/bsa.html), hosted by the Financial Crimes Enforcement Network of the Department of the Treasury of the United States, describes federal requirements for money service businesses.

[45] For more information, see the Cyber Operations website at http://www.fbi.gov/cyberinvest/cyberhome.htm.

[46] For more information, see the Task Force website at http://www.secretservice.gov/ectf.shtml.

[47] For more information, see the FinCEN website at http://www.fincen.gov/index.html.

While the Gramm-Leach-Bliley sets security standards for financial institutions, there is no similar federal law for nonfinancial institutions. Retailers and merchants are the most visible example, but some nonbank payments providers may fall into this situation. The FTC has, to some extent, filled this gap by enforcing data security standards for retailers and other organizations. The FTC views breaches of payments data security as an unfair and deceptive business activity. In cases of breaches of payments data, it has reached settlements with firms as diverse as retailers, payment processors, and software developers.[48]

4.3.2.2 Prudential supervision

As noted above, bank supervisory agencies have authority over some nonbank payments processors that are not affiliated with a bank. More specifically, bank supervisors can regulate and supervise companies that provide certain services to banks. These organizations are referred to as Technology Service Providers (TSPs).[49] Many, but not all, of supervised TSPs provide payments processing services. Supervisory agencies have developed common methods of supervising and examining TSPs.[50]

Supervisors use a risk-based screening process to determine which service providers enter the supervision program. Screening is based on factors such as the risk in services provided, number of clients, and internal control environment of the organization. Clearing and settlement or wholesale payment services are examples of high-risk services, while ACH, ATM, point-of-sale (POS) transaction processing, and credit card processing are medium risk services. Also considered is the number of clients or the number of transactions processed by the TSP so that the largest TSPs would have a greater likelihood of being supervised.

At year-end 2004 there were 125 TSPs in the supervision program. The most common service offered by supervised service providers is computer services for accounting and information systems (core processing), a legacy of the Bank Service Company Act, which was enacted at a time when banks were beginning to outsource this activity. But payments processing is well represented among services offered by TSPs: 87 of the 125 supervised TSPs offer some type of payments service.

The risk screening process not only determines what TSPs are supervised but also the frequency of monitoring and examination. TSPs with high risk rating receive more frequent offsite monitoring reviews and onsite examinations.

Federal supervisory agencies have detailed guidelines for examining TSPs. The examination is based on the Uniform Ratings System for Information Technology (URSIT).[51] This system reviews the audit program for internal controls, management

---

[48] Examples include the retailer DSW, the credit agency ChoicePoint, and the software vendor Guidance Software.

[49] This section is based on Sullivan (2006), where additional details of the TSP supervision program can be found.

[50] The common method and approach is coordinated through the Federal Financial Institution Examination Council. More information is available at http://www.ffiec.gov/.

[51] Federal Financial Institution Examination Council (2003).

quality of addressing IT risks, the quality of acquiring and maintaining information technology applications, and the ability to deliver reliable and secure information.

The agencies write a report of examination based on their findings, which is made available to examiners of banks who are clients of the TSP. The report assists bank examiners by conveying information on the internal control environment of the TSP and what a bank needs do to in order to control risk in its outsourcing relationships.

4.3.2.3 Limitations of TSP supervision

The regulatory treatment of outsourcing, including that of payments related activities, depends on the bank status of the outsourcing entity. In the United States, the TSP supervision program explicitly covers technical service providers to banks. However, there are some limitations to the TSP supervision program. Three are specific to payments and a fourth applies to all supervised TSPs:

- First, protection of the payments system is a secondary purpose to the TSP supervision program. The main purpose is to protect the depositors of banks that outsource to the TSP. The report of examination provides bank examiners with information that helps them understand the risks that banks face if they choose to employ a supervised TSP. While TSP supervision helps to mitigate risk in payments, the legislative history and tradition of the program suggests that this is more of a side benefit than a major purpose to the program.
- Second, many payment providers are not eligible for supervision. The Bank Service Company Act of 1962 authorizes oversight of nonbank payment providers only when a financial institution is outsourcing specified services to a provider. Common outsourced activities include credit card processing services, cheque processing services, or ATM transaction processing. But many nonbank payments providers do not have this outsourcing relationship. A payroll processor may purchase ACH services from a bank, or an Internet payments processor may purchase transaction processing services from a financial institution, or a cheque cashing service may purchase services from a bank to process cheques.
- Third, an unknown number of service providers are not in the supervision program. For example, after a 2005 security breach at a payments processor, news stories reported the existence of roughly 500 companies that process credit card payments.[52] But there is no comprehensive data source that would show the number of companies that provide payment services to financial institutions. The screening process does ensure that this group probably includes the largest service providers.
- Fourth, supervisory agencies can examine the payment provider but have limited enforcement power (relative to enforcement over financial institutions) if they find weaknesses at the organization. Supervisors can prohibit financial institutions from doing business with the service provider. One reason for limited enforcement power is because the primary purpose of examination is to limit risk

[52] Dash (2005).

of banks who are clients of the service company, not to protect the service company.

4.3.3. Industry self-regulation

The payments industry contributes significantly to risk mitigation through a number of self-regulation efforts. Recent initiatives are most visible in payments networks, but there are other efforts. To a considerable extent these programs set standards for control and mitigation of payments risk.

4.3.3.1 The ACH network

The National Automated Clearing House Association (NACHA) consists of financial institutions, industry councils, and other stakeholders in the ACH system. NACHA sets rules and standards for ACH transactions, and also has some enforcement responsibilities. In 2005, NACHA reorganized its risk management infrastructure, creating a Risk Management Advisory Group to help implement a new risk management framework.[53] Subsidiary work groups are addressing three areas of risk mitigation: control of access to the ACH system, the monitoring and control environment, and enforcement activity.

4.3.3.2 Credit card networks

The credit card networks developed a Payment Card Industry (PCI) data security standard that began a phased implementation in 2005. It sets twelve requirements involving topics such as data encryption, intrusion detection, activity monitoring, and access controls. The standards apply to all card network members, merchants that accept credit cards, and credit card payments processors. Some of the expectations in the standard are risk based, with larger retailers and payments processors subject to stricter requirements for ensuring data security.

4.3.3.3 Other efforts

The payments industry has also established mechanisms designed to foster cooperation across the industry in developing techniques to limit risk and to share information that can assist in fighting fraud. For example, the Financial Services Information Sharing and Analysis Center (FS-ISAC) was established by the financial services industry in 1999.[54] This private sector initiative allows members to share information about security incidents that represent threats to the U.S. financial infrastructure. By allowing confidential reports of security incidents, FS-ISAC can overcome the reluctance of firms to release information that can damage a firm's reputation. As a result, FS-ISAC can build a large database of security events, which FS-ISAC can analyze to determine vulnerabilities and develop responses to threats in a timely manner.

---

[53] NACHA (2006).

[54] For more information, see the FS-ISAC website at http://www.fsisac.com.

Similarly, in 2006 First Data and five large banks formed a joint venture called Early Warning Services LLC.[55] The company would be a vehicle for payments providers to share information and expertise on fraud prevention and screening of customers. It intends to use this information to develop mechanisms to better identify and authenticate customers.

The Partner Group is a private industry effort whose goal is to foster cooperation among the payments channels and address emerging risks that may cross payment applications.[56] Historically, each payments channel—cheques, ACH, EFT networks, and credit card networks— has developed separate standards and approaches to reducing risk. To accomplish its goal, The Partner Group has established three working groups with representative from each payment channel to address sharing of fraud information, liability assignment among networks, and access of third parties to the payments system.

4.4. EU – U.S. comparison

The regulatory framework facing banks and nonbanks operating in the payments arena contains both similarities and differences in comparing the European Union and the United States. One important similarity is the expectation that banks that outsource payments processing are to be responsible for controlling risk in the outsourced activity. A second is, in both cases, supervisors are given the authority to oversee payment processors affiliated with banks. And third, there is some reliance on self-regulation, although the U.S. approach appears to be somewhat less formal than that of the European Union.

However, there also are a number of differences in the regulatory frameworks. For one thing, the governance structure is very different. Europe has governing bodies that can direct countries to take certain actions—once agreement is reached at the EU level, the countries, in a sense, are bound to implement the common decision. In the United States, in contrast, the federal government can pass laws that apply to all the states, but generally the federal government creates its own administrative units to implement the laws. Thus, in Europe, there exist strict cooperation mechanisms, embodied in the Treaty, that regulate the relations among EU institutions. Member States and/or other relevant authorities (for example the European System of Central Banks) in their respective fields of competence ensure implementation of common policies through legislative or administrative action, while in the United States there is nothing equivalent.

Other differences include:

(1) The ECB has clear regulatory authority over payments, while the Federal Reserve's authority is somewhat more limited and less well established in legislation.

(2) Supervision of nonbank payments processors is not uniform across the various countries of the European Union, while it is more uniformly applied across the states of the United States. The proposed Payments

[55] "US Banks Collaborate on Data Security," (2006); Breitkopf (2006).

[56] The Partner Group (2007). The Partner Group is sponsored by Banking Industry Technology Secretariat (BITS), a financial industry consortium that is a vehicle for industry collaboration on emerging issues. For more information, see the BITS website at http://www.bitsinfo.org/index.html.

Directive, however, should bring more harmony to treatment of both bank and nonbank payment processors in the European Union.

(3) In the European Union, a legislative initiative is underway to allow the provision of payment services to end-users by a new category of (nonbank) payment institutions.

(4) The United States has no equivalent to the ELMIs or the "payments institutions" anticipated in the proposed EU Payments Directive.

(5) The European Union appears to be more active in antitrust actions than the United States.

5. Central bank oversight

As noted in the previous section, one of the main objectives of payments regulation is to maintain public confidence in payment instruments and systems by entrusting a public authority with the responsibility to carry out oversight of payments systems. Usually this task is assigned to central banks, and the primary objectives of the oversight function are to ensure the safety and efficiency of payment systems. This section explores central bank oversight issues, focusing primarily on risk but also briefly addressing efficiency and possible tradeoffs between risk and efficiency. Emphasis is placed on the implications and policy issues arising from the increased prevalence of nonbanks in retail payment systems.

5.1. Risk

5.1.1. Risks in payments clearing and settlement

During the payment process various types of risks may arise, and all the parties involved may be exposed to some of them at different stages, and to different degrees. Operational risk is present when payment orders are transmitted over communication networks. Parties that exchange assets to extinguish payment obligations may be exposed to financial risks (e.g. liquidity and credit risk). All parties entering into contractual relations in the context of payments processing may be exposed to legal risk. Financial institutions that participate in the clearing settlement systems are vulnerable to operational, liquidity and credit risk. These risks sometimes compound one another. If operational risk results in a computer outage, one payment participant may not receive funds from other participants, and it may need to refinance at higher prices, or suffer liquidity risk if it is unable to fulfill subsequent payment obligations, or incur legal risk if it is held liable to other parties.

These risks and their relevance for the safe and smooth functioning of the payment system, financial markets, and the economy have been analyzed at length, particularly by central banks, and appropriate principles for their management and mitigation have been set at an international level. Definitions of the main risk categories are provided in Box 2. Although in general retail payments do not carry systemic risk, there are cases where retail payment systems have been considered systemically important (as in the Eurosystem; see section 4.2).

Box 2: Main risks in payments and settlement

Credit risk	The risk that a counterparty will not settle an obligation for full value, either when due or at any time thereafter. In exchange-for value systems, the risk is generally defined to include replacement cost risk and principal risk, and settlement agent risk.
Liquidity risk	The risk that a counterparty will not settle an obligation for full value when due. Liquidity risk does not imply that a counterparty or participant is insolvent, since it may be able to settle the required debit obligations at some unspecified time thereafter.
Operational risk	The risk that deficiencies in information systems or internal controls, human errors or management failures will result in unexpected losses (internal and external events). Recent changes in the retail payments system have increased awareness of the following types of risk, which are often thought of as subcategories of operational risk. These are particularly relevant for those payments processing models relying on open communication networks or involving storage of personal data: • *Data security risk*: a form of operational risk involving unauthorized modification, destruction, or disclosure of data used in transactions or used to support transactions. • *Fraud risk***:** Risk of financial loss for one of the parties involved in a payment transaction arising from wrongful or criminal deception. The risk that a transaction cannot be properly completed because either the identity of the payer cannot be easily ascertained or the payee does not have a legitimate claim on the payer. • *Counterfeit* (for e-money): The legal offence of making a false instrument in order that it may be accepted as genuine, thereby causing harm to others (forgery).[57]
Legal risk	The risk of loss because of the unexpected application of a law or regulation or because a contract cannot be enforced.
Settlement risk	The risk that settlement in a transfer system does not take place as expected, usually due to a party defaulting on one or more settlement obligations. This risk comprises in particular operational risks, credit risks and liquidity risks.
Settlement agent risk	The risk of failure of the settlement agent, i.e. of the entity whose assets are used to settle the payment obligations. In interbank payment systems, one way to eliminate this risk category is to settle in central bank money (banks use as settlement accounts the accounts they hold with the central bank). When a bank acts as settlement bank for other banks or intermediaries, settlement is said "in commercial bank money."
Reputational risk	The risk that the materialization of another risk category damages the confidence in a payment services providers. The loss of reputation of a main payment services provider may further increase actual problems of that service provider (e.g. access to liquidity) and may even finally result in the loss of public confidence in the payment instrument.

[57] Smullen and Hand (2005).

Illicit use	The risk that a payment method may be used for illicit purposes such as money laundering, terrorism financing, or illicit commerce.
Compliance risk	The risk of loss associated with non-compliance with laws, rules, regulations, prescribed practices, or ethical standards. The risk is borne by the issuing, the distributing and the transaction archiving institutions and in general by the institutions subject to a compliance duty.
Systemic risk	The risk that the failure of one participant in a transfer system, or in financial markets generally, to meet its required obligations will cause other participants or financial institutions to be unable to meet their obligations (including settlement obligations in a transfer system) when due. Such a failure may cause significant liquidity or credit problems and, as a result, might threaten the stability of financial markets.

The risk profiles of payment systems (and the risk mitigation techniques employed to minimize exposure to them) may change over time, following the introduction of new business models, the restructuring of business processes, the reorganization of systems, or simply the introduction of new technologies and the adoption of innovative means of communication. In particular, the recent use of open communication networks for the transmission and storage of payment related information (including sensitive personal data) has affected all payment systems. Because the pace of change has accelerated, a risk category that is particularly relevant for retail payment instruments is reputational risk, due to the reliance on public trust for their acceptance. In addition, data security risk, fraud risk and counterfeit risk for e-money have become more prominent.

The next section addresses the question of how the widespread and rising presence of nonbanks in retail payment processing affects risks that are normally present in payment systems. Included are examples of incidents involving nonbanks that in theory could have affected the safe functioning of payments systems and payment schemes or affected public confidence in payment instruments.

5.1.2. Implications of rising nonbank presence for risk

Access to payment systems traditionally has been restricted, at least in part, to banks and other intermediaries that are subject to prudential supervision. One reason is to reduce risk exposures that may emerge among payment systems participants during the clearing and settlement process (typically in retail payment systems). Another reason is that the accounts used by banks to settle reciprocal payment obligations (as principals or on behalf of their customers) are accounts held either one-with-another (nostro and loro accounts, as in correspondent banking) or with one central institution that serves a larger banking community. Examples of such central institutions are central banks, which have a long tradition of establishing and operating payment systems for the banking sector. Both self-interest and regulation have led banks to develop strong safeguards against illicit intrusion in their information technology systems and networks.

The rising importance of nonbanks and the multiple roles they play both at the front-end and back-end of the payments chain have changed this traditional setting. In some

ways, nonbanks contribute to an increase in the relevance of certain risks. In other ways, nonbanks decrease the relevance of other risks or facilitate the containment of risks.

Nonbank presence may increase the vulnerability of payment systems to certain risks. This may happen in at least three ways:

First, on the simplest level, nonbanks pose risk because they may offer alternative points of entry for criminals into the payments system, particularly in the early stage of the introduction of new payment solutions. One example of this kind occurred in 2000, when two individuals used unauthorized access to Internet service providers (ISPs) in the United States to misappropriate credit card, bank account and other personal financial information from more than 50,000 individuals, hijacked computer networks and then used the compromised processors to commit fraud through PayPal and the online auction company eBay.[58] Since this incident, PayPal has been successful at improving its data security and fraud detection systems.[59]

Second, and more broadly, banks traditionally act as gatekeepers to the payments system.[60] When banks outsource payment processing services to nonbanks they provide nonbanks with a de facto, technical access to the payments systems that may increase vulnerability to various sources of operational risk. Traditionally, banks have managed these relationships to reduce this risk, but incidents may materialize, as shown by a recent example: the U.S. company CardSystems, Inc. experienced a breach of its computer system in 2005 that exposed 40,000,000 records of transactions with 263,000 records stolen. Credit card associations determined that CardSystems violated their security and record retention standards and, as a result, Visa chose to refuse transactions from CardSystems.

In addition to outsourcing, a very similar risk may arise when banks sell payments services to nonbanks. Banks mitigate this risk with know-your-customer practices that allow banks to detect attempts to exploit payment services and carry out illicit activities. An example of bank liability for improper monitoring of payment services provision to a nonbank customer was reported in the United States in 2003, when the Federal Trade Commission issued press releases explaining how it had closed down several companies (the Assail Telemarketing Network and affiliates) that engaged in fraudulent telemarketing activities. Assail used the ACH services of First Premier Bank; the bank admitted that it had failed to perform due diligence on the activities and legitimacy of its customers (but it did supply information to the investigative agencies); the bank later paid $200,000 in fines as part of a wider settlement and agreed to vigorously engage in know-your-customer actions and ongoing monitoring of customer activity.[61]

---

[58] U.S. Department of Justice (2002). In addition, <http://www.physorg.com/news84545784.html> (December 5, 2006) describes some of the techniques used by criminals to perpetrate fraud through online auction sites.

[59] While these efforts have not totally eliminated fraud, they have had considerable success: statistics reported in the press show loss rates due to fraud for merchants who use PayPal that are noticeably below the e-commerce average; see Cox (2001), Wilson (2002) and Garver (2005).

[60] Braun and others (2007).

[61] Federal Trade Commission (2005). This was the first time that the Federal Trade Commission tried to hold a bank responsible for the deceptive practices of its customer.

To limit such risks, banks must screen and understand potential nonbank clients and service providers, execute contracts that delineate responsibilities and liabilities, and monitor the business activity and internal control environment of the nonbank. While this risk is not new to banks, the difficulty faced today is that the payment system gatekeeping function may be more of a challenge because established methods of screening and monitoring may be inadequate given the development of new payment types and emergence of new types of business (such as online retailers). Moreover, this gatekeeping function may have become more critical compared to the past because of the complexity of the computer technology involved, which can be exploited in a manner that is fast, can be scaled to large values, and can be difficult to detect or trace.

Third, in some cases nonbanks play a key role for the functioning of an entire retail payment system, either because they run the infrastructure used by it, or because they de facto concentrate the processing for an entire retail payments market segment. Under these circumstances, nonbank presence may have implications at the system level. While concentration is the often the natural consequence of the huge scale economies present in the payment industry, it also makes these key service providers a potential single point of failure that could trigger a large scale disruption. For example, the international credit card system relies on very few cards schemes. A major disruption at a key player may have the potential to impair the ability of millions of customers in several countries to make card payments.

The above discussion points out that nonbank access to payment systems may entail some risks. Furthermore, such risks may be exacerbated by the trend towards electronic payments, as electronic payment networks require a high degree of simultaneous coordination among all participants, with an increased need for co-operation between banks and nonbanks. In principle, this is not directly related to the nonbank status of the new service providers, but rather to the fact that the presence of many different entities in a payment network complicates its design, its functioning, the sequence and execution of transactions, and the regulation and implementation of security standards.

Nonbanks have been very active in introducing new access modalities to traditional bank payment services, and in facilitating the conversion of one payment instrument into an electronic format that allows its processing in the infrastructures that originally where designed for other payment instruments. This innovation has caused some blurring of the lines between payments channels. Various U.S. payment channels, for example, are becoming less distinct. Most visibly, some cheque payments are now being converted into ACH payments. But there are other changes that make the lines between payments systems less obvious. The ACH system is developing its systems to be more and more useful for retail payments. The ACH is also being used for some significant large-scale payments, such as the settlement of payments arising from the credit cards networks.

A useful concept for resiliency in the payments system is redundancy: if one channel has problems, users may be able to get by using another channel until the problems are solved. But because of the interdependence of payments channels, the level of redundancy may have decreased, with adverse effects on service continuity.

The extension of payments systems to new uses also increases potential for cross-channel risk. For example, criminals typically exploit weaknesses in the payments

system. If one payment channel improves its security, criminals will probe other channels as alternatives (this may explain why fraud attacks concentrate on innovative payment communication networks and do not seem to attempt the relatively more isolated and protected typical transmission networks such as SWIFT).

It should be noted that nonbanks also bring new technology and perspectives that can significantly contribute to reducing risk in the payments system. For instance, outsourcing some security-related activities like customer authentication to specialized firms may result, in principle, in better management by the outsourcing banks of certain threats to payments security and, thus, in an improvement of the risk mitigation techniques they employ. Furthermore, the payments industry as a whole benefits from the adoption of innovative process-designs for traditional payment instruments. For example, the overall level of credit risk exposure may decrease by the adoption of on-line real time controls of funds or credit limit coverage for submitted payment instructions. Nonbank service providers are proposing to the industry significant innovative technological solutions, such as biometric authentication, which may reduce fraud exposure.

5.1.3. Policy issues related to risks

As mentioned above, the containment of risks in payment systems and the safe use of payment instruments are objectives of central bank oversight. Because rising nonbank presence potentially contributes to an increase in certain types of risk, a consequent question to ask is whether the current scope of oversight by central banks remains sufficient. The proper scope of central bank oversight needs to be defined in light of the institutional and historical factors unique to each country or currency area. It does not need to be uniform across countries with different institutional settings. For example, market forces are crucial to controlling payments risk, and the level and scope of oversight should be tailored to the specific ability of the payments market to control and mitigate risk. Furthermore, the scope of oversight needs to remain dynamic in its definition, and as markets and infrastructures evolve, it may need to be adapted to ensure the achievement of oversight objectives and maintain effectiveness. For instance, payment systems oversight originally focused on large-value payment systems, but in some countries has subsequently widened its reach to retail payment systems and instruments.

Issues that deserve attention from this perspective are first, the legal basis for oversight (from which the scope of oversight is traditionally derived), and second, the need for co-ordination among various authorities with different competencies that directly affect nonbank payment service providers.

As noted in section 4, within the European Union and the United States, there is wide variation in authority. Federal Reserve Chairman Bernanke recently stated that "In contrast to the situation in some other countries, the Federal Reserve lacks explicit legal authority to oversee systemically important payments systems."[62] By contrast, a clear legal competence of the Eurosystem in payment systems is established in the legal statutes. Furthermore, the national central banks in Europe often enjoy specific, explicit, national legal recognition of their powers and responsibilities in the oversight of retail

[62] Bernanke (2007).

payment instruments. For example, the Banque de France has broad power to oversee all cashless payments. Thus, in Europe, payment systems and payment instrument oversight is more recognized as a basic function of the central bank. As described in Section 4.2, the co-ordination between European and national policies is ensured by a clear allocation of competencies and responsibilities which were made public with a "Policy Statement" (ECB, 2000).[63] In particular, it is explicitly provided that where new developments occur or where retail schemes would have potential cross-border implications, general policy lines for oversight are defined at the Eurosystem level and that the Eurosystem may also formulate policy concerning the security of payment instruments in order to maintain the confidence of the users of the payment systems.

In the United States, the main entry point of authority to oversee payments in terms of risk is through bank supervision.[64] But the main purpose of bank supervision is normally to ensure that a bank is operating in a safe and sound manner so as to protect depositors. While this does protect payments, the historical purpose of such supervision is not to explicitly protect the payments system. Furthermore, the supervisory system in the United States is spread across the Federal Reserve System, the FDIC, the OCC, the NCUA, and state supervisory agencies. All of these agencies have separate priorities and even if they were asked to place emphasis on the safety of payments, a great deal of coordination would be required to ensure uniform approaches to oversight through this channel.

Additionally, important elements of oversight in the United States are outside of the banking and bank regulatory system (such as law and antitrust enforcement) or straddle banks and nonbanks (such as consumer protections, privacy, and data security).[65] Some of these elements of oversight have a direct role in risk and risk mitigation for payments. The influence of others may be indirect either because they define rights and responsibilities that are crucial to the incentives that payments participants have in controlling risk, or because there are significant trade-offs between efficiency and risk.

Coordination of oversight may be more important in today's payment system. At present, many of these elements of oversight in the United States have a great degree of independence. At the same time, payments have become more dependent on network architecture and, as a result, all elements of the network are significantly interdependent. Oversight policy perhaps should adopt a perspective that accounts more carefully and completely of payments as a system.

---

[63] See section 4.2. In particular, the Governing Council formulates the common policy stance (e.g. in the cases where the implementation of monetary policy, systemic stability, the establishment of a level playing field among market participants or cross-border payments are involved). In the areas not specifically covered by the common oversight policy, policies defined at an NCB level apply within the framework of the Eurosystem policy, and in relation to them the ECB Governing Council can always take an initiative if felt necessary (it should be noted that the ECB shall be consulted on any provision in its field of competence and this includes national rules and regulations in the field of payment systems).

[64] Chairman Bernanke also stated that "Federal Reserve powers in this area derive to a considerable extent from its bank supervisory authority. Notably, some key institutions providing clearing and settlement services hold bank charters that place them under Federal Reserve oversight....The Fed is also either the direct or umbrella supervisor of several large commercial banks that are critical to the payments system through their clearing and settlement activities"; Bernanke (2007).

[65] Sullivan (2007).

Bank outsourcing of payments processing functions and activities raises the issue of whether such outsourcing should be subject to oversight review. Should this review have a purpose of protecting payment systems or of ensuring safety of payment instruments? How effective would such oversight be?

Sometimes the oversight objectives of payment risk reduction may be achieved by market self-regulation rather than by regulatory action. However, can overseers rely on nonbank self-regulatory initiatives in order to control risk? Experience shows that voluntary regulation by the payments industry is important but may face considerable hurdles to be effective, particularly in the absence of proper incentives or penalties for non-compliance. The card network's PCI standards, for example, began taking effect in June 2005, but reports suggest that U.S. compliance rates are relatively low.[66]

Industry self-regulation can be effective if compliance monitoring is well-designed (such as allowing self-assessments only for low risk payments providers) and if severe penalties for non-compliance are imposed, including potential exclusion from the network or payment scheme. However, an important question with a market-based approach is whether private incentives are sufficient.

An individual payment participant will control risk to the point where marginal private benefits and costs are equal. But because of the interdependencies in a payment network, other members of the network will derive some benefit. This implies that the marginal private costs of risk control will be less than the social benefit and that the collective level of risk control effort will fall short of the level that is socially optimal. This does not necessarily imply that regulatory intervention is warranted. Rather, it would depend on the size of the externality as well as the effectiveness of regulation.

In Europe, the forthcoming regulatory opening to a new category of nonbank companies (the payment institutions, including merchants, telecommunication companies and so on) of the front-end services market raises additional policy issues. One example is whether it would be necessary to complement the envisaged supervisory framework (which focuses on the service provider) with minimum safety standards for the payment instruments or schemes, in order to safeguard public trust in their safe use. For instance, some innovative payment solutions present today a limited risk profile given their limited use and the fact that they process payments of very limited or small amount. However, it is not excluded a priori that the possible success of certain schemes may lead to extend the payment service to buy new classes of goods and services of higher value, thus leading to payments of possible larger individual or aggregate amount, depending on the expected profitability of the services and on the risk appetite of the payment institution.

From the perspectives of customer protection, and of safeguarding public trust in payment instruments, it is important that all parties involved have a clear understanding of the risks involved in the various solutions, so that they can choose the service most suitable to the individual risk preferences. In order to assess such future developments, a thorough analysis of the possible risk categories involved and their relevance would need to be carried out. Possible standards for payment instruments or schemes could be based on a functional approach, ensuring that to the extent that similar risks arise, appropriate

[66] Sidel (2006). Visa has recently increased sanctions for noncompliance and has implemented a reward program to encourage implementation; see Aplin (2006).

and proportionate safeguards are in place, irrespective of the legal status of the provider. It should be noted that safety standards for the payment industry may not need to be mandatory, as oversight recommendations or industry self-regulation may represent effective solutions. Furthermore, oversight or self-regulatory standards/recommendations may not initially be needed in view of the limited initial use of innovative products. However, it cannot be excluded that they may become useful in the future once the customer base has widened.

Finally, when reviewing risks in payment schemes, one very relevant element is the incentive structure of its participants and users. In particular, there may be merit in applying the basic rule that liability for a payments participant's actions be matched with the ability to control risk. There are numerous examples in the payments industry where this is not the case. For example, why should a consumer take extra care to protect a credit card when he/she often faces zero liability if the card is lost or stolen and used fraudulently? Why should a retailer take precautions to secure card payment data when card issuing banks find it difficult to recover the cost of reissuing payment cards caused by the retailer's data breach?[67] Why would a bank develop internal systems to detect and prevent fraud or illicit payments if the cost is passed on to account holders? Given the problem of externalities in risk control, it is doubly important that other barriers to a socially optimal level of risk control are absent.

5.2. Efficiency

5.2.1. Efficiency considerations in payments

Efficiency is another major objective of central bank oversight of payment systems. The increasing importance of network effects in concert with the growing prominence of nonbanks raises a number of policy questions:

- Is there a market test adequate for evaluating efficiency of payment innovations? Technological innovation is a major driving force for improving efficiency, but some innovations may be counter-efficient by circumventing appropriate regulation or building up market power or entry barriers. There may be no simple rule to evaluate the efficiency of innovations.
- Is market power counter-efficient in the payment industry? The presence of network externalities in the payment market may lock in a competitive structure that may not be socially optimal. In addition, given the existence of network externalities, economics of scale, and switch costs, payment markets tend to be concentrated, which could result in monopoly pricing and inefficient output. On the other hand, the market power of incumbent firms could also have some efficiency-improving effects such as scale economies in production, added R&D and technological innovation, or internalization of market externalities.

[67] After a 2004 data breach at the retailer BJ's Wholesale Club, several financial institutions sued BJ's to recover costs of reissuing thousands of debit cards at a cost of $10 to $20. The lawsuits were dismissed because the financial institutions did not have a direct contractual relationship with BJ's. See Pereira (2007).

- To what extent is public intervention warranted? Public intervention is not always effective in addressing market failures. Historically, government attempts to regulate industries with large economies of scale have sometimes failed due to asymmetric information and misaligned incentives. Government intervention in a standard setting may also be undesirable if it leads to an outcome worse than even a second-best technology chosen by the market.

5.2.2. Tradeoffs between risk and efficiency

While central banks strive to ensure both safety and efficiency, these goals are not independent. Oversight can be complicated by a tradeoff between safety and efficiency, which suggests the following policy questions.

- Should nonbanks be granted more access to the payments system? From an efficiency point of view, it is preferred that as many participants as possible share a payment infrastructure. However, from a safety point of view, some exclusion is necessary to ensure adequate risk mitigation. Moreover, the longer the supply chain or the larger the network for a given payments technology, the greater is the potential for disagreement about the appropriate level of risk control.
- Should public authorities be more active in setting risk mitigation standards? Some efficient technologies or business models may inevitably have higher risks than others, and often the market is relied on to decide the balance between safety and efficiency. A critical question is whether market solutions are adequate and in what circumstances public intervention can improve market outcome. Oftentimes, a mandatory one-model-fit-all approach to safety compliance may induce undesired efficiency losses.
- What is the appropriate cost of controlling risk of illicit use of payments? In principle, many of the features that provide value for legitimate transactions can also make them susceptible to misuse by individuals engaging in money laundering and terrorism financing. Although payment systems can guard against illicit use through various measures, the high degree of similarity between the needs of legitimate and illegitimate users of payments technologies, as well as the need to balance societal costs and benefits, suggests that it is a complex issue to determine what constitutes an acceptable threshold of illicit use for society.

6. Summary and future research

Retail payments systems throughout the world are undergoing fundamental change. Traditional paper-based forms of payment are giving way to electronic forms of payment. Technological advances are making possible new front-end payment instruments and new back-end processing methods. New products, new business models, new markets, and new alliances are an everyday occurrence.

One key element of this new environment is the increased importance of nonbanks in the payments system. Nonbanks are making their presence felt at all stages of the payments chain. At this time, nonbanks appear most prominent in the United States, but

they are prominent in many European countries as well. And, most importantly, their presence appears to be increasing in virtually all countries.

What does a rising presence of nonbanks imply for retail payment systems? Potential impacts are many: heightened innovation, more competition, easier end-user access, and a changing risk profile. What does a rising presence of nonbanks imply for public policy? Again, potential impacts are many: a need to evaluate current regulatory frameworks, a need to study possible tradeoffs between efficiency and risk, and a need to better understand the risk profiles of innovative payment solutions and the complexities of payment technologies and third-party business linkages.

This paper represents a first step in learning more about nonbanks in the payments system. Much additional work needs to be done. Staff at the ECB and the Federal Reserve Bank of Kansas City will be exploring some of the open questions above, and plan on publishing an extended version of this paper in the months to come.

REFERENCES

Aplin, Donald G. (2006), "Visa Offers Banks PCI Compliance Rewards, But Will Also Increase Enforcement Sanctions," *BNA Banking News*, December 22.

Bank for International Settlements (2003), *Sound Practices for the Management and Supervision of Operational Risk*, Basle, Switzerland.

Bank for International Settlements (2004), *Survey of Developments in Electronic Money and Internet and Mobile Payments*. Basle, Switzerland.

Bernanke, Ben S. (2007), "Central Banking and Bank Supervision in the United States," Allied Social Sciences Association, January 5.

Bradford, Terri, Matt Davis, and Stuart E. Weiner (2003), *Nonbanks in the Payments System*. Federal Reserve Bank of Kansas City.

Braun, Michele, Jamie McAndrews, William Roberds, and Richard Sullivan. (2007), "The Economics of Managing Risks in Emerging Retail Payments," Federal Reserve Bank of New York *Economic Policy Review*, forthcoming.

Breitkopf, David (2006), "Fight vs. Fraud Spurs Five-Bank First Data Deal," *American Banker*, May 26.

Cordone, Nicola (2004), "SiNSYS: the birth of the new pan-European reality in card processing," in Giorgio Pacifici and Pieraugusto Pozzi, eds., *Money-on-line.eu Digital payment systems and smart cards*. Milan: Franco Angeli.

Cox, Paul (2001), "PayPal and FBI Team Up," *Wall Street Journal,* June 22.

Dash, Eric (2005), "Take a Number,'" *The New York Times*, July 30: 1.

Deutsche Bundesbank (2006), "Recent Developments in Payment Cards and Innovative Electronic Payment Procedures," *Monthly Report*. Frankfurt am Main, Germany.

"FDC-Concord Settlement Requires FDC to Sell NYCE," (2003), *Digital Transactions News,* December 15.

European Central Bank (2007), *Payment and Securities Settlement Systems in the European Union*. Frankfurt am Main, Germany. forthcoming.

European Central Bank (2006a), *Opinion of the European Central Bank of 26 April 2006 on a Proposal for a Directive on Payment Services in the Internal Market (ECB/2006/21)*, Official Journal of the European Union C 109,09.05.2006, 10-30.

European Central Bank (2006b), *SEPA, The Single Euro Payments Area, An Introduction*, Frankfurt am Main, Germany.

European Central Bank (2005a), *Assessment of the Euro Retail Payment Systems against the Applicable Core Principles*. Frankfurt am Main, Germany.

European Central Bank (2005b), *Report on retail payment innovations 2005*. Frankfurt am Main, Germany.

European Central Bank (2003a), *Electronic Money Systems Security Objectives According to the Common Criteria Methodology*. Frankfurt am Main, Germany.

European Central Bank (2003b), *Oversight Standards for Euro Retail Payment Systems*. Frankfurt am Main, Germany.

European Central Bank (2000), *The Role of the Eurosystem in the Field of Payment Systems Oversight*. Frankfurt am Main, Germany.

European Central Bank (1998), *Report on Electronic Money*. Frankfurt am Main, Germany.

European Commission (2007), "Communication from the Commission Sector Enquiry under Art 17 of Regulation 1/2003 on Retail banking (Final Report)," Commission of the European Communities. COM(2007) 33,final, Brussels: Belgium.

European Commission (2006), "Commission Staff Working Document on the Review of the E-Money Directive (2000/46/EC)," Commission of the European Communities. SEC(2006) 1049,19.07.2006, Brussels: Belgium.

European Commission (2004), "Application of the e-Money Directive to Mobile Operators: Guidance Note from the Commission Services," http://ec.europa.eu/internal_market/bank/docs/e-money/guidance_en.pdf.

European Commission (2003), "Comparative Tables of National Rules," http://ec.europa.eu/internal_market/payments/framework/comparison_en.htm.

European Commission (2002), "Commission Decision Relating to a Proceeding under Article 81 of the EC Treaty and Article 53 of the EEA Agreement." *Case No. COMP/29.373-Visa International-Multilateral Interchange Fee.* 318, 22.11.2002, 17-36.

Eurostat (2007), *Europe in Figures - Eurostat Yearbook 2006-07*. Office for Official Publications of the European Communities: Luxemburg.

Federal Financial Institution Examination Council (2003), *Supervision of Technology Service Providers*, IT Examination Handbook.

Federal Reserve Board. (2007), *Federal Reserve Policy on Payments System Risk*. Washington D.C.: United States of America.

Federal Trade Commission (2005), "International Telemarketing Network Defendants Banned from Telemarketing," Press Release, January 24.

Financial Action Task Force – Groupe d'action financière (2006), *Report on New Payment Methods*. Paris: France.

Garver, Rob (2005), "eBay and Banking: Is PayPal a Serious Rival? *American Banker,* November 15.

Masi, Paola (2004), "The Evolution of Electronic Payment Systems and Instruments," in Giorgio Pacifici and Pieraugusto Pozzi, eds., *Money-on-line.eu Digital Payment Systems and Smart Cards*. Milan: Franco Angeli.

Moeller, Götz (2006), "Outsourcing Payment Transaction Processing in a SEPA Environment," *Journal of Payments Strategy & Systems*, 1: 71-86.

NACHA (2006), *Risk Management News,* Vol. 2. Issue 2. pp. 1-2.

Partner Group (2007), "Third Party Payments System Access Control Working Group White Paper," available at http://www.bitsinfo.org/downloads/Publications%20Page/PaymentsThirdPartyWGFINALWMatrix.doc

Pereira, Joseph (2007), "Bill Would Punish Retailers for Leaks of Personal Data," *The Wall Street Journal*, February 22: B1.

Rosati, Simonetta and Stefania Secola (2006), "Explaining Cross-border Large-value Payment Flows: Evidence from TARGET and EURO1 Data", *Journal of Banking & Finance*, 6: 1753-1782.

Shy, Oz (2001), *The Economics of Network Industries*. Cambridge University Press, UK.

Sidel, Robin (2006), "Credit Firms Push to Thwart Fraud," *The Wall Street Journal,* September 25: C1.

Smullen, John and Nicholas Hand (2005), *A Dictionary of Finance and Banking,* Oxford University Press. Oxford Reference Online http://www.oxfordreference.com

Sullivan, Richard J. (2006), "The Supervisory Framework Surrounding Nonbank Participation in the U.S. Retail Payments System: An Overview," Federal Reserve Bank of Kansas City, Payments System Research Working paper 04-03.

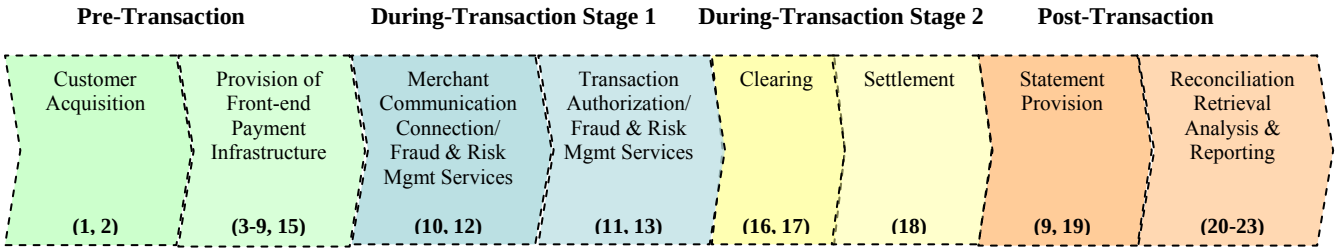
Sullivan, Richard J. (2007), "Risk and Oversight Implications of Nonbank Participation in the U.S. Retail Payments System," Federal Reserve Bank of Kansas City *Economic Review*, forthcoming.

"US Banks Collaborate on Data Security," (2006), *Cards International,* June 13.

U.S. Department of Justice (2002), "Russian Computer Hacker Sentenced to Three Years in Prison," Press Release, October 4.

Wilson, Ralph F. (2002), "Assessing Criticism of PayPal," *Web Commerce Today*, March 15.

Figure 1: Broad Payment Activities



Note: Numbers in parentheses refer to Primary Activities in Table 3.

Figure 2: Nonbank Involvement in a MasterCard/Visa Credit Card Transaction Initiated by Mobile Telephone

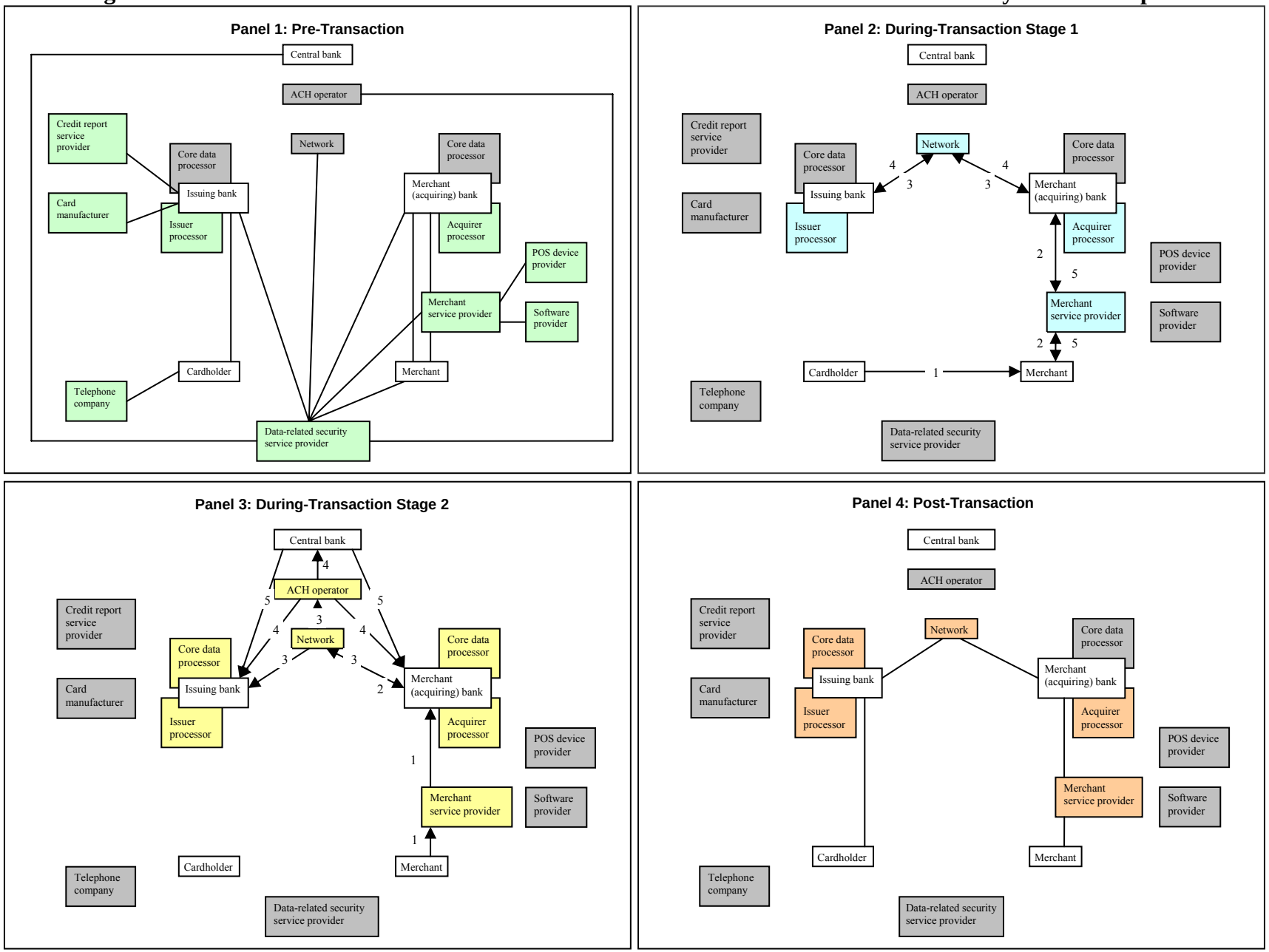


Table 1: Broad Payment Types

1	Electronic Cheques
2	Credit Transfers
3	Direct Debits
4	Payment (Credit/Debit) Cards
5	Money Remittance/Transfer
6	e-Money and Other Pre-funded/Stored Value Instruments (including Internet P2P)
7	Other Payment Instruments

Table 2: Detailed Payment Types

	1	2	3	4	5
	Broad type	**European version**	**Physical environment**	**US version**	**Physical environment**
1	electronic cheques	cheque to ACH (truncated cheques); cheque imaging at POS	POS	check to ACH	POS
			mail		mail
					telephone
					Internet
2	credit transfer	national ACH; PE-ACH; correspondent banking or other settlement channels in some countries	POS	ACH	POS
			telephone		e-mail
			Internet		Internet
3	direct debit	national direct debit schemes; SEPA scheme being developed (PE-ACH)	POS		
			Internet		
4	payment cards (credit/debit)		POS		POS
			mail		mail
			telephone		telephone
			Internet		Internet
5	money remittance/transfer	money remittance/transfer without opening of any payment account for the customer	POS (physically send)	money remittance/transfer without opening of any payment account for the customer	POS (physically send)
			Internet		Internet
			telephone & card		
6	e-money and other pre-funded/stored value instruments	general purpose server-based schemes; national e-money schemes, including some pre-paid telephone companies national schemes that operate under an e-money license waiver; general purpose stored-value; general purpose pre-paid wallet (e-purse); limited purpose pre-paid cards (e.g. mass transport, telephone cards)	POS (e-purses)	open-loop stored-value cards; closed-loop stored-value cards; pre-paid wallet; proprietary balance transter agent	POS
			telephone (SMS)		telephone
			Internet		Internet
7	other payment instruments	Post office money transfer systems (in some jurisdictions, Post office is a bank or has another licence allowing it to hold saving accounts used also for payments.); other bank-based (post-billed) payment services provided by non-bank entities	POS	instant credit	telephone
			telephone		Internet

Table 3: Detailed Payment Activities

Primary Activity		Subactivity	
Pre-Transaction			
1	Customer acquisition	a	Registration and enrollment of customers as payers (consumers)
		b	Registration and enrollment for merchant accounts
2	Services for issuer's front-end customer (payer) acquisition	a	Provision of credit evaluation/credit risk assessment tools
		b	Application processing services
3	Provision of payment instruments/devices to the front-end customer (payee or payer)	a	Card issuance, card production; card personalization; card delivery; card activation
		b	Hardware and software production (e.g. card reader) for usage with a consumer's online device (PC, mobile, handheld)
		c	Provision of e-money wallet / access code to e-money values
		d	Cheque manufacturing
4	Provision of hardware to accept payment instruments/devices	a	Provision of ATM terminals (sell/lease; manage)
		b	Provision of POS terminals
		c	Provision of cheque readers/cheque POS terminals
5	Provision of software to accept payment instruments/devices	a	Web hosting services
		b	Provision of shopping cart software
		c	Provision of software to connect payment gateway service providers
		d	Provision of cheque verification software
6	Provision of internet security-related technology/support	a	Certificate-authority services (e.g. PKI-based secure environments); provision of digital identity services for consumer authentication
		b	Provision of online transaction security systems to front-end customers (payees, merchants...), and back-end customers (e.g. 3D-secured card transactions via internet)
		c	Provision of e-signatures and other e-authorisations for payment authorisation purposes
7	Payment Card Industry (PCI) compliance services to merchants and/or payers	a	
8	Provision of data center services to back-end customers	a	Outsourcing complete data center functions/secured, supervised floor space/multi-site backup storage for disaster recovery
9	e-invoicing	a	Creation and delivery of electronic invoices to front-end customers (payor)
During-Transaction Stage 1			
10	Communication connection for merchants	a	Provision of gateway to acquirer/payment processors; a front-end service
		b	Provision of gateway to various networks/check or ACH authorization vendors; a front-end service
11	Transaction authorization (fund verification)	a	Provision of network switch services; a back-end service
		b	Provision of communication connection between networks and payment instrument issuers; a back-end service
		c	Provision of decision management/fraud screening/neutral network scoring system to card issuers for authorization; a back-end service
		d	Process to verify and confirm if payer has sufficient funds (or credit lines) available to cover the transaction amount; a back-end service
12	Fraud and risk management services to front-end customers (payees)	a	Verification services (address, IP address, card verification number, other data), Payment instrument authentication and authorisation services
		b	Identity authentication
		c	Decision management/fraud screening/neutral network scoring system (hosted at third-party service providers)
13	Fraud and risk management services to card issuers	a	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 (during transaction)	a	Debiting the front-end customer's (payer's) account / e-money purse; a back-end service
15	Ex-ante Compliance services	a	Anti-money laundering and terrorist financing regulation e,g, controls to identify suspicious transactions (database, software etc.)
During-Transaction Stage 2			
16	Preparation	a	Sorting merchant's sales information by payment instrument/network for clearing
		b	Submission of sales information to each payment instrument network
		c	Calculation of each network member's (either financial institution or processor) net position and transmission of net position information to each member
		d	Provision of transformation services into other payment instrument formats (e.g. MICR to ACH)
		e	Provision of sorting transactions by destination groups to Fis
17	Clearing	a	Transmission of clearing orders (CT, DD, cards, cheques) to a FI
		b	Transmission of clearing orders to ACH operator
		c	Distribution of advices showing the amounts and settlement dates
		d	Clearing (different from an ACH,.)
18	Settlement	a	Posting credit and debit at each financial institution's central bank account
		b	Posting credit and debit at each financial institution's commercial bank account
		c	Posting debit (credit in case of a return) to front-end payer account
		d	Posting credit (debit in case of a return) to merchant (payee) account
		e	Check settlement
Post-Transaction			
19	Statement	a	Provide statement preparation/delivery services for front-end customers (payers) (e.g. mobile credit advice; online bank/card account statements)
		b	Provision of statement/payment receipt notification services for merchants (payees)
20	Reconciliation, incl. collection and receivable management services	a	Matching invoices and payments
21	Retrieval	a	Provision of chargeback and dispute processing services
22	Reporting and data analysis services	a	to merchants, e.g. support services for treasury and accounting
		b	to consumers
		c	to FIs
23	Ex post Compliance services	a	Compliance with anti-money laundering and terrorist financing regulation, e.g. reporting to authorities, back-feeding to ex-ante databases

Table 4: Nonbank Importance: High European Countries
Austria

Payment Activity		e-Cheques	Credit Transfers	Direct Debits	Payment Cards	Money Remittance/Transfer	e-Money (Pre-funded/Stored Value Instruments)	Other Instruments
Pre-Transaction								
1	a							
	b							
2	a							
	b							
3	a							
	b							
	c							
	d							
4	a							
	b							
	c							
5	a							
	b							
	c							
	d							
6	a							
	b							
	c							
7	a							
8	a							
9	a							
During-Transaction - Stage 1								
10	a							
	b							
11	a							
	b							
	c							
	d							
12	a							
	b							
	c							
13	a							
14	a							
15	a							
During-Transaction - Stage 2								
16	a							
	b							
	c							
	d							
	e							
17	a							
	b							
	c							
	d							
18	a							
	b							
	c							
	d							
	e							
Post-Transaction								
19	a							
	b							
20	a							
21	a							
22	a							
	b							
	c							
23	a							

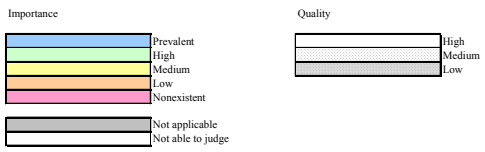


Table 4: Nonbank Importance: High European Countries
Germany

Payment Activity		e-Cheques	Credit Transfers	Direct Debits	Payment Cards	Money Remittance/Transfer	e-Money (Pre-funded/Stored Value Instruments)	Other Instruments
Pre-Transaction								
1	a							
	b							
2	a							
	b							
3	a							
	b							
	c							
	d							
4	a							
	b							
	c							
5	a							
	b							
	c							
	d							
6	a							
	b							
	c							
7	a							
8	a							
9	a							
During-Transaction - Stage 1								
10	a							
	b							
11	a							
	b							
	c							
	d							
12	a							
	b							
	c							
13	a							
14	a							
15	a							
During-Transaction - Stage 2								
16	a							
	b							
	c							
	d							
	e							
17	a							
	b							
	c							
	d							
18	a							
	b							
	c							
	d							
	e							
Post-Transaction								
19	a							
	b							
20	a							
21	a							
22	a							
	b							
	c							
23	a							

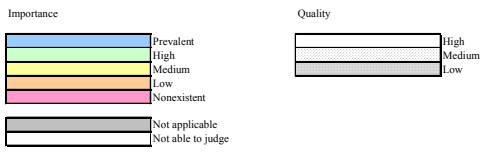


Table 4: Nonbank Importance: High European Countries
Italy

Payment Activity		e-Cheques	Credit Transfers	Direct Debits	Payment Cards	Money Remittance/Transfer	e-Money (Pre-funded/Stored Value Instruments)	Other Instruments
Pre-Transaction								
1	a							
	b							
2	a							
	b							
3	a							
	b							
	c							
	d							
4	a							
	b							
	c							
5	a							
	b							
	c							
	d							
6	a							
	b							
	c							
7	a							
8	a							
9	a							
During-Transaction - Stage 1								
10	a							
	b							
11	a							
	b							
	c							
	d							
12	a							
	b							
	c							
13	a							
14	a							
15	a							
During-Transaction - Stage 2								
16	a							
	b							
	c							
	d							
	e							
17	a							
	b							
	c							
	d							
18	a							
	b							
	c							
	d							
	e							
Post-Transaction								
19	a							
	b							
20	a							
21	a							
22	a							
	b							
	c							
23	a							

Importance

- Prevalent
- High
- Medium
- Low
- Nonexistent
- Not applicable
- Not able to judge

Quality

- High
- Medium
- Low

Table 5: Nonbank Importance: Low European Countries
Finland

Payment Activity		e-Cheques	Credit Transfers	Direct Debits	Payment Cards	Money Remittance/Transfer	e-Money (Pre-funded/Stored Value Instruments)	Other Instruments
Pre-Transaction								
1	a							
	b							
2	a							
	b							
3	a							
	b							
	c							
	d							
4	a							
	b							
	c							
5	a							
	b							
	c							
	d							
6	a							
	b							
	c							
7	a							
8	a							
9	a							
During-Transaction - Stage 1								
10	a							
	b							
11	a							
	b							
	c							
	d							
12	a							
	b							
	c							
13	a							
14	a							
15	a							
During-Transaction - Stage 2								
16	a							
	b							
	c							
	d							
	e							
17	a							
	b							
	c							
	d							
18	a							
	b							
	c							
	d							
	e							
Post-Transaction								
19	a							
	b							
20	a							
21	a							
22	a							
	b							
	c							
23	a							

Importance

- Prevalent
- High
- Medium
- Low
- Nonexistent
- Not applicable
- Not able to judge

Quality

- High
- Medium
- Low

Table 5: Nonbank Importance: Low European Countries
France

Payment Activity		e-Cheques	Credit Transfers	Direct Debits	Payment Cards	Money Remittance/Transfer	e-Money (Pre-funded/Stored Value Instruments)	Other Instruments
Pre-Transaction								
1	a							
	b							
2	a							
	b							
3	a							
	b							
	c							
	d							
4	a							
	b							
	c							
5	a							
	b							
	c							
	d							
6	a							
	b							
	c							
7	a							
8	a							
9	a							
During-Transaction - Stage 1								
10	a							
	b							
11	a							
	b							
	c							
	d							
12	a							
	b							
	c							
13	a							
14	a							
15	a							
During-Transaction - Stage 2								
16	a							
	b							
	c							
	d							
	e							
17	a							
	b							
	c							
	d							
18	a							
	b							
	c							
	d							
	e							
Post-Transaction								
19	a							
	b							
20	a							
21	a							
22	a							
	b							
	c							
23	a							

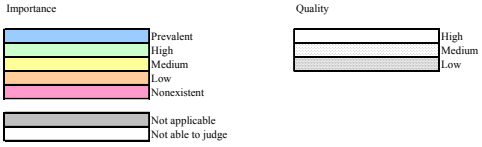


Table 5: Nonbank Importance: Low European Countries
Latvia

Payment Activity		e-Cheques	Credit Transfers	Direct Debits	Payment Cards	Money Remittance/Transfer	e-Money (Pre-funded/Stored Value Instruments)	Other Instruments
Pre-Transaction								
1	a							
	b							
2	a							
	b							
3	a							
	b							
	c							
	d							
4	a							
	b							
	c							
5	a							
	b							
	c							
	d							
6	a							
	b							
	c							
7	a							
8	a							
9	a							
During-Transaction - Stage 1								
10	a							
	b							
11	a							
	b							
	c							
	d							
12	a							
	b							
	c							
13	a							
14	a							
15	a							
During-Transaction - Stage 2								
16	a							
	b							
	c							
	d							
	e							
17	a							
	b							
	c							
	d							
18	a							
	b							
	c							
	d							
	e							
Post-Transaction								
19	a							
	b							
20	a							
21	a							
22	a							
	b							
	c							
23	a							

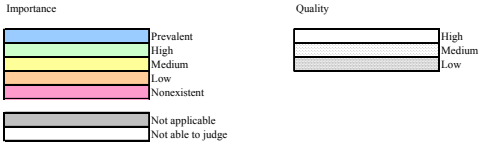


Table 5: Nonbank Importance: Low European Countries
Slovenia

Payment Activity		e-Cheques	Credit Transfers	Direct Debits	Payment Cards	Money Remittance/Transfer	e-Money (Pre-funded/Stored Value Instruments)	Other Instruments
Pre-Transaction								
1	a							
	b							
2	a							
	b							
3	a							
	b							
	c							
	d							
4	a							
	b							
	c							
5	a							
	b							
	c							
	d							
6	a							
	b							
	c							
7	a							
8	a							
9	a							
During-Transaction - Stage 1								
10	a							
	b							
11	a							
	b							
	c							
	d							
12	a							
	b							
	c							
13	a							
14	a							
15	a							
During-Transaction - Stage 2								
16	a							
	b							
	c							
	d							
	e							
17	a							
	b							
	c							
	d							
18	a							
	b							
	c							
	d							
	e							
Post-Transaction								
19	a							
	b							
20	a							
21	a							
22	a							
	b							
	c							
23	a							

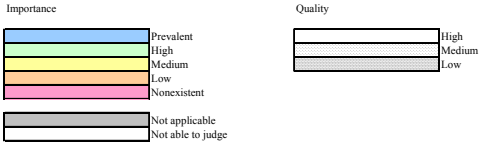


Table 6: Nonbank Importance: Medium European Countries
Bulgaria

Payment Activity		e-Cheques	Credit Transfers	Direct Debits	Payment Cards	Money Remittance/Transfer	e-Money (Pre-funded/Stored Value Instruments)	Other Instruments
Pre-Transaction								
1	a							
	b							
2	a							
	b							
3	a							
	b							
	c							
	d							
4	a							
	b							
	c							
5	a							
	b							
	c							
	d							
6	a							
	b							
	c							
7	a							
8	a							
9	a							
During-Transaction - Stage 1								
10	a							
	b							
11	a							
	b							
	c							
	d							
12	a							
	b							
	c							
13	a							
14	a							
15	a							
During-Transaction - Stage 2								
16	a							
	b							
	c							
	d							
	e							
17	a							
	b							
	c							
	d							
18	a							
	b							
	c							
	d							
	e							
Post-Transaction								
19	a							
	b							
20	a							
21	a							
22	a							
	b							
	c							
23	a							

Importance

- Prevalent
- High
- Medium
- Low
- Nonexistent
- Not applicable
- Not able to judge

Quality

- High
- Medium
- Low

Table 6: Nonbank Importance: Medium European Countries
Cyprus

Payment Activity		e-Cheques	Credit Transfers	Direct Debits	Payment Cards	Money Remittance/Transfer	e-Money (Pre-funded/Stored Value Instruments)	Other Instruments
Pre-Transaction								
1	a							
	b							
2	a							
	b							
3	a							
	b							
	c							
	d							
4	a							
	b							
	c							
5	a							
	b							
	c							
	d							
6	a							
	b							
	c							
7	a							
8	a							
9	a							
During-Transaction - Stage 1								
10	a							
	b							
11	a							
	b							
	c							
	d							
12	a							
	b							
	c							
13	a							
14	a							
15	a							
During-Transaction - Stage 2								
16	a							
	b							
	c							
	d							
	e							
17	a							
	b							
	c							
	d							
18	a							
	b							
	c							
	d							
	e							
Post-Transaction								
19	a							
	b							
20	a							
21	a							
22	a							
	b							
	c							
23	a							

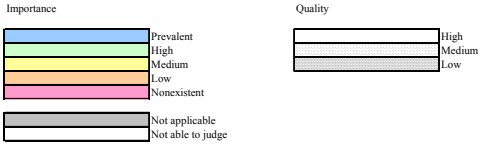


Table 6: Nonbank Importance: Medium European Countries
Czech Republic

Payment Activity		e-Cheques	Credit Transfers	Direct Debits	Payment Cards	Money Remittance/Transfer	e-Money (Pre-funded/Stored Value Instruments)	Other Instruments
Pre-Transaction								
1	a							
	b							
2	a							
	b							
3	a							
	b							
	c							
	d							
4	a							
	b							
	c							
5	a							
	b							
	c							
	d							
6	a							
	b							
	c							
7	a							
8	a							
9	a							
During-Transaction - Stage 1								
10	a							
	b							
11	a							
	b							
	c							
	d							
12	a							
	b							
	c							
13	a							
14	a							
15	a							
During-Transaction - Stage 2								
16	a							
	b							
	c							
	d							
	e							
17	a							
	b							
	c							
	d							
18	a							
	b							
	c							
	d							
	e							
Post-Transaction								
19	a							
	b							
20	a							
21	a							
22	a							
	b							
	c							
23	a							

Importance

- Prevalent
- High
- Medium
- Low
- Nonexistent
- Not applicable
- Not able to judge

Quality

- High
- Medium
- Low

Table 6: Nonbank Importance: Medium European Countries
Greece

Payment Activity		e-Cheques	Credit Transfers	Direct Debits	Payment Cards	Money Remittance/Transfer	e-Money (Pre-funded/Stored Value Instruments)	Other Instruments
Pre-Transaction								
1	a							
	b							
2	a							
	b							
3	a							
	b							
	c							
	d							
4	a							
	b							
	c							
5	a							
	b							
	c							
	d							
6	a							
	b							
	c							
7	a							
8	a							
9	a							
During-Transaction - Stage 1								
10	a							
	b							
11	a							
	b							
	c							
	d							
12	a							
	b							
	c							
13	a							
14	a							
15	a							
During-Transaction - Stage 2								
16	a							
	b							
	c							
	d							
	e							
17	a							
	b							
	c							
	d							
18	a							
	b							
	c							
	d							
	e							
Post-Transaction								
19	a							
	b							
20	a							
21	a							
22	a							
	b							
	c							
23	a							

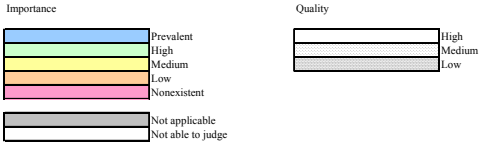


Table 6: Nonbank Importance: Medium European Countries
Lithuania

Payment Activity		e-Cheques	Credit Transfers	Direct Debits	Payment Cards	Money Remittance/Transfer	e-Money (Pre-funded/Stored Value Instruments)	Other Instruments
Pre-Transaction								
1	a							
	b							
2	a							
	b							
3	a							
	b							
	c							
	d							
4	a							
	b							
	c							
5	a							
	b							
	c							
	d							
6	a							
	b							
	c							
7	a							
8	a							
9	a							
During-Transaction - Stage 1								
10	a							
	b							
11	a							
	b							
	c							
	d							
12	a							
	b							
	c							
13	a							
14	a							
15	a							
During-Transaction - Stage 2								
16	a							
	b							
	c							
	d							
	e							
17	a							
	b							
	c							
	d							
18	a							
	b							
	c							
	d							
	e							
Post-Transaction								
19	a							
	b							
20	a							
21	a							
22	a							
	b							
	c							
23	a							

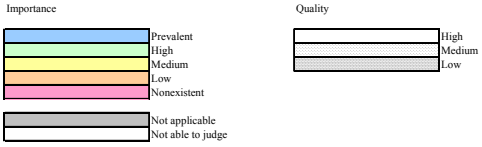


Table 6: Nonbank Importance: Medium European Countries
Portugal

Payment Activity		e-Cheques	Credit Transfers	Direct Debits	Payment Cards	Money Remittance/Transfer	e-Money (Pre-funded/Stored Value Instruments)	Other Instruments
Pre-Transaction								
1	a							
	b							
2	a							
	b							
3	a							
	b							
	c							
	d							
4	a							
	b							
	c							
5	a							
	b							
	c							
	d							
6	a							
	b							
	c							
7	a							
8	a							
9	a							
During-Transaction - Stage 1								
10	a							
	b							
11	a							
	b							
	c							
	d							
12	a							
	b							
	c							
13	a							
14	a							
15	a							
During-Transaction - Stage 2								
16	a							
	b							
	c							
	d							
	e							
17	a							
	b							
	c							
	d							
18	a							
	b							
	c							
	d							
	e							
Post-Transaction								
19	a							
	b							
20	a							
21	a							
22	a							
	b							
	c							
23	a							

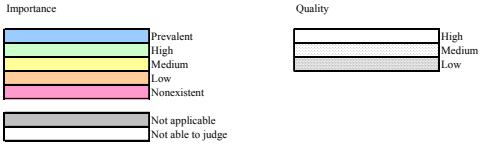


Table 7: EU Nonbank Companies

	Primary Activity		Subactivity	EU Nonbank Examples (in brackets the country of the NCB that mentioned the example)
Pre-Transaction				
1	Customer acquisition	a	Registration and enrollment of customers as payers (consumers)	American Express, Diners Club, Visa, First Data (GR), National processors , PayPal, Paybox, Click & Pay, various national e-money schemes
		b	Registration and enrollment for merchant accounts	Visa, Mastercard, Card Process (DE), ConCardis (DE), Datamax (BG) JCC Payment systems (CY), Deutsche Telekom (DE) Euronet(GR)
2	Services for issuer's front-end customer (payer) acquisition	a	Provision of credit evaluation/credit risk assessment tools	American Express, Diners Club, First Data (GR), SIA (IT), Centax (IT), Cetelem (BE, FR), Suomen Asiakastieto (FI), Cofinoga (FR), Cerved (IT)
		b	Application processing services	American Express, Mastercard, First Data (DE, FR, LV), ATOS (FR, DE), SBB (IT), Datamax (BG)
3	Provision of payment instruments/devices to the front-end customer (payee or payer)	a	Card issuance, card production; card personalization; card delivery; card activation	Oberthur, First Data, ACI Worldwide, ATOS, AustriaCard (LV), Borica (BG), Cetis (SI), Ghirlanda (IT), G&E(IT), Bankart (SI), Geva Business solutions (DE), Falk-4-Group (LV), SECETI, SSC (IT), Experian, Setec Oy/Gemalto(FI, LV)
		b	Hardware and software production (e.g. card reader) for usage with a consumer's online device (PC, mobile, handheld)	Oberthur, First Data, Diebold (IT), Wincor Nixdorf (IT), Datacard (FR), Datamax (BG),
		c	Provision of e-money wallet / access code to e-money values	PayPal, Paybox (AT, FR), SSB (IT), Visa (AT), Cidel (FR)
		d	Check manufactoring	
4	Provision of hardware to accept payment instruments/devices	a	Provision of ATM terminals (sell/lease; manage)	First Data (GR, LV, LT), NCR (BE, DE, FR), Borica (BG), Automatia (FI), Wincor Nixdorf (BE, SI, DE, GR)
		b	Provision of POS terminals	Thales (BE, FR), POSserviss (LV), Bankart (SI), JCC Payment systems (SY)
		c	Provision of cheque readers/cheque POS terminals	Hypoercom (LV), Ingenico (FR), Thales (FR)
5	Provision of software to accept payment instruments/devices	a	Web hosting services	1&1 Internet AG (DE), First Data (FR, GR), NCR (SI), SBB (IT), Paybox (AT), Experian (FR), Luttokunta (FI), SECETI (IT), Bankart (SI), ATOS (FR)
		b	Provision of shopping cart software	First Data (LV, LT), Hypercom (LV, SI), Itella (FI, LV), Wincor Nixdorf (LV, SI)Borica (BG), ACI Worldwide (SI), Diebold (SI, LV), Oberthur (SI), PayPal, Paybox, Click & Buy
		c	Provision of software to connect payment gateway service providers	PayBill (DE), PayPal, DA Sistemy Italy (SI), Experian (FR)), Equens (DE), First Data (SI), Wincor Nixdorf (SI, GR), EBPP (FR), SAP(DE), Borica (BG)
		d	Provision of cheque verification software	A2IA (FR)
6	Provision of internet security-related technology/support	a	Certificate-authority services (e.g. PKI-based secure environments); provision of digital identity services for consumer authentication	Some banks (IT), A-SIT Zentrum für sichere Informationstechnologie - Austria, Bankservice, Datamaz(BG), Deutsche Post (DE), Psta Slovenije (SI), Deutsche Telekom (DE), Visa (BE, LV,AT), Mastercard (BE, LV), Compass Plus (LV), First Data (LV, LT)
		b	Provision of online transaction security systems to front-end customers, and back-end customers	American Express, Visa, Diners Club, Experian (FR), First Data (LV) IBM (DE), SBB (IT), JCC payment systems (CY), Net Solving (IT), Bankart (SI), ATOS (FR) Itella (DE)
		c	Provision of e-signatures and other e-authorisations for payment authorisation purposes	Pošta Slovenije (SI), Duetshce Telekom (DE), D-Trust (DE), Bankservice (BG), Siemens (DE), Fiducia (DE), Sparkassen Informatik (DE)
7	Payment Card Industry (PCI) compliance services	a		Bankart (BG), B+S Card Services (DE), Cybertrust (IT, SI), Datamax (BG), First Data (LV), SECETI, SSB (IT), Euronet (GR), Ingenico (FR), Finanssidata (FI), Thales (BE),
8	Provision of data center services to back-end customers	a	Outsourcing complete data center functions/secured, supervised floor space/multi-site backup storage for disaster recovery	Actis Bsp Germany GmbH (DE) Itella (LV) ATOS (FR) Bankart (SI) BV Zahlungs-systeme GmbH (DE) CEDACRI (IT) Crosskey (FI) E-Shelter (DE) Fidenta (FI) Xenetic (FI) Meridea (FI) Nordic Processor (FI) Samlink (FI) Centurion Financne storitve d.o.o. (SI) Experian (FR) Euroinformation/EP3C (FR) EDPS (GR) First Data (FR, GR, LV) JCC PAYMENT SYSTEMS LTD (CY) IBM (DE, IT) Fiducia AG (DE) GAD (DE) SECETI (IT) SSB (IT) Sparkassen Informatik (DE) Euronet (GR)
9	e-invoicing	a	Creation and delivery of electronic invoices to front-end customers (payor)	Amazon (DE) Analyste, Opus-Capita (FI) Itella (LV) DocFlow (IT) E-Factura (IT) E-invoice (IT) Deutsche Telekom AG (DE) EBPP (FR) SSB (IT) SIA (IT)
During-Transaction Stage 1				
10	Communication connection for merchants	a	Provision of gateway to acquirer/payment processors; a front-end service	Borica (BG) ATOS (DE) Card Process (DE) First Data (DE, GR, LV, LT) NoteShot, Manison, Systek, Paravant (FI) EDPS (GR) Albacom (IT) CIM (IT) SECETI (IT) SSB (IT) Card Tech Ltd. (LV) CHD (LV) Modirum Oy (LV) Compass Plus Ltd (LV)
		b	Provision of gateway to various networks/check or ACH authorization vendors; a front-end service	JCC PAYMENT SYSTEMS LTD (CY) American Express (DE) B+S Card Services (DE) Euronet (GR) D8 (LV) Bankart (SI) Centurion Financne storitve d.o.o. (SI)
11	Transaction authorization (fund verification)	a	Provision of network switch services; a back-end service	Borica (BG) JCC PAYMENT SYSTEMS LTD (CY) American Express (DE)
		b	Provision of communication connection between networks and payment instrument issuers; a back-end service	B+S Card Services (DE) Card Process (DE) Visa (DE, GR, LV, LT) MasterCard (DE, GR, LV, LT) Luottokunta (FI) Handelsbanken Rahoitus (FI) ATOS (FR) Euroinformation/EP3C (FR) First Data (FR, DE, GR, LV, LT) EDPS (GR) Euronet (GR) CIM (IT) SECETI (IT) SSB (IT) SIA (IT) Bankart (SI)
		c	Provision of decision management/fraud screening/neutral network scoring system to card issuers for authorization; a back-end service	American Express (AT) Visa (AT) Diners Club (AT, GR) Borica (BG) Borica (BG) B+S Card Services (DE) EURO Kartensysteme GmbH (DE) Click&Buy Service Deutschland (DE) Equens (DE) MasterCard (DE) American Express (DE, FR) Luottokunta (FI) Diners Club (FR) Cetelem (FR) Cofinoga (FR) ATOS (FR) EDPS (GR) Euronet (GR) Albacom (IT) CIM (IT) Bankart (SI)
		d	Process to verify and confirm if payer has sufficient funds (or credit lines) available to cover the transaction amount; a back-end service	Borica (BG) BV Zahlungs-systeme GmbH (DE) Fiducia AG (DE) Luottokunta (FI) Diners Club (GR) Euronet (GR) American Express (IT) CEDACRI (IT) Centax (IT) Criff (IT) PayPal (Several countries) Bankart (SI)

Table 7: EU Nonbank Companies (cont.)

	Primary Activity		Subactivity	EU Nonbank Examples (in brackets the country of the NCB that mentioned the example)
During-Transaction Stage 1				
12	Fraud and risk management services to front-end customers (payees)	a	Verification services (address, IP address, card verification number, other data), Payment instrument authentication and authorisation services	Borica (BG) JCC PAYMENT SYSTEMS LTD (CY) American Express (DE) ATOS (DE) BV Zahlungs-systeme GmbH (DE) Click&Buy Service Deutschland (DE) Equens (DE) PayPal (Several countries) Fiducia AG (DE) GAD (DE) Visa (DE) MasterCard (DE) Sparkassen Informatik (DE) First Data (DE, GR, LT) Luottokunta (FI) Handelsbanken Rahoitus (FI) SECETI (IT) SSB (IT) Bankart (SI) Centurion Financne storitve d.o.o. (SI)
		b	Identity authentication	Sparkassen Informatik (DE) Diners Club (GR) Bankart (SI) Centurion Financne storitve d.o.o. (SI)
		c	Decision management/fraud screening/neutral network scoring system (hosted at third-party service providers)	JCC PAYMENT SYSTEMS LTD (CY) EURO Kartensysteme GmbH (DE) Sparkassen Informatik (DE) First Data (GR) Bankart (SI)
13	Fraud and risk management services to card issuers	a	Monitoring transactions and notifying cardholders of potential fraud, enabling them to take immediate action	Paybox (AT) Diners Club (AT, GR) Visa (AT, GR) Borica (BG) JCC PAYMENT SYSTEMS LTD (CY) BV Zahlungs-systeme GmbH (DE) Card Process (DE) Click&Buy Service Deutschland (DE) ConCardis (DE) Deutsche Telekom AG (DE) easycash (DE) Fiducia AG (DE) GAD (DE) Giropay GmbH (DE) Sparkassen Informatik (DE) ATOS (DE, FR, IT) First Data (DE, GR, LV, LT) Handelsbanken Rahoitus (FI) Luottokunta (FI) Experian (FR) Euronet (GR) MasterCard (GR) CEDACRI (IT) SECETI (IT) SIA (IT) SSB (IT) BITE Latvija (LV) Latvijas Mobilais telefons (LV) Telecom Baltija (LV) PayPal (Several countries) Bankart (SI) Centurion Financne storitve d.o.o. (SI) Diebold (SI) The Western Union Company (SI, BG)
14	Initiate the debiting of the front-end customer's (payer's) account (during transaction)	a	Debiting the front-end customer's (payer's) account / e-money purse; a back-end service	American Express (AT) Telecom Baltijam (LV) ATOS (DE, IT) Bankart (SI) Card Process(DE) CEDACRI (IT) Giropay GmbH (DE) BITE Latvija (LV) Latvijas Mobilais telefons (LV) Diners Club (AT, GR) Diners Club(GR) Centurion Financne storitve d.o.o.(SI) Click&Buy Service Deutschland (DE) Deutsche Telekom AG(DE) First Data(DE,GR, LV, LT) JCC PAYMENT SYSTEMS LTD (CY), SECETI(IT) Paybox (AT) PayPal (Several countries) , SSB (IT), Visa (AT) Euronet (GR)
15	Ex-ante Compliance services	a	Anti-money laundering and terrorist financing regulation e,g, controls to identify suspicious transactions (database, software etc.)	Actis Bsp Germany GmbH (DE),Bankart (SI) The Western Union Company (SI, BG) First Data (GR) Luottokunta(FI) Handelsbanken Rahoitus (FI)
During-Transaction Stage 2				
16	Preparation	a	Sorting merchant's sales information by payment instrument/network for clearing	JCC PAYMENT SYSTEMS LTD (CY) American Express (DE) ATOS (DE) Card Process (DE) Click&Buy Service Deutschland (DE) ConCardis (DE) easycash (DE) First Data (DE, GR, LT) Luottokunta (FI) Diners Club (GR) Visa (GR) MasterCard (GR) Euronet (GR) SECETI (IT) SSB (IT) SIA (IT) First PayPal (Several countries) Bankart (SI) Diebold (SI)
		b	Submission of sales information to each payment instrument network	ACI Worldwide (SI) ATOS (DE) Bankart (SI) Borica (BG) Card Process (DE) Diners Club (GR) Click&Buy Service Deutschland (DE) ConCardis (DE) easycash (DE) First Data (DE, LV) JCC PAYMENT SYSTEMS LTD (CY) NCR (SI, LV) Fiducia AG (DE) GAD (DE) SECETI (IT) SSB (IT) SIA (IT) Euronet (GR) Wincor Nixdorf (SI)
		c	Calculation of each network member's (either financial institution or processor) net position and transmission of net position information to each member	Itella (LV) ATOS (DE) Bankart (SI) Automatia (FI) Bankservice (BG) Borica (BG) Card Process (DE) Central Depository (BG) Diners Club (GR) Click&Buy Service Deutschland (DE) ConCardis (DE) DIAS (GR) easycash (DE) First Data (DE, LV) JCC PAYMENT SYSTEMS LTD (CY) SECETI (IT) SSB (IT) SIA (IT) Visa (DE) MasterCard (DE, SI)
		d	Provision of transformation services into other payment instrument formats	Bankart (SI) BV Zahlungs-systeme GmbH (DE) DIAS (GR) JCC PAYMENT SYSTEMS LTD (CY) SECETI (IT) SSB (IT) Sparkassen Informatik (DE)
		e	Provision of sorting transactions by destination groups to FIs; possibly posting credit/debit for internal ACH	Diners Club (GR)m Euronet (GR)
17	Clearing	a	Transmission of clearing orders to a FI	American Express (AT, DE) Itella (LV) ATOS (DE) Bankart (SI) Bankservice (BG) Borica (BG) Card Process (DE) SWIFT (GR) Central Depository (BG) Diners Club (AT, GR) Click&Buy Service Deutschland (DE) ConCardis (DE, SI) Equens (DE) DIAS (GR) easycash (DE) First Data (DE, GR, LV, LT) JCC PAYMENT SYSTEMS LTD (CY) NCB (LV) Luottokunta (FI) PayPal (Several countries) Visa (DE, SI, GR) MasterCard (DE, SI, GR) Sparkassen Informatik (DE) Euronet (GR)
		b	Transmission of clearing orders to ACH operator	American Express (AT, BE) Bankart (SI) BV Zahlungs-systeme GmbH (DE) Diners Club (AT) ConCardis (SI) easycash (DE) First Data (GR, LV) JCC PAYMENT SYSTEMS LTD (CY) Fiducia AG (DE) GAD (DE) SECETI (IT) SSB (IT) SIA (IT) Visa (DE, SI, AT, GR) MasterCard (DE, SI, GR) Sparkassen Informatik (DE) Euronet (GR)
		c	Distribution of advices showing the amounts and settlement dates	Visa (DE, SI, AT, GR) American Express (DE) Bankart (SI) Bankservice (BG) Borica (BG) BV Zahlungs-systeme GmbH (DE) Central Depository (BG) Diners Club (AT) ConCardis (SI) easycash (DE) First Data (LV) JCC PAYMENT SYSTEMS LTD (CY) NCB (LV) GAD (DE) SECETI (IT) SSB (IT) SIA (IT) Visa (DE, SI, AT, GR) MasterCard (DE, SI.GR) Euronet (GR)
		d	Clearing (different from an ACH)	Itella (LV) Bankservice (BG) The Western Union Company (BG) Equens (DE) easycash (DE)

Table 7: EU Nonbank Companies (cont.)

Primary Activity		Subactivity		EU Nonbank Examples (in brackets the country of the NCB that mentioned the example)
During-Transaction Stage 2				
18	Settlement	a	Posting credit and debit at each financial institution's central bank account	National Central Bank in IT, FI, CY and LV. Other companies in other countries (e.g. SI, BG)
		b	Posting credit and debit at each financial institution's commercial bank account	American Express (AT, DE) ATOS (DE) Bankart (SI) BV Zahlungs-systeme GmbH (DE) Card Process (DE) Diners Club (AT) Centurion Financne storitve d.o.o. (SI) Click&Buy Service Deutschland (DE) ConCardis (DE) easycash (DE) First Data (DE) Fiducia AG (DE) GAD (DE) PayPal (Several countries) Visa (DE, SI) MasterCard (DE, SI) Sparkassen Informatik (DE)
		c	Posting debit (credit in case of a return) to front-end payer account	American Express (DE) ATOS (DE) Bankart (SI) Bankservice (BG) Borica (BG) BV Zahlungs-systeme GmbH (DE) Card Process (DE) Centurion Financne storitve d.o.o. (SI) Click&Buy Service Deutschland (DE) ConCardis (DE) Diners Club (GR) easycash (DE) Euronet (GR) Fiducia AG (DE) First Data (DE, GR) GAD (DE) Handelsbanken Rahoitus (FI) IdeaPark (FI) Luottokunta (FI) MasterCard (DE, SI) Paybox (AT) PayPal (Several countries) Paysafecard (AT) Sparkassen Informatik (DE) Visa (DE, SI)
		d	Posting credit (debit in case of a return) to merchant (payee) account	American Express (AT, DE) ATOS (DE) Bankart (SI) Bankservice (BG) Borica (BG) BV Zahlungs-systeme GmbH (DE) Card Process (DE) Centurion Financne storitve d.o.o. (SI) Click&Buy Service Deutschland (DE) ConCardis (DE) Diners Club (AT, GR) easycash (DE) Euronet (GR) Fiducia AG (DE) First Data (DE) GAD (DE) Handelsbanken Rahoitus (FI) JCC PAYMENT SYSTEMS LTD (CY) Luottokunta (FI) MasterCard (DE, SI) Paybox (AT) PayPal (Several countries) Paysafecard (AT) Sparkassen Informatik (DE) Visa (DE, SI)
		e	Check settlement	American Express (DE) National Central Bank (IT)
Post-Transaction				
19	Statement	a	Provide statement preparation/delivery services for front-end customers (payers) (e.g. mobile credit advice; online bank/card account statements)	ACI Worldwide (SI) American Express (AT, DE) ATOS (DE) Bankart (SI) Borica (BG) BV Zahlungs-systeme GmbH (DE) Card Process (DE) Centurion Financne storitve d.o.o. (SI) Click&Buy Service Deutschland (DE) ConCardis (DE) Datamax (BG) Diners Club (GR) easycash (DE) Euronet (GR) Fiducia AG (DE) First Data (GR) GAD (DE) JCC PAYMENT SYSTEMS LTD (CY) MasterCard (DE) Paybox (AT) PayPal (Several countries) SECETI (IT) Sparkassen Informatik (DE) SSB (IT) Visa (AT, DE)
		b	Provision of statement/payment receipt notification services for merchants (payees)	Itella (LV) Bankart (SI) First Data (LT) Euronet (GR)
20	Reconciliation, incl. collection and receivable management services	a	Matching invoices and payments	Accenture (IT) American Express (AT) Itella (LV) ATOS (DE) Card Process (DE) Diners Club (AT) Centurion Financne storitve d.o.o. (SI) First Data (DE) JCC PAYMENT SYSTEMS LTD (CY) Visa (DE, AT) MasterCard (DE)
21	Retrieval	a	Provision of chargeback and dispute processing services	Agos (IT) American Express (AT) ATOS (DE, IT) Bankart (SI) Card Process (DE) Diners Club (AT, GR) Centurion Financne storitve d.o.o. (SI) First Data (DE, LT) JCC PAYMENT SYSTEMS LTD (CY) Luottokunta (FI) Handelsbanken Rahoitus (FI) Visa (DE, AT, GR) MasterCard (DE, GR, LV, LT) Euronet (GR)
22	Reporting and data analysis services	a	to merchants, e.g. support services for treasury and accounting	ATOS (DE) Bankart (SI) Card Process (DE) Diners Club (GR) Centurion Financne storitve d.o.o. (SI) Experian (IT) First Data (DE, LT) JCC PAYMENT SYSTEMS LTD (CY) MasterCard (DE) Euronet (GR)
		b	to consumers	Experian (IT) EBPP (FR) First Data (GR) Euronet (GR)
		c	to FIs	Bankservice (BG) Borica (BG) Central Depository (BG) Experian (IT) First Data (GR) MasterCard (GR) Euronet (GR)
23	Ex post Compliance services	a	Compliance with anti-money laundering and terrorist financing regulation, e.g. reporting to authorities, back-feeding to ex-ante databases	Bankart (SI) The Western Union Company (SI) Diners Club (GR) Centurion Financne storitve d.o.o. (SI) Visa (GR) MasterCard (GR) Euronet (GR)

The NCB is indicated in some cases, as a public institution

Table 8: Nonbank Importance: United States

Payment Activity		e-Cheques	Credit Transfers	Direct Debits			Payment Cards			Money Remittance/ Transfer	e-Money (Pre-funded/Stored Value Instruments)				Other Instruments
				Automatic	One-time	Tempo/ PayByTouch	4-party Credit/ Sig. Debit	PIN-Debit	3-party Credit		Prepaid Card Open-Loop	Prepaid Card Closed-Loop	PayCash	PayPal	(Bill Me Later)
Pre-Transaction															
1	a														
	b														
2	a														
	b														
3	a														
	b														
	c														
	d														
4	a														
	b														
	c														
5	a														
	b														
	c														
	d														
6	a														
	b														
	c														
7	a														
8	a														
9	a														
During-Transaction - Stage 1															
10	a														
	b														
11	a														
	b														
	c														
	d														
12	a														
	b														
	c														
13	a														
14	a														
15	a														
During-Transaction - Stage 2															
16	a														
	b														
	c														
	d														
	e														
17	a														
	b														
	c														
	d														
18	a														
	b														
	c														
	d														
	e														
Post-Transaction															
19	a														
	b														
20	a														
21	a														
22	a														
	b														
	c														
23	a														

Importance
- Prevalent
- High
- Medium
- Low
- Nonexistent

Data Quality
- High
- Medium
- Low

- Not applicable
- Not able to judge

Table 9: U.S. Nonbank Companies

	Primary Activity		Subactivity	Nonbank Examples
Pre-Transaction				
1	Customer acquisition	a	Registration and enrollment of customers as payers (consumers)	First Data, TSYS, Paymentech, PayCash, PayPal, BillMeLater, Tempo, PayByTouch
		b	Registration and enrollment for merchant accounts	First Data, Paymentech, PayCash, PayPal, BillMeLater, Tempo, PayByTouch
2	Services for issuer's front-end customer (payer) acquisition	a	Provision of credit evaluation/credit risk assessment tools	Fair Isaac, Experian, TransUnion, Equifax
		b	Application processing services	
3	Provision of payment instruments/devices to the front-end customer (payee or payer)	a	Card issuance, card production; card personalization; card delivery; card activation	Oberthur Card Systems, Datacard Group, Stored Value Systems
		b	Hardware and software production (e.g. card reader) for usage with a consumer's online device (PC, mobile, handheld)	
		c	Provision of e-money wallet / access code to e-money values	Q*Wallet, MyPoints, e-Rewards,Amex Blue, PayPal, PayCash, BillMeLater
		d	Cheque manufacturing	Deluxe,Checks in the Mail, Wal-Mart, Checks Unlimited
4	Provision of hardware to accept payment instruments/devices	a	Provision of ATM terminals (sell/lease; manage)	Diebold, NCR, Fujitsu
		b	Provision of POS terminals	Hypercom, Verifone, Lipman, First Data
		c	Provision of cheque readers/cheque POS terminals	Hypercom, Verifone, Lipman, First Data, IBM, Unisys
5	Provision of software to accept payment instruments/devices	a	Web hosting services	Digital Insights, Metavante[1]
		b	Provision of shopping cart software	MonsterCommerce, GoECart, GoldbarOne, Xcart
		c	Provision of software to connect payment gateway service providers	Google Checkout, PayPal, Authorize.Net, CyberSource
		d	Provision of cheque verification software	
6	Provision of internet security-related technology/support	a	Certificate-authority services (e.g. PKI-based secure environments); provision of digital identity services for consumer authentication	VeriSign, Identrust, Itrust Security, Cybertrust, Gemalto
		b	Provision of online transaction security systems to front-end customers and back-end customers	Savant Protection Inc., General Dynamics, Risk IDS
		c	Provision of e-signatures and other e-authorisations for payment authorisation purposes	AlphaTrust, Silanis, Identrust
7	Payment Card Industry (PCI) compliance services	a		Qualys, Ambiron TrustWave, Security Metrics, First Data, CyberSource
8	Provision of data center services to back-end customers	a	Outsourcing complete data center functions/secured, supervised floor space/multi-site backup storage for disaster recovery	IBM, Symantec, Cybercon, First Data
9	e-invoicing	a	Creation and delivery of electronic invoices to front-end customers (payor)	PaySimple, Billtrust, Metavante, Princeton eCom
During-Transaction Stage 1				
10	Communication connection for merchants	a	Provision of gateway to acquirer/payment processors; a front-end service	CyberSource, Authorize.Net
		b	Provision of gateway to various networks/check or ACH authorization vendors; a front-end service	CyberSource, First Data
11	Transaction authorization (fund verification)	a	Provision of network switch services; a back-end service	Paymentech[1], Authorize.Net, Visa[1], MasterCard, Star, NYCE, PULSE[1]
		b	Provision of communication connection between networks and payment instrument issuers; a back-end service	First Data, TSYS
		c	Provision of decision management/fraud screening/neutral network scoring system to card issuers for authorization; a back-end service	First Data, TSYS
		d	Process to verify and confirm if payer has sufficient funds (or credit lines) available to cover the transaction amount; a back-end service	First Data, TSYS, eFunds, TeleCheck
12	Fraud and risk management services to front-end customers (payees)	a	Verification services (address, IP address, card verification number, etc), Payment instrument authentication and authorisation services	Visa[1], MasterCard, Discover[1], Amex,CyberSource, VeriSign
		b	Identity authentication	DataXLtd., RemitPro, Experian, VerifyMe
		c	Decision management/fraud screening/neutral network scoring system (hosted at third-party service providers)	CyberSource, MasterCard
13	Fraud and risk management services to card issuers	a	Monitoring transactions and notifying cardholders of potential fraud, enabling them to take immediate action	First Data, TSYS
14	Initiate the debiting of the front-end customer's account (during transaction)	a	Debiting the front-end customer's (payer's) account / e-money purse; a back-end service	Metavante, Fiserv, Jack Henry
15	Ex-ante Compliance services	a	Anti-money laundering and terrorist financing regulation e,g, controls to identify suspicious transactions (database, software etc.)	Bridger Systems (ChoicePoint), Attus Technologies, Innovative Systems
During-Transaction Stage 2				
16	Preparation	a	Sorting merchant's sales information by payment instrument/network for clearing	First Data, Paymentech[1], CyberSource
		b	Submission of sales information to each payment instrument network	First Data, Paymentech[1], CyberSource
		c	Calculation of each network member's (either financial institution or processor) net position and transmission of net position information to each member	Visa[1], MasterCard, Star, NYCE, PULSE[1]
		d	Provision of transformation services into other payment instrument formats	TeleCheck, Electronic Payment Services, Solutran, Fiserv
		e	Provision of sorting transactions by destination groups to FIs	
17	Clearing	a	Transmission of clearing orders to a FI	First Data, Paymentech[1], Visa[1], MasterCard, Star, NYCE, PULSE[1]
		b	Transmission of clearing orders to ACH operator	ACH Outsourcers
		c	Distribution of advices showing the amounts and settlement dates	EPN
		d	Clearing (different from an ACH)	Merhcnat side: PayPal
18	Settlement	a	Posting credit and debit at each financial institution's central bank account	n/a
		b	Posting credit and debit at each financial institution's commercial bank account	n/a
		c	Posting debit (credit in case of a return) to front-end payer account	Metavante, Fiserv, Jack Henry, eFunds
		d	Posting credit (debit in case of a return) to merchant (payee) account	Metavante, Fiserv, Jack Henry, First Data, Fifth Third Processing[1]
Post-Transaction				
19	Statement	a	Provide statement preparation/delivery services for front-end customers (payers) (e.g. mobile credit advice; online bank/card account statements)	First Data, TSYS, Fiserv, Jack Henry, Metavante, eFunds
		b	Provision of statement/payment receipt notification services for merchants (payees)	Paymentech[1], CyberSource
20	Reconciliation, collection and receivable management services	a	Matching invoices and payments	First Data, Paymentech[1], CyberSource
21	Retrieval	a	Provision of chargeback and dispute processing services	First Data, Paymentech[1], CyberSource
22	Reporting and data analysis services	a	to merchants, e.g. support services for treasury and accounting	First Data, Paymentech[1], CyberSource
		b	to consumers	
		c	to FIs	Visa, MasterCard
23	Ex post Compliance services	a	Compliance with anti-money laundering and terrorist financing regulation, e.g. reporting to authorities, back-feeding to ex-ante databases	Bridger Systems (ChoicePoint), Attus Technologies, Innovative Systems

1. Denotes a nonbank entity that is a subsidiary/business unit of a bank.