Nonbanks and Risk in Retail Payments

By:

Stuart E. Weiner*, Terri Bradford*, Fumiko Hayashi*, Richard J. Sullivan*, Zhu Wang*, and Simonetta Rosati#

Paper for presentation at the Joint ECB-Bank of England Conference on Payment Systems and Financial Stability

Frankfurt, 12-13 November 2007

Abstract

This paper documents the importance of nonbanks in retail payments in the United States and in 15 European countries and analyses the implications of the importance and multiple roles played by nonbanks on retail payments risks. It shows that nonbanks play multiple roles along the whole payments processing chain of five main payment instruments (card payments, electronic cheques, credit transfers, direct debits and e-money and other pre-funded/stored value instruments). The importance of nonbanks is assessed as prominent in the United States across all the considered payment instruments, and high and growing in Europe where however differences among the different countries and payments classes persist. In Europe the importance of nonbanks is expected to grow in the future, driven by industry and regulatory developments. The paper argues that nonbanks' presence has shifted the locus of risks in retail payments towards a higher relevance of operational risk in its various forms (malfunctioning, data security and data protection), as well as higher relevance of fraud risk and system-wide impact of disruptions at key providers concentrating processing for important payment market segments. Banks have become increasingly dependent on nonbank service providers, and the adoption of new technologies in payments processing, particularly as regards communication networks, while on the one hand supporting mitigation of credit and liquidity risks connected to payments authorisation, increases the number of possible points along the processing chain that may be vulnerable to fraud and illicit use. The paper reviews the main regulatory safeguards in place, and concludes that there may be a need to reconsider some of them in view of the growing role of nonbanks and of the global reach of risks in the electronic era.

*Federal Reserve Bank of Kansas City. 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.
#European Central Bank. The views expressed in this paper are those of the author and do not necessarily reflect the views of the ECB or the Eurosystem.

Table of Contents

1. Introduction

Retail payment systems throughout the world continue to evolve in many ways. Chief among them is the continued migration from paper-based to electronic-based systems. Accompanying this electronification of payments has been an increase in the prevalence of nonbanks in the payments system.

In an earlier paper (ECB, FRBKC 2007), we took a first step in documenting and analyzing the role of nonbanks in European and U.S. retail payment systems. We found that nonbanks are most prominent in the United States but are prominent—and becoming ever more so—in many European countries as well. We also found that the regulatory framework surrounding nonbank payments participants is uneven both within and across countries.

This second finding is particularly important for central banks because central banks are almost uniformly charged with ensuring that payment systems are safe as well as efficient. At the core of "safety" considerations, of course, is the presence and mitigation of various types of risk. The earlier paper spent some time exploring risk issues, but at a fairly general level. The purpose of this paper is to delve more deeply into risk issues.

Specifically, this paper explores the various types of risk associated with the many activities along the payments chain, and asks, to what extent does the presence of nonbanks heighten or lessen these risks? As with the first paper, this paper draws on the results of a joint study undertaken by staff at the European Central Bank (ECB) and the Federal Reserve Bank of Kansas City. 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 following questions are addressed:

1. What payments activities and subactivities are performed along the payments chain?
2. What types of risk are associated with these activities and subactivities?
3. Do the risks associated with various payments activities and subactivities vary by type of payments instrument?
4. Does the increased presence of nonbanks in various payments activities heighten or lessen the degree of risk?
5. Are adequate safeguards—private and/or public—in place to ensure that risk levels are manageable and acceptable?

The paper is organized as follows. The next section assesses the importance of nonbanks in retail payments. It first summarizes the methodology used in this and the previous paper: the definition of "nonbank," the difference between front-end and back-end payment services, and the various categories of payment types and payment activities. It then documents the role played by nonbanks in the EU and the United States.

The third section of the paper takes up risk in retail payments. It first describes the various types of risk that may be present in a payments environment, for example, settlement risk, operational risk, reputational risk, and so forth. It then examines which types of risk are most likely to be associated with which types of activities along the payments processing chain. The fourth section of the paper "superimposes" this risk analysis on the prior section's documentation of nonbank presence by activity, permitting one to evaluate at a relatively detailed level nonbanks' potential impact on payments risk. Finally, the paper closes with a summary and suggestions for future research.

2. Nonbanks in retail payment systems

2.1 Methodology

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[1], 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 subsection provides a framework for documenting and analyzing these roles.

2.1.1 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.[2]

[1] In Europe, e-money is defined as "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 (Directive 2000/46/EC)." Thus, strictly speaking e-money is not a payment instrument but a means of payment, that is, a substitute for cash and deposits. E-money issuance is usually accompanied by the service or device needed to transfer it, and for simplicity in this survey with the term e-money we refer to the payment devise or instrument used to transfer e-money. E-money can be issued only by banks and by e-money licensed institutions (ELMIs), entities subject to a simplified prudential regime which is however modelled on that of banks, and are subject to certain limitations (for instance in terms of activities they can carry out, and investment of the funds).

[2] Examples of bank-controlled nonbank payment service providers include subsidiaries of banks, for example, TSYS, a large U.S. processor owned by Synovus Bank (although about to be spun off), 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.

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.

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

Table 1 (p. 41) shows the broad payment types that are used in this paper. Categories include electronic cheques; credit transfers; direct debits; payment (credit and debit) cards; and e-money and other prefunded or stored-value instruments, including Internet person-to-person (P2P) payments.[3] 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, 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.

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. 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;

[3] ECB, FRBKC (2007) includes two additional instrument categories: money remittance and transfer transactions; and other payment instruments. They are not considered in this paper because of insufficient data in some of the surveyed countries.

- *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 2 (p. 42).

2.2 Nonbank prevalence

2.2.1 Overview

A payment transaction can be initiated in several ways, and 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. 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 subsection documents in a systematic way the role played by nonbanks in the EU and U.S. retail payment systems. The analysis is conducted through the use of tables showing, for each of the various payment activities and each of the various payment types, the importance of nonbanks relative to banks.

In the case of Europe, five tables are presented, one for each of the major payment instruments, Payment Cards, Credit Transfers, Direct Debits, e-Cheques, and e-Money.

Within each of these tables, for each payment activity, the degree of nonbank prevalence is shown, moving, left to right, from surveyed countries accounting for the largest share of EU27 payments of that type to countries accounting for the smallest share of EU27 payments of that type. Thus, each table is a matrix, in which the rows are payment activities, the columns are countries, 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-country combination.

In the case of the United States, a single table is presented. Rows are again payment activities. Columns are now payment types, moving, left to right, from those payment types accounting for the largest share of noncash payments to those accounting for the smallest share of noncash payments. Thus, the table is again a matrix, in which 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. For both the United States and Europe, 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 an assessment of the quality of the data (high, medium, or low) on which the "prevalence" assessment is based.

2.2.2 EU nonbank prevalence

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 survey was voluntary, and not all the ESCB National Central Banks participated. The results presented include 15 countries, ten from the euro area (Austria, Belgium[4], Germany, Finland, France, Greece, Italy, the Netherlands, 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 67 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 (in particular the U. K., which alone counts for more than 20 percent of the number of payments processed in the EU), the focus of the analysis is mainly on the euro area: the above mentioned ten euro area countries in the survey together process about 92 percent of the total number of euro area payment transactions, and 66 percent of the total EU payment transactions.[5] All in all, these ten countries represent 65 percent of the EU GDP (88 percent of the euro area), and 54 percent of the EU population (86 percent of the euro area population).

The survey was carried out using a common methodology. Some respondents stressed that they faced data limitations that did not allow considering the results as a

4 For Belgium an assessment of on nonbanks importance was available only for cards and e-money payments.

5 The percentages provided are based on 2003 data and includes the countries that joined the EU in 2004 (i.e., the excluding Bulgaria and Romania who joined in 2007).

comprehensive and exhaustive description of the role of nonbanks in their respective countries. Thus, the survey 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. Moreover, the level of detail and the quality of the data varies from country to country, as respondents relied on different data sources and research methodologies, ranging from publicly available information to interviews with major banks and nonbanks. For some countries, the survey's findings provide more of an overview than a fully representative picture. These differences in comprehensiveness and quality of data gathered in the various countries make it difficult to carry out cross-country comparisons, and require care in considering the results. Nevertheless, in the absence more precise or homogeneous data, we accept these data limitations and believe that 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.

The results are reported, for each payment instrument (electronically processed cheques, credit transfers, direct debits, payment cards, e-money and other payment instruments), in Tables 3-7 (pp. 43-47). The results are presented following the order of importance of the various cashless payment instruments in terms of number of transactions processed in Europe: in 2003 (the most recent year for which cross-country comparable data are available) cards represented 31 percent of European payment transactions, followed by credit transfers (30 percent), direct debits (24 percent), cheques (13 percent), and e-money (1 percent). It should be noted that comprehensive statistics are not available for money transfers or for "other, innovative payment instruments" included in the survey sent to respondents. Furthermore, the data collected through the survey on nonbanks for these two instruments were extremely limited and do not allow making any but a preliminary assessment of the role of nonbanks.

Before moving into each table, it is importance to underline three preliminary observations:

First, information on the role of nonbanks is not equally available across countries and across payment instruments, as shown by the large white areas in many of the countries. 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,[6] traditions, historical development of the industry, or different stages of maturity in the payment services industry. For instance, cheques are not used in the Netherlands (where their use declined already in the '90s, and the Dutch banks stopped issuing cheques in July 2001), they 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,

[6] 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.

declining)[7]. Italy, Belgium, and Finland can be considered "credit transfers countries" (and in Bulgaria about 90 percent of payments are credit transfers) while direct debits have been introduced relatively recently in several countries and are becoming increasingly popular (in 2003 direct debits were about 24 percent of payments in EU, but in Austria, Germany and Spain they represented about 40 percent of the national volumes). 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.

Second, nonbank presence varies significantly by country. In general, when considering nonbanks importance across all payment instruments for each country, countries can be divided in three groups (ECB, FRBKC 2007). In a first group, including Austria, Germany, the Netherlands and Italy, 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, where nonbanks seem to play a more limited role. The last group includes the remaining countries: Bulgaria, Cyprus, Czech Republic, Greece, Lithuania and Portugal. Nonbank presence in these countries can be considered somewhere in between.

Third, in the majority of the 15 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. (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).

The tables show that the role of nonbanks is high in most surveyed countries for cards, with the exception of France (where there is a tradition of reserving the payments business to banks) and the Czech Republic, where it was assessed as medium for all payment instruments. However, in France, nonbanks play still an important role in the pre-transaction stage. For the other payment instruments, as mentioned earlier, respondents to the survey were able to provide relatively less data, as showed by the high number of grey and white cells. Where more information was available (as for credit

[7] 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.

transfers and direct debits) nonbanks seem to play a relatively more important role in those countries that represent a higher share of the EU traffic in that instrument and the payment instrument concerned represents a high share of the national payments (for example, for credit transfers: Germany, Austria, Italy, the Netherlands), again, with the exception of France.

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.

In a very few countries (Netherlands, Bulgaria), however, nonbanks may play a role in the settlement stage. However, a closer look at the entities involved shows that they are jointly owned by the banking sector, and thus can be considered in the banking domain (e.g. the companies Equens in the Netherlands, Borica (Bank Organisation for payments initiated by cards) and Bankservise in Bulgaria). A remarkable exception is Belgium, where nonbanks's importance in settlement activities 18a and 18b (posting credit and debit of financial institution's central bank and commercial bank account) is assessed as "prevalent". This is related to the role played by the cards national processor, the previously bank-owned Banksys. The company is now integrated into the Atos Origin group, an international IT group. Thus, this is an example of shift from the banking sector to a nonbank (and nonbank-owned company) of activities at the heart of the settlement cycle.

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 than payment instruments alternative to those offered by banks.[8] 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, which until recently, when it requested a banking licence in Luembroug, had operated as an ELMI).[9]

8 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".

9 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

In summary, based on the limited data available, it can be concluded that nonbanks play an important role in several European countries, and we expect their role to grow further, particularly at the back-end, in those countries where their role is still somewhat more limited. Drivers will be: first, the growth of cashless payments; second, SEPA, and the resulting restructuring and consolidation ongoing within the payments processing outsourcing industry; third, the maturing of payments markets segments and substitution among payment classes favouring instruments whose growth is largely supported by nonbanks (cards and direct debits); and fourth, at the front-end, following the regulatory opening up of the market to a new category of nonbank payment services providers, the "payment institutions".

From a *back-end* perspective, it should be noted that 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.[10] This market now seems to be undergoing a very dynamic phase in Europe, driven by the recent development of SEPA, the project to create a single European payment area by removing all legal, technical and commercial barriers within the European industry and making cashless payments in euro as easy, efficient and safe as it is today within one country.[11] Mazzi (2007) reports that according to figures and estimates available for the market share of third party processors in the cards issuing market (EU 15 countries), for instance, in the four-year-period between 2002 and 2006, the number of debit cards increased from 293 million to 342 million, and that of credit cards from 278 million to362 million. Issuing processing carried out by banks in-house decreased from 42 percent to 33 percent for debit cards, and from 60 percent to 51 percent for credit cards while the market shares of third party processors increased from 3 percent to 7 percent for debit cards, and from 21 to 28 percent for credit cards (the rest was processed through shared bank-owned utilities).

Furthermore, a consolidation process has started with the objective to achieve a sufficient scale to allow repositioning of national players as European players serving the common euro payment area. The process has recently accelerated and has taken various forms, through a wave of alliances, joint ventures, but also mergers and acquisitions, involving companies active at the same stage of the processing chain (horizontal integration) and at different stages of the chain (vertical integration).[12] For instance, in September 2006 the Dutch ACH Interpay and the German payments processors Transaktioninstitut agreed to merge to form Equens, a company aiming at serving the European market. Similarly, the international cards payments processor SiNSYS was

---

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).

[10] For example, SBB in Italy or Banksys and BCC in Belgium (the Belgian companies, previously owned by a consortium of Belgian banks, are now owned by Atos Origin, and international IT group.)

[11] SEPA is an industry-led project supported by the European Commission and by the ECB. Detailed information can be found on the websites of the ECB (www.ecb.europa.eu) and of the European Payment council (www.europeanpaymentscouncil.eu), the decision-making and co-ordination body of the Euroepan banking industry in relation to payments).

[12] Cordone (2004) and Moeller (2006) provide different examples of such cooperative ventures. See also Mazzi (2007) for a general picture about the status of the industry consolidation.

created by three national processors (from Italy, the Netherlands and Belgium), and is now owned by SIA-SSB (an Italian firm providing technology for cards payments, financial markets, payment systems and networks) and Atos (a France-based multinational IT services group providing end-to-end technological payment services). At the beginning of 2007, the Atos group acquired the Belgian companies Banksys (in charge authorization, security and guarantee of electronic payments in the country) and BCC (which affiliates merchants and manages the payment systems linked to Visa and MasterCard on behalf of nearly forty Belgian banks).

The geographical scope of the SEPA project is wider than the euro-area countries and includes also all other Member States of the European Union, together with Iceland, Liechtenstein, Norway and Switzerland (the latter four subject to their adoption of a consistent legal framework). It is no surprise, therefore, that the consolidation developments mentioned above have started to involve also these countries: for instance, in March 2007, the Danish cards processor PBS and the Norwegian banking service provider BBS agreed to merge their card transaction processing activities into the new company Northern European Transaction Services (NETS), with the aim to service Nordic and European banks.

An example of a global firm expanding in Europe by means of acquisitions is First Data.[13] The group, which has operations in 38 countries worldwide including 13 European countries, has acquired several national players in various European countries, e.g. in Poland (POLCARD, a leading independent merchant acquirer and card processor), in Germany (Gesellschaft für Zahlungssysteme mbH, a leading processor of cashless, card-based payment transactions, and Telecash, the country's premier network services provider), in Austria (Austrian Payment Systems Services, the national processor), and in Greece (Delta Singular Outsourcing Services, a leading payments processor). The company has also acquired a leading card processor in Central and Eastern Europe (EuroProcessing International), and the card processing unit of an Italian bank.

Industry consolidation in Europe has taken place at cross-border level both horizontally (involving companies operating at the same stage in the processing chain) and vertically (involving companies operating at different stages, e.g. ACH and cards processor). An interesting trend observed in this industry transformation process is that in various cases leading companies that were bank-owned and processed sometimes a large share of their national transactions have moved outside the banking domain from a governance point of view, and belong now to specialised IT international or multinational firms. The process of consolidation in the payments outsourcing business is not completed and is expected to accelerate further.[14]

[13] First Data was a public company until September 2007, when its agreed acquisition by an affiliate of the private equity firm Kohlberg Kravis Roberts & Co. (KKR) was completed.

[14] See for instance the Atos Origin Half Year Report 2007 (p.12 "the payment services business process outsourcing (BPO) market is extremely diverse, containing a combination of suppliers with a back-ground in various industry-specific processes, as well technology specialists and IT services providers. The market is stating to mature and we expect consolidation amongst service providers to continue. Growth is being driven by regulatory changes (such as the Single European Payments Area), a proliferation of payment

At the front-end, the role of nonbanks is also expected to grow in the future, as one of the main innovations introduced by the recently adopted Payment Services Directive is the opening up of the market by allowing actors other than banks and e-money institutions to provide payment services, the "payment institutions", which are entitled to provide the payment services listed in annex to the Directive.

There are five categories of services which enable the transfer of funds handled by the users: cash withdrawals and deposit transactions, transactions from an account or a line of credit including card payments, credit transfers and direct debits, international money remittances, transactions using mobile phones or the Internet, and issuance of payment instruments and acquisition of data related to the subsequent transactions (Margerit, 2007). Contrary to E-money licensed institutions, the payment institutions will be allowed to carry out other business activities (for instance, they could be merchants or telephone companies), but authorities may require them to establish a separate entity for the payments services. The 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). One important innovation is that payment institutions will be allowed to set up "payment accounts" in the name of users, but the Directive introduces certain requirements aimed at safeguarding the funds received from users (the safeguarding measures introduced are described in more detail in section 4.1).

2.2.3 U.S. nonbank prevalence

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 (p. 48) 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. Payment types are listed in descending order, from those accounting for the highest share of noncash transactions in the United States (in terms of number of transactions) to those accounting for the lowest share of noncash transactions. Shares are based on 2004 data. In 2004, payment cards accounted for 45.9 percent of noncash transactions; direct debits accounted for 6.9 percent; credit transfers accounted for 6.0 percent, e-cheques[15] accounted for 4.4 percent, and the e-Money share was nearly negligible. Within some of these broader categories, in turn, are shown more specific payments instruments: three types of payment card transactions (four-party

styles (such as mobile payments), and security (such as chip and pin in the United Kingdom, and the use of holograms)").

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

credit and signature debit (e.g., MasterCard and Visa), PIN-debit, and three-party credit (e.g., American Express, Discover, and private-label); three types of direct debits (automatic, one-time, and those completed under, for example, the Tempo and PayByTouch schemes); and 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).

The most striking general observation about Table 8 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 applicable to that payment type, be it bank or nonbank, for example, transaction authorization activities for automatic debit 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.

3. Risks in retail payments processing

3.1 Risks in retail payments

During the payments process various types of risks may arise, affecting different parties at different stages, and to varying degrees. This subsection provides a brief review of various risk categories relevant to processing retail payments and to clearing and settlement procedures.

- *Liquidity and Credit Risks*

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

The risk that a counterparty will not settle an obligation for full value, either when due (liquidity risk) or at any time thereafter (credit risk).

- *Operational Risk*

Operational risk is defined as the risk that deficiencies in information systems, internal controls, human errors, or management failures will result in unexpected losses (internal and external events). Thus, one important component of operational risk is related to malfunctioning, which may be the result of unintentional circumstances or events (e.g. a computer breakdown or a processing slowdown, or organisational deficiencies) or intentional circumstances or events (e.g., attack or misuse of information or procedures). 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.

• *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*: the legal offence of making a false instrument in order that it may be accepted as genuine, thereby causing harm to others (forgery).

Operational risk is, in general, relevant along the entire processing chain in the form of malfunctions. Other types of operational risk may be specific to a certain activity or a certain payment instrument. For example, fraud risk is most relevant for those steps of the processing chain involving authentication or identification with the related data being transmitted over telecommunication networks. For payment instruments that involve the use of specific hardware (e.g. card readers), fraud risk is relevant if the hardware can be compromised or altered for illicit purposes (e.g. skimming or cloning of cards). Data security risk is relevant for all activities involving the storage and transit of payment sensitive data (data that may be used for identity theft or for illicit authentication or authorisation of payment transactions). Data security risk may result in fraud risk if exposed records are then used for illicit purposes.

Traditionally, counterfeit risk applies to currency that is reproduced without authorization. Due to recent technological developments, some payment cards and tokens may store monetary value (e-money stored on a card/e-wallet). E-money that is reproduced or altered without authorization has characteristics that are comparable to counterfeit paper money. The term counterfeit is now also commonly applied to unauthorized manufacture of cheques, card payment instruments or other physical tokens used in monetary transactions.[17]

[17] A cheque that bears a false signature or has been altered is properly called forgery. For our purposes, we include forgery with counterfeit risk.

- *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. It comprises credit risks, and liquidity risks when they emerge in clearing and settlement systems. It also includes a specific form of credit risk, the risk of failure of the settlement agent, that is, the entity whose assets are used to settle the payment obligations (settlement agent credit risk). Settlement risk may also result from crystallisation of operational risk, as inadequate operational reliability, security and business continuity may affect the integrity of the data exchanged within the clearing and settlement process, and may result in financial losses for the involved or liable parties.

- *Legal Risk*

The risk of loss because of the unexpected application of a law or regulation or because a contract cannot be enforced. For instance, application of law or enforcement of legal rights may be complex or challenging in case of payment instruments used internationally or in case of innovative products whose nature is not initially clearly defined, as can happen when a new payment solution presents elements of different payment instruments. In general, legal risk in clearing and settlement arrangements may be a source of settlement risk if the unexpected application of a law affects the positions of participants in the clearing and settlement process (e.g. unwinding, or insolvency of the counterparty resulting in freezing of assets or revocation of transfers by the liquidator).

- *Reputational Risk*

The risk that the materialization of another risk category damages the confidence in a payment service provider. For example, it may result from the materialisation of operational or legal risk involving end-users and damaging the payment service provider brand or the payment instrument more generally in the case of a generalised disruption. The loss of reputation in a payment service 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.

- *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. The activities where this risk is most relevant are those related to security-related technology where market standards are in place (such as the Payment Card Industry (PCI) data security standard), and those where public regulations and laws aimed at combating the criminal use of the payment system (such as ex-ante anti-money laundering and terrorist financing controls and ex-post data archiving and reporting to authorities for the purpose of back-feeding to ex-ante databases and defining

suspect operations profiles). At times these standards may affect a payment participant indirectly, such as when bank payment acquirers are directly responsible for PCI standards but they hold firms to which they outsource payment processing responsible for the standards.[18] To the extent that payment schemes are subject to oversight by the central banks (as is the case in several European countries), compliance risk may arise if the rules and management of the payment scheme do not comply with the regulatory standards.

- *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. As far as retail payment systems are concerned, systemic risk does not usually represent a threat due to the limited value of payments settled. However, there are cases where some retail payment systems are considered to be systemically important as their malfunctioning may threaten the financial market (in the Euro area, when assessing the systemic importance of a retail payment system, the ECB and the NCBs take account of the market penetration within the respective retail payments market, the financial risks pertinent to the system, and the risk of domino effects).

- *System-wide Risk*

From the perspective of specific payment instruments, it is unlikely that the disruption of the functioning of a single payment scheme or the impossibility to settle a specific payment instrument may result in systemic risk. However, a system-wide impact is possible, that is, the failure to settle an entire class of transactions could under certain conditions disrupt, at least temporarily, the functioning of the real economy by severely altering the capacity of economic agents to discharge their obligations on account of the unavailability of and/or lack of confidence in the payment instrument concerned (and substitutable payment instruments). Of course, the severity of the impact will in practice be dependent on the market structure for payment services and, in particular, on the importance of the specific payment instrument and its substitutes (see for example ECB (2007) for the case of cards schemes).

3.2 Risks along the processing chain

As briefly described in the previous subsection, various types of risks may arise during the payment process, and 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 (for example, liquidity and credit

[18] Similarly, manufacturers of point-of-sale payment terminals and ATM manufacturers are not directly obligated by contractual relationships with payment networks, but must comply with network security standards if they hope to successfully market their products.

risk). All parties entering into contractual relations in the context of payments processing may be exposed to legal risk. Financial institutions that participate in clearing and 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 fulfil subsequent payment obligations, or incur legal risk if it is held liable to other parties.

In case of outsourcing of activities to third parties, they may become subject to legal risks (if the responsibilities of the parties are not sufficiently clear or legally sound), and operational risk (if the outsourcing party becomes dependent on an improperly managed third party). In the case of outsourcing to a third party that concentrates the activities for a whole payment market segment, system-wide risk may arise if the third party becomes suddenly impaired or unable to operate. For payment service providers whose outsourcing activities are subject to regulation (as in the case of banks), compliance risk may arise.

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. Although in general retail payments do not carry systemic risk, there are cases where retail payment systems have been considered systemically important.

In this section we look at the vulnerability of certain payment activities to specific categories of risk by using a matrix representation (see Table 9, pp. 49-50). Our aim is to identify the types of risk to which specific payment activities are exposed, but we do not attempt to indicate the magnitude of the risk exposure. In later sections we will discuss controls that are in place to mitigate these risks.

Before entering in the detailed analysis of the risks along the processing chain, we need to underline that certain risk categories by nature have a general relevance and are thus not represented as columns in the matrix. For instance, legal risk applies to payment transactions and to the payment process as a whole, and thus cannot be restricted to specific activities. Similarly, systemic risk may affect the funds transfer systems (where also retail payments may be settled) but it would be inappropriate to attach it to a specific activity in the process chain of an individual retail payment transaction. The likelihood and the severity of a system-wide impact would depend on the characteristics of the payment industry as a whole. Finally, reputational risk is a general category risk that applies to all activities as each of them, if unduly performed, has the potential to damage the reputation of the payment service provider or affect public confidence in the safety or efficiency of the involved payment instrument.

In the matrix we show liquidity risk, credit risk, and settlement agent credit risk. The matrix highlights with a yellow background where these risks materialize in the settlement process (settlement risk). Outside of the settlement process, credit and liquidity risk is borne by various parties involved in a payment scheme depending on the timing of the process, what party has custody of funds, and on the design of (and legal

and contractual provisions governing) the specific payment instrument involved. For instance, typically a merchant accepting a payment instrument in exchange for goods or services is exposed to credit risk unless the payment is settled with success in real time or at the same time of the delivery of the goods or services, or unless the payment instrument contractual framework provides for its mitigation or transfer to another party (for example, payments by cards may be assisted by a guarantee provided by the card issuer or by the card scheme). In card schemes, the card issuer is typically exposed to credit risk vis-à-vis cardholders of its cards. When a card transaction is properly authorised and accepted for execution by/within a card scheme, the card issuer takes the credit risk by guaranteeing payment to the merchant.

In the case where a retail payment is executed using a debit transfer order (for example, a direct debit) the payee's account may be credited in some cases before the actual debiting of the payer's account in the books of its bank. When this is the case, and if the payee's bank has advanced the funds to its customer before the successful final debiting of the payer's account, it may be exposed to liquidity risk or credit risk if the latter (payee) has already withdrawn the credited funds. In general, pre-paid payment instruments entail a credit risk for the holder of the instrument vis-à-vis the issuer (such as in case of pre-paid cards or e-wallets), while in case of post-paid payment instruments it is the payment service provider of the payee or the payee itself that is exposed to credit or liquidity risk. For example, this happens with post-billing payment services provided by certain mobile and telecommunication companies. This may also happen when a payment service is provided in real time to both payer and payee, but the top-up covering the specific payment is settled at a later stage (for example, a PayPal payment topped-up by direct debit on the payer's bank account).

As far as operational risk is concerned, we represent in Table 9 its general aspect (such as malfunctioning or human error) which is applicable to all activities, and operational risk in connection with data security and counterfeiting. Data security has recently attracted attention because numerous data breaches have allowed unauthorized access to sensitive data. Because the primary concern of data security is the potential for payments fraud as well as violation of responsibility to protect privacy of customers, the column notes these consequences in its label. Counterfeiting does not generally get the attention of data security, but statistics for the United States suggest that in terms of its cost, fraud through counterfeiting is far more costly than that from data breaches. Cheque fraud, for example, is estimated to cost at some 10 to 20 billion dollars per year in the United States, a sum that is larger than estimates of fraud in all other forms of retail payments.

In card schemes, the party suffering the loss deriving from materialisation of fraud risk is determined by the scheme's rules, and depends on a number of factors, including the physical environment in which the transaction was executed (POS or card-not-present), the time of the transaction in case the cardholder had informed the issuer that the card had been stolen or lost, and the security and risk mitigation techniques employed by the merchant and acquirer; as a rule, the loss is suffered by card holders only up to certain amount (but they may also be exempted) provided they have complied with notification requirements, by the card issuers if the transaction had been authorised and accepted, by the merchant if it had not complied with the security standards for POS

transactions, and by the acquirer in case of card-not-present fraud.

Although operational risk is relevant to the settlement process, it has a particular prominence for retail payments, and we find it useful to highlight those activities where the payments process may be particularly vulnerable to them.

The next-to-last column of Table 9 shows compliance risk. Payment participants can be required to comply with specific laws, regulations, and contractual arrangements. In the United States, payments are subject to legal requirements under the uniform commercial code and regulations such as the Federal Reserve's Regulation E. Members of payment networks (ATM, ACH, online debit, offline debit, and credit card) are contractually bound to comply with operating and security standards set by the network. One of the most significant recent efforts to improve data security in card payments is the payment card industry data security standard (PCI standard).[19] The standard was revised in January 2005 and the payments industry is in a transition phase to the new standard. Banks that are in the participating card network are responsible for complying with the standard as well as ensuring that its outsourcing partners and payment clients comply with the standard. Payment participants subject to compliance risk can face significant penalties if it is found that they do not properly follow guidelines set forth for data security and other operational requirements.

The last column of Table 9 is for risk associated with illicit use of payments. One of the traditional focuses of law enforcement efforts to curb illicit use of payments is money laundering. Payment participants, such as a bank, are sometimes required to monitor use of bank accounts and to report suspicious activities. More recently, policymakers have been concerned with the use of the payments system to fund terrorist activities, which is another form of illicit use of the payments system. A tool used to combat illicit use of the payments system is to carefully identify and screen new customers before granting access to the payments system. In the United States, banks are now required to use more reliable forms of identifying consumers when they open bank accounts. Banks are also obligated to carefully identify and screen merchants before accepting them as clients for payment services, and to monitor their ongoing use of payments. These efforts help to keep out those who desire to use the payments system for illicit purposes. Payment participants that fail to implement required guidelines to curb illicit use of payments face the risk of penalties if their failure to comply is discovered. In Europe not only banks but also other parties are required by the Third Anti Money Laundering Directive[20] to comply with obligations concerning customer due diligence, reporting of suspicious transactions, record keeping and statistical data, and take other supporting measures, such as ensuring a proper training of personnel and the establishment of appropriate internal preventive policies and procedures.

[19] The standards were developed as collaboration between American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International.

[20] Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing. is applicable to the financial sector as well as lawyers, notaries, accountants, real estate agents, casinos, trust and company service providers. Its scope also encompasses all providers of goods, when payments are made in cash in excess of €15.000.

In Table 9 we associate the various payment activities with liquidity, credit and settlement risks, with operational risk and its main sub-categories, and with compliance and illicit use risk. We believe there are three broad messages evident in the table. First, settlement risk is a prominent feature of retail payments. But, though it is present, analysts and policymakers generally believe that settlement risk in retail payments is well controlled.[21] Second, counterfeit risk is limited to a small number of payment activities. However, despite the limited impact on payment activities, counterfeit risk is one of the most significant problems in payments today, accounting for most of the losses due to payments fraud. Third, operational risk is one of the most prominent sources of risk in terms of the number of payment activities it affects. Most of the risk is in problems such as malfunctions and in data security. Associated with the prominence of operational risk is compliance risk, because imposition of rules and regulations on payment participants is a major containment tool used by regulators and payment networks to compel behaviour that properly manages operational risk.[22] The key to understanding the prominence of operational risk is the shift of payments towards electronic forms. The payment activities and subactivities listed in the table are dominated by processes that facilitate or depend upon electronic forms of messaging. These processes have emerged as we have adopted electronic payments. As a result the locus of retail payments risk has shifted towards operational risk.

In the light of the above results, do nonbanks raise special risk considerations? In the next section we look at this question in the light of the importance of nonbanks in payment activities as described in Section 2.2.

4. Impact of nonbanks on risk

4.1 Risks and nonbank presence in the EU

As seen in section 2.2.2, nonbanks are important in several European countries, and we expect their role to grow further, both at the front-end and at the back-end, particularly in those countries where their role is still somewhat more limited. Their role is most visible and seems more important in processing of payment instruments where the pre-transaction phase is highly automated, as in the case of cards.

4.1.1 Risks that can be generated at various points along the whole processing chain

The growth of payment instruments which are processed on-line and characterised by real-time authorisation brings along a business model where all the parties involved –and not only the banking sector – communicate with each-other and interact. This involves a more complex mechanism with a multiplicity of contact points and the dissemination of

[21] This serves as a reminder that the purpose of Table 9 is to help identify where risk occurs in the many activities that underlie payments, not their severity.

[22] This method of containing risk is retail payments is common, in part because methods such as pricing for risk or insurance have proven inadequate to bring the level of risk in retail payments to tolerable levels (see Braun et al , forthcoming 2007).

sensitive data at various points along the processing chain, and the consequent vulnerability to risks in terms of data security and data (privacy) protection as any interaction point can be, in itself, a weak point in the chain suitable to being exploited by a criminal to intrude the payment network for illicit purposes. Payments fraud implies a possible liability for banks even if the data compromise enabling the fraud may have taken place at level of a nonbank. In this sense, banks need to co-operate and co-ordinate with nonbanks to properly control risk throughout the processing chain.

The industry and regulators are making great efforts to combat payments fraud on several fronts, including regulatory (the implementation of the Payment Services Directive will, inter alia, facilitate the use of data for payments fraud prevention purposes), and in terms of co-operation between the public and private sector and among enforcement agencies. As regards the industry, the adoption by merchants of PCI compliant systems and processes for data security and the implementation of EMV standards are an important step towards mitigation of these risks. In Europe the migration to EMV is progressing (According to industry reports, 58.8 percent of the payment cards, 66.1 percent of the bank ATMs and 51.7 percent of the point of sale terminals have already been migrated to EMV in Europe. Work is progressing towards full migration in time for SEPA (2010). There are however significant country differences).[23] As far as PCI is concerned, it was recently reported that 57 percent of the surveyed large merchants were not compliant with at least one PCI standard (the percentage fell from 73 percent of last year[24]). In the European countries where cards market penetration is less advanced and still growing, as is the use of e-payment solutions which often rely on cards transfers for completion or top-up, these risks may not yet be particularly perceived. However, these countries may be better positioned in ensuring that these threats are properly minimised at an early stage of adoption, and well before maturity, because banks and nonbanks (merchants in particular) are not constrained by legacy-systems and may adopt directly state-of-the-art and PCI and EVM compliant technology. There are indications that fraud is a phenomenon of international and in Europe, of pan-European dimension, as organised crime operates from multiple locations and exploits to its benefit the global reach of the internet (Vulpiani, 2006 and Sarazin 2006). This raises an issue of international co-ordination among industry members, regulators and enforcement agencies.

The recently adopted Payment System Directive harmonises completely the regulation of liability related to fraud and execution of “unauthorised transactions”. Here the bank or nonbank nature of the payment service provider is not relevant as the provisions apply to all payments generally (before notifying the service provider or the loss or theft or fraudulent use of its payment instruments the consumer may have to bear a loss of up to 150 EUR, but Member States may reduce this cap when transposing the Directive into national legislation (Margerit, 2007)).

Other risks that are relevant in general and may generate from improper control throughout the whole processing chain are legal risk, reputational risk and, under certain circumstances, systemic risk. The Eurosystem has statutory competence in the field of

[23] Fraud Prevention Experts Group (2007b)

[24] Compliance-magazin.de (2007), accessed on 24.10.2007

oversight of payment systems, including both payment systems and payment instruments, and therefore may ensure monitoring and, if required, intervention (in various forms, regulatory, operational, through moral suasion and industry co-operation) aimed at preserving public trust in the safe and efficient functioning of payment systems in the euro area.

4.1.2 Risks related to settlement activities

Settlement activities remain largely a prerogative of the banking sector, and in the euro area clearing and settlement systems are subject to oversight by the Eurosystem. The fact that in some Europe countries nonbanks-processors may play a role also at the settlement stage may point to the importance of nonbanks in activities that are at the heart of interbank transfers, and thus a possible impact in terms of settlement risk. However, only in one case (Belgium), the nonbank company involved is today also nonbank owned. The change was mostly related to governance only, and the company was and continues to be subject to oversight by the National Central Bank. This ensures that its role and impact on the functioning of the payment systems are fully understood and catered for.

One issue that may be relevant from the point of view of settlement risks is the nature of assets used for discharging obligations among participants in 4-party card schemes. As mentioned in Section 2.2.2, in Europe there are different solutions in place as regards the settlement stage of cards-related interbank obligations. In some countries (as in France), national card transactions are settled in the ACH or other national retail payment system. In others, they may be settled by banks bilaterally (for example in Austria). Furthermore, as it relates to international cards transactions, the correspondent banking channel normally is used for settling interbank positions. When transactions are settled in commercial bank money, members of a cards scheme are exposed not only to credit risk vis-à-vis the other members that participate in the scheme's multilateral clearing, but also to the failure of the settlement agent. This risk is usually minimised by the scheme selecting large and high-standing banks as settlement agents. However, the risk cannot in principle be ruled out. Moreover, when large amounts are involved, or the payment instrument is a prominent one for a country or there are no easy substitutes, moral hazard issues may arise as the settlement agent bank may be considered "too-important-to fail." In Europe, the national central banks that carry out oversight of payment instruments usually oversee also the national card scheme and contribute to ensuring the safety and soundness of these payment and the systems involved. Furthermore, the National Bank of Belgium oversees MasterCard Europe.[25] In May 2007, the Eurosystem started a public consultation of a Draft Oversight Framework for Card Payments Schemes proposing requirements which, if observed, would contribute to the soundness of CPSs. The requirements emanate from a risk analysis conducted by the Eurosystem.[26]

[25] ECB (2007b), Blue Book 2007, Volume I, p. 78
[26] ECB (2007a).

4.1.3 Credit and liquidity risks outside the settlement stage

We have seen that credit and liquidity risks may be related to various steps in the processing chain and the party that is exposed to them depends on the contractual features of specific the payment instrument concerned. We related these risks to the activities involving the enrolment of customers and merchants and as far as the "during transactions" stages is concerned, the initiation of the crediting or debiting of the parties' accounts.

In the EU, payment services can be provided by credit institutions, by e-money licensed institutions and by other nonbank providers. 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 banks' settlement business line is explicitly considered in the framework of operational risk management and subject to coverage in the form of capital requirements[27].
- 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.
- As far as other nonbank front-end providers of payment services are concerned, payment services may currently be provided under very different conditions within the European Union, as shown in EC (2003)[28], 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). However, this is an area where a great innovation has been introduced by the recently adopted Payment Services Directive. The Directive has in fact opened up of the market by allowing actors other than banks and e-money institutions to provide payment services, the "payment institutions", which are entitled to provide the payment services listed in annex to the Directive. There are five categories of services which enable the transfer of funds handled by the users, knowing that the funds may be withdrawn by the users after the transactions have been executed: cash withdrawals and deposit transactions, transactions from an account or a line of credit including card payments, credit transfers and direct debits, international money remittances, transactions using mobile

[27] 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."

[28] 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.

phones or the internet, and issuance of payment instruments and acquisition of data related to the subsequent transactions (Margerit, 2007). The payment institutions will be subject to a simplified prudential framework compared to that applied to banks and e-money licensed institutions, with the aim to ensure their safe and prudent management and to protect users from risks arising from payments services provisions. For instance, use of customers 'funds would be subject to limits (they could be used only for payment transactions; the balance of an account should not be co-mingled with those of other user accounts, nor with the own funds of the payment service provider, although under certain circumstances the Member States or the national authorities may choose alternative solutions to funds segregation, for instance protecting them from claims of other creditors of the payment institutions in case of insolvency, or a financial guarantee). The Member States will have to designate the authorities in charge of licensing and supervising the payment institutions. These authorities could consult payment systems overseers (the central banks) when granting authorisation, without prejudice to the Eurosystem's oversight statutory powers.

4.1.4 Risks related to outsourcing to third parties

In the previous section we saw that the activities required for processing of retail payments present possible vulnerability to the traditional risks categories along the whole processing chain, not only at the settlement stage. Following the massive adoption of electronic communication and processing technology in payments processing, there was a shift of risk relevance towards operational risk in its various form. Does the role played by nonbanks in Europe impact on these risks trends? In those countries where nonbank processors and vendors are already prominent, they have often supported the industry growth and move towards straight-through-processing (STP), which substantially increases efficiency and reduces malfunctioning related to manual handling and human error, but increases dependency on automated systems reliability. Banks have traditionally been able to control very well these operational risks when dealing with payments processing in-house and through bank-owned processors. From this perspective, outsourcing to companies that are best equipped to grant high levels of security and business continuity can significantly contribute to maintain the operational soundness of the payments process while reducing its cost (in fact, specialised processors usually operate on a large scale and can benefit from significant economies). Through outsourcing technical and IT-intense processes, banks not only free up resources that they may devote to their core business, but ensure that these processes are handled by specialised companies which invest high resources in state-of-the-art technology and concentrate specialised knowledge and skills. The vulnerability to risks inherent to the payments processing chain does not depend on the bank or nonbank status of the processor, but on the way risks are controlled. The relevant regulation depends on the institutional status of the outsourcing company:

- Banks are subject to strict regulation which ensures they control risks and remain responsible for their management and containment vis-à-vis banking regulators also when outsourcing processes to third parties. 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.

- 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).
- Regulatory safeguards regarding outsourcing by other nonbank providers of payment services is not harmonized at EU level, but it will be once the Payment Services Directive will come into force: the Directive prescribes information requirements to the competent authorities and sets conditions and limits for outsourcing of "important operational activities."[29] The Directive also 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

In Europe, the consolidation process implies the emergence of a smaller number of larger payment processors which serve larger shares of the payments market segments. This concentration may bring about a higher profile for system-wide risk, and an increased dependency of the banking sector on the non-banking sector.

4.2 Risks and nonbank presence in the U.S.

4.2.1 Comparison of nonbank prevalence to risk in payment activities

Nonbanks in the United States payment system are subject to every type of risk cited in Table 9 and so the general comments above on risk in payments applies accordingly. There are some specific subactivities tied to the enrolment of customers and authorization of payments where nonbanks play a vital role in controlling liquidity and credit risk. Nonbanks are generally present along the entire payment processing chain and so have a role in operational risk and the consequent issues of related risks such as compliance, data security, and illicit use of payments.

4.2.2 Risk implications

There is little quantitative information on the extent to which nonbanks contribute to payment risk in the United States. Losses due to fraud are a frequently cited measure of payments risk, but there is no information available that allows an assessment of nonbank responsibility for payments fraud.

Data breaches are widely reported as a problem for payments and may serve as a measure of data security risk. Table 10 (p. 51) shows an analysis of data breaches that have occurred in the United States from January 2005 to April 2007. The data were

[29] 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 the Directive, or its financial performance, or the soundness or the continuity of its payment services (Art 11).

assembled by the Privacy Rights Clearinghouse, which relies on public information sources. They list breaches where information exposed would be useful for identity theft, which often manifests itself in fraudulent use of some type of payment. The information is sufficient to roughly identify the sectors of the economy where the data were compromised.

During this 28-month period, 541 data breaches were publicly reported. Most of the breaches—402—occurred in the second half of the period (after April 1, 2006). We cannot conclude with certainty that the number of data breaches actually increased because numerous new laws on notification were implemented after the middle of 2005, at least partially causing a rise in publicly-disclosed data breaches.

Still, the publicly-disclosed data breaches can be interpreted as revealing one of two undesirable aspects of retail payments risk. Either the 139 incidents reported in the first half of the period significantly understates actual data breaches, or the number of breaches increased rapidly in the second half.

Data breaches compromised nearly 154 million records. Roughly three-quarters of the records were compromised in just three incidents: the large data breaches at TJX and CardSystems, and a data breach reported in May 2006 at the U.S. Department of Veteran's Affairs that compromised 28.6 million records. These three incidents compromised a total of 116 million records. Like many measures of risk, very few incidents can account for a large portion of losses.

Occurrences of data breaches and compromised records do not necessarily go hand in hand. The nonbank payment processor sector accounted for only 2.5 percent of all data breaches but 26.5 percent of compromised records. This sector was responsible for nearly 75 percent of compromised records in the first half of the period. On this data, a re-evaluation of public policy towards risk management for nonbank payment processors may be valuable.[30]

The bank and financial services sector accounted for 9.4 percent of incidents and 4.1 percent of records compromised over the entire period. The worst blemish for bank and financial services was the 10.7 percent share of records compromised in the first half of the period. However, the share fell to only 0.6 percent in the second half.

Importantly, Table 10 reveals that a large number of data breaches have occurred in education, retail, health care, and government sectors. These four sectors together account for 77 percent of data breaches in this particular period. Data breaches in the education and health care sectors account for only 3.2 and 0.8 percent of all records compromised, so these breaches tend to reveal small numbers of records. The retail and government sectors have been hit with breaches that have revealed large numbers of records. However, given that data breaches that reveal large numbers of records are rare, we cannot assume that it is unlikely that the education and health care industries will be a victim of a large data breach. Any industry that stores a significant amount of sensitive data is an attractive target for hackers.

[30] Given the flaws in this data, this is a tentative conclusion that should be explored further as better data and more experience with existing risk management processes becomes available.

The education, retail, health care, and government sectors are not normally associated with the United States payments system. However, to the extent that sensitive information useful to making fraudulent payments, these sectors may be important to efforts to reduce the vulnerability of the payments system.[31]

4.2.3 Public regulation and oversight of payment risk management in the U.S.

Public policy toward risk management in payments has encompassed consumer protection, data security, prudential supervision, and law enforcement.[32] Table 11 (p. 52) describes these areas of concern, their legal basis, and other details of regulation and enforcement. The extent and complexity of public involvement vary across elements of the payments process (from initiation to final settlement), institutional aspects of the payments industry, and the legal issues tied to payments. As shown in the last column of Table 10, bank and nonbank payment providers face different oversight regimes in the area of data security and prudential supervision.

For example, the Graham-Leach-Bliley Act of 1999 set data security requirements for financial institutions and therefore applies to payments data. If a bank outsources payment processing to a nonbank, then the nonbank is subject to the same data security standards as banks. There is no similar federal data security requirement for nonfinancial institutions. To some extent, the Federal Trade Commission (FTC) has 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.[33]

4.2.4 Supervision and regulation

The difference in prudential supervision of some nonbank payment processors can be traced to enabling legislation that recognizes the special nature of banks and a desire to limit the extension of bank-like oversight to nonbank entities. As a result, oversight of some nonbank payment providers that are subsidiaries of financial institutions is conducted under the same supervisory process applied to the banking organization. Payment providers that are completely independent of financial institution but are in an outsourcing relationship with financial institutions are supervised under an alternate regime. In addition, some larger nonbank payment providers that are bank affiliated are

---

[31] How important particular economic sectors are regarding data breaches and payments risk requires additional research into the true underlying risk across economic sectors. Federal and state disclosure guidelines, for example, are not uniform. If disclosure standards were not equal, then data across sectors or states may not be comparable. In addition, exposed records across sectors may not be equally useful for misuse. Data from the bank and financial services or the nonbank payments processing sectors may be particularly useful in perpetrating payments fraud compared to that of other sectors.

[32] Another important area of oversight is systemically important payments systems, which is governed in the U.S. by the *Federal Reserve System's Policy on Payments System Risk* (2007).

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

also supervised under the alternate regime.[34]

Selected nonbank payments providers are overseen by the same agencies that supervise financial institutions. Supervision of payment providers is conducted within a broader program that oversees technology service providers (TSPs). The TSPs offer a wide variety of technology services, and some (but not all) services are related to payments. A risk evaluation of individual TSPs identifies those that would come under the supervisory program and determines the time frame for examination and monitoring activity.[35]

At year end 2004, 125 TSPs were supervised (Table 12, p. 53). Both bank-affiliated and independent TSPs are in the program, but twice as many independent TSPs are supervised. Core processing (computer processing of general ledger accounting and of information systems), offered by 68 of the supervised TSPs, is the single most important line of business.[36] But payments are important to these TSPs, with nearly 70 percent offering at least one type of payment processing service.

While the largest independent payments providers are probably represented in the TSP supervision program, it does not cover all TSPs that offer payments services. 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.[37] But at most 87 payments processors were supervised at year end 2004 (Table 12).

One reason that many nonbank payments providers are not supervised is that the enabling legislation is sufficiently narrow to exclude many significant payment providers. In particular, independent TSPs must be in an outsourcing relationship with a bank to be eligible for supervision. But many payment providers are customers of banks. For example, PayPal or Ceridian Corp. originate many payments and pass that information to banks for further processing.[38] In this instance the originator is purchasing payment services from the bank. A similar relationship exists between banks and acquirers of point-of-sale transactions or originators of many automated clearinghouse transactions. As such, risk management via direct supervision is currently not an option for these elements of the United States payment network.

There are two factors that may make prudential supervision of nonbank payment providers in the United States weaker than supervision of financial institutions. First, the purpose of TSP supervision is not the survival of the TSP or the viability of its business

---

[34] Sullivan (2007). Whether a particular payments provider is supervised is not publicly available information.

[35] FFIEC (2003).

[36] Business activities shown in Table 4 are based on information provided by examiners. Examiners do not expect that these reports would be subject to statistical analysis and therefore the completeness of the reported lines of business is uncertain. However, it seems unlikely that any misreporting would be biased regarding payments activity and so the relative position of bank versus nonbank payments providers should not be misleading.

[37] Dash (2005). There is no comprehensive data source that would show the number of companies that provide payment services to financial institutions.

38 If they do provide outsourced services to banks, these organizations may be eligible for the TSP supervision program.

model.[39] Rather, the TSP supervision program is targeted as a service to the supervisors of depository institutions. It is useful because examiners of depository institutions have a resource that they can draw upon to understand the risks that an outsourcing relationship might pose for the depository institution. A TSP examination seeks to ensure that there is a control environment that adequately addresses these risks. Protection of the payments system is a secondary, though important, concern of prudential supervision.

Second, supervisory agencies can examine independent payment providers but have limited enforcement power if they find weaknesses at the organization. Enforcement powers over financial institutions include voluntary agreements, cease and desist orders, removal or prohibition of individuals from an institution or the industry, civil money penalties, termination of deposit insurance, appointment of bank conservators, and divestment of activities.[40] Enforcement powers over independent payment providers include only voluntary agreements and prohibitions on financial institutions from doing business with the service provider.

4.2.5 Oversight of the U.S. payment system

The Federal Reserve has responsibility to oversee the payments system by monitoring payments systems, assessing them for safety and efficiency, and inducing change when necessary.[41] The Federal Reserve System issued its *Policy on Payments System Risk* to provide guidance on principles and minimum standards for managing risk in systemically important payments systems.[42] While aimed primarily at wholesale, large-value payment systems, it is also relevant to retail payments systems. The Federal Reserve applies these standards to the retail payments systems (ACH and cheques) that it operates and where it has explicit supervisory authority over financial institutions that operate clearing and settlement systems. The Federal Reserve also participates in national and international policy processes that set standards for operating and controlling risk in payments systems.

The authority of the Federal Reserve System to oversee payments, however, is limited. Recently Chairman Ben Bernanke stated that "[i]n contrast to the situation in some other countries, the Federal Reserve lacks explicit legal authority to oversee systemically important payments systems."[43] Federal Reserve examiners can review payment activities of the banks in its jurisdiction and they also participate in the TSP supervision program. Federal Reserve authority to set regulations also has important influence on some operational aspects of payments and on incentives to control risk by determining liability in cases of fraud and operational disruptions. But neither the Federal Reserve, nor any other federal agency, has explicit authority to manage retail payments

[39] Federal Reserve Board (2000).

[40] Spong (2000).

[41] Committee on Payment and Settlement Systems (2005).

[42] Federal Reserve Board (2007).

[43] In addition, Chairman Bernanke 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)). By contrast, the Banque de France has broad power to oversee noncash payments; see European Central Bank Oversight Division (2007, p. 21).

risk from a system perspective.

4.3 Changing risk profiles: implications of rising nonbank presence for risk

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.

This 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.

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 has 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.[44] Since this incident, PayPal has been successful at improving its data

[44] U.S. Department of Justice (2002).

security and fraud detection systems.[45]

Second, and more broadly, banks traditionally act as gatekeepers to the payments system. 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. At the beginning of 2007, another major data breech occurred at the large retailer group TJX, which operates over 2000 stores in various countries, including the UK and Ireland. The breach exposed more than 90 million cards accounts numbers. Losses to banks and other issuers have been estimated at between 68 million and 83 million USD for the 65 million visa accounts exposed alone (Kerber, 2007).

In the period between end June 2004 and November 2006, the MasterCard Stop-It service to combating phishing resulted in identifying 3743 phishing/spoof sites, 99 percent of which were taken down by the end of November. The service also detected 1334 carding/ecommerce sites (web sites where criminals sell cards data), of which 95 percent were shut down within 24-48 hours, and identified 54,653 unique MasterCard account numbers for sale/trade.[46] According to a Visa Europe report on account data security in 2005 there were 91 incidents (one every four days), and there were several hacks involving European acquirers and merchants. This resulted in over 1 million cards exposed, and the cost of fraud amounted to USD 30 million (Littas, 2006). Although these examples point out those criminals attempt attacks on an increasingly high scale through IT technology, the actual level of fraud can be considered low (for instance, according to Visa Europe Annual Report 2006, the fraud to sales ratio was 0.069 percent of total POS spending).

Another incident involved data breaches related to unloyal staff of outsourcing companies. For instance, a UK journalist reported that he was able to buy details about 1000 UK customers from a Delhi call centre worker, for GBP 4.25 each, saying that both cards credit numbers and account password were for sale.[47]

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

[45] Cox (2001); Garver (2005).

[46] Ates (2006).

[47] Mc Kenna (2005)

$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.[48]

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.[49] 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.

Dependencies of banks on external nonbanks parties/networks other than outsourcing companies have also increased, not only in terms of business relations but also in terms of capability to mitigate risks. For instance, co-operation of payment service providers with internet providers is key to combating payment fraud via IT systems in terms of prompt shutting down fraudster web-sites and phishing sites. Nonbank third-party processors may also subcontract to other nonbanks and one possible issue is how risk related to activities that are subcontracted is controlled, especially because in case of problems banks may face compliance risk as well as the ultimate reputational risk with users of payment instruments.

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

[48] Iowa Attorney General, (2005).
[49] McPhail (2003).

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. This may however bring about more complex processing models, and increase the profile of exposure to operational risk in its various forms.

Data security risk, fraud risk, and reputational risk have become more prominent with the increased occurrence of fraud cases. Risk of intrusion (outsiders, hackers' attacks) has increased, due to higher number of contact points/links/interfaces between internal systems and open networks and increased local storage of payment sensitive data that may be used in remote payment initiation. In recent years, payment fraud by using IT systems or IT-compromised payment data allowing false authentication and illicit execution of payments is considered to have increased in most European countries, although comprehensive and comparable statistics are not available yet. In particular, it is believed that in general the organised crime has shifted its attention from attacks aimed at individual users of e-banking and e-payment solutions to the more potentially effective hacking of data warehouses (in terms of possibility to achieve mass data compromise).

The United Kingdom has a more advanced effort to statistically monitor payment fraud. Even though the UK is not included in our survey, their figures may provide a general idea of the size of the potential losses involved. U.K. authorities have calculated that the losses resulting from payment cards fraud amounted in 2004 to 504.8 million GBP (about EUR 740 million). Of this amount, about 30 percent derived from card-not-

present transactions (GBP 150.8 million, or EUR 221 million) and another 25 percent from counterfeit cards, manufactured from skimmed data or by card cloning techniques (GBP 129.7 million, or EUR 190 million).[50] Efforts to mitigate fraud-related threats have been successful, thanks to progress in technology for encryption, identification and authentication, and to significant industry efforts such as the migration to chip/PIN cards and the use of smartcards. However, as solutions are implemented to combat a specific threat, fraudsters devise new methods of exploiting other weaknesses. In the U.K. the successful adoption of CHIP and PIN cards led to a fall of fraud losses, and in 2006 the total losses have declined to GBP 428 million (about EUR 627 million). In particular, there was a 23 percent decline in cards counterfeit card losses. However, this was accompanied by a strong increase in card-not-present fraud (up 40 percent from 2004) Thus, fraud in the electronic world is a moving target and requires constant monitoring of IT threats that can be employed at the expense of the financial sector and of the payments industry in particular.

Recent developments in retail payments systems have raised concerns that market forces may not adequately control risk because of greater reliance on electronic payment networks and the associated increase in nonbank payment providers. The primary issue is that an individual participant in an electronic payment network has incentive to implement risk controls that reflects private costs and benefits. But the interrelated nature of participants in the payments network implies that some benefit of individual risk control accrues to other network participants. This implies that the social benefits of implementing risk controls will be greater than the private benefits. From society's point of view, without some form of policy interference in the payments market, insufficient resources may be applied to controlling risk in payments.[51]

There are many examples of security incidents at one point of the payment system causing problems elsewhere in the system. Banks have been forced to reissue their payments cards because of unauthorized access to data elsewhere in the payments system. Merchants are exposed to chargeback expenses because a criminal uses a counterfeit card. Consumers have been victims of payment fraud that result in significant out-of-pocket expenses. Nonbank processors bear the expense of upgrading the security of their payments infrastructure. In the end, all participants of in the payments system are exposed in some manner.

Insufficient incentives to manage risk in the payment system may contribute to these problems. However, it is difficult to know the severity of incentive problems. Self-interest will lead to some risk management efforts by all participants in payments. Moreover, if everyone in the payment system managed risk in a socially optimal manner, we would still observe some amount of security problems and payments fraud. As a result, a balanced public policy towards management of risk in payments seems warranted. Efforts by private industry to manage payment risk should be encouraged and supported. Carefully designed regulations can help coordinate industry efforts and maintain industry standards. Laws and criminal penalties can deter fraud and other misuse of the payments system. Finally, the importance of confidence in the overall

[50] Fraud Prevention Expert Group (2007), Report on Identity theft and fraud, available at http:// ec.europa.eu/internal_market/fpeg/index_en.htm

[51] Bank of England (2000), p. 172.

payment system--a public good--should not be underestimated.

5. Conclusions and closing remarks

In this paper we have reviewed the role played by nonbanks in the retail payments industry, both as front-end and back-end providers of services. We assess this role as being prominent in the United States and high in several of the surveyed European countries. In the United States, this is true across all payment instruments and along the entire processing chain. In Europe, this is true for cards in most countries and, in some countries, for most payment instruments, although there are differences concerning national preferences in the use of certain payment products, as well as in available data. In Europe, for some payment instruments, little information is available, particularly for payment instruments that are not widely used or whose use is declining.

We conclude that the role of nonbanks has margin for further growth in Europe, driven by the SEPA project, the restructuring and consolidation of the payments processing industry, and the growth of payment instruments whose processing models rely more heavily on third-party processors (for example, cards, which imply real-time authorisation and interplay among the parties involved in the scheme). Card transactions are growing significantly in Europe, particularly in those countries where maturing payment instruments are being replaced with electronic-based payments. Finally, changes in the regulatory environment will soon allow nonbank front-end payment service providers (the payment institutions) to operate within Europe in a harmonised framework, and their role is expected to increase.

Next, we analysed the risk categories that are most relevant for retail payments and showed that, while some of them (legal risk, reputational risk, and systemic risk) are of a general nature, others may be associated directly with specific activities along the payments processing chain. Due to the adoption of advanced technologies and more complex processing and business models (characterised by the interplay of numerous parties, IT systems, and databases), we found that some categories of risk have become more prominent. This is particularly the case with operational risk in its various forms (malfunctioning, data security, and fraud), and associated reputational risk.

Evaluating how these developments impact the nature and balance of risks between banks and nonbanks and the multiple roles they play, we conclude that controlling for risk may have become more challenging in the new environment.

First, nonbanks increasingly have gained access to payment systems (directly, or indirectly in the form of a technical access following outsourcing), and the resulting more complex networks of systems, relations, and interactions require a higher degree of coordination among participants. The regulation and implementation of security standards, for example, may have become more complex, and different incentives and interests may need to be reconciled. In principle, unless safeguards are in place, a heightened nonbank presence could present new points of entry for criminals into the payment systems. Looking to the future, as new technologies are introduced and new contact points and players enter the picture, new potential vulnerabilities may need to be addressed. For example, vulnerabilities in wifi communication networks could present new security challenges, and telephone malware could be used to spread viruses to

consumer applications and to gain control of payments data stored in cell phones or data warehouses. These are just examples to show that the more contact points there are between networks and users and the more complex is their functioning, the more challenging is risk control.

Second, the trend toward using a given payment infrastructure for different payment instruments (for example, converting one payment type into another for easier processing, or introducing payment instruments that present features of other instruments), increases potential for cross-channel risk. For instance, criminals may tend to focus attacks on more-recently adopted open networks instead of bank-controlled proprietary networks. If criminals are able to misappropriate authentication and authorisation data and procedures, they may be able to submit "apparently" correct instructions to banks and into the payment system. The result would be fraud, whose ultimate cost, in terms of both financial cost and reputational damage, would in many cases be faced by banks.

Third, to the extent nonbank processors concentrate a larger share of payments in a certain market, a system-wide impact of disruption at a key player is possible.

While some of these risk issues do not originate from the bank or nonbank status of payment service providers, their control may be more challenging because the implementation of risk safeguards, particularly those introduced by regulation, may be designed and enforced starting from the assumption that payments safety depends on banks. These models may in some cases need to be reconsidered or complemented in light of the increased importance of nonbanks. In Europe, for example, the regulatory framework for banks and nonbanks providing payment services has been harmonised both at the front-end and back-end. Furthermore, the Eurosystem has clear statutory competence in oversight of payment systems and may take action in various forms, if deemed appropriate, to safeguard the safety and efficiency of payment systems, as well as public confidence in the payment instruments, irrespective of the bank or bank-nature of the entities involved.

We also note that nonbanks and some of the technologies they have introduced into payments processing have in many instances contributed to a reduced exposure to various sources of risks. Such contributions should not be underestimated, as they support banks' and other nonbanks' efforts towards reducing operational risk and fraud risk, in particular.

Given the global reach and open-access nature of many of the technologies currently being utilised in payments networks, increased cooperation among bank and nonbank supervisory authorities, and among bank and nonbank industry players performing functions at various stages of the payments chain, would be appropriate, not only at the domestic level but, increasingly, at the international level as well.

Finally, we note that many of the observations and conclusions in this paper are necessarily preliminary. Reflecting the lack of comprehensive and comparable data, we could not assess the severity of the various risks categories, nor the net overall effect on payments safety. Although efforts are being made by both the private and public sectors, particularly as regards the relevance of fraud risk, this is an area where more research is clearly warranted. As regards the role of nonbanks in Europe, the analysis of this paper could be complemented once more detailed and comparable data for the surveyed

countries were available. This study has focused primarily on the euro area. A more complete assessment of nonbanks' role in Europe would require data for the remaining European markets.

REFERENCES

Ates, E. (2006). Payment card fraud – "The involvement of organised crime," presentation delivered at the EC High Level Conference on Fraud, Brussels, 22-23 November.

Atos Origin (2007), Atos Origin Half Year Report 2007

Bank of England. 2000. "The Bank of England's Oversight of Payment Systems," *Financial Stability Review* (December), p. 173.

Berry, Kate and David Breitkopf. (2006). "Big Step for Visa May Prove Bigger For Industry; Merchants Gain More Clout; Association Model Fades Further," *American Banker*, October 26.

Bernanke, Ben S. (2007). "Central Banking and Bank Supervision in the United States." Remarks given at the Allied Social Sciences Association, January 5, *www.federalreserve.gov/boarddocs/speeches/2007/20070105/default.htm*.

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

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

Committee on Payment and Settlement Systems. (2005). *Central Bank Oversight of Payment and Settlement Systems*, Bank for International Settlement (May), *www.bis.org/publ/cpss68.pdf*.

Compliance-magazin.de (2007). "Viele Unternehmen erfuellen PCI-Regeln nicht," 24 September 2007, accessed on 24 October 2007.

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

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.

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

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

_____. (2007a). Consultation announcement: oversight framework for card payment schemes, Press Release, 3 May 2007.

_____. (2007b). Blue Book 2007, Payments and Securities Settlement Systems in the European Union, August.

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

European Central Bank Oversight Division and Federal Reserve Bank of Kansas City Payments System Research Department. (2007). "Nonbanks in the Payments System: European and U.S. Perspectives." Paper presented at the Federal Reserve Bank of Kansas City *Conference on Nonbanks in the Payments System*.

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

Federal Reserve Board. (2000). "Information Technology Examination Frequency," Supervision and Regulation letter SR00-3 (SUP), February 29.

_____. (2007). Federal Reserve Policy on Payments System Risk. Available at http://www.federalreserve.gov/paymentsystems/psr/policy07.pdf.

Fraud Prevention Expert Group. (2007a). Report on Identity theft and fraud. Available at http:// ec.europa.eu/internal_market/fpeg/index_en.htm

_____. (2007b). Draft Minutes of the 12th Meeting, 27 June 2007. Available at http:// ec.europa.eu/internal_market/fpeg/index_en.htm

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

Iowa Attorney General. 2005. "First Premier Bank Agrees to Deny Automatic Withdrawal Services to Telemarketing Scams," July 6, *www.state.ia.us /government/ag/latest_news/releases/july_2005/First_Premier.html*.

Littas, R. (2006). Fraud prevention challenges after the chip card migration, presentation delivered at Seminar on payment fraud in the EU Member States, the EU Accession Countries & other European countries, Brussels, 8–9 March 2006. Available at http://ec.europa.eu/internal_market/payments/docs/fraud/taiex_seminar/littas1st.pdf

MacKenna, B. (2005). "Credit card details in the clear and up for sale in India," Network Security, July.

Margerit, V. (2007). “The Payment Services Directive”, Banque de France Bulletin, August 2007.

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.

Mazzi, G. B. (2007). “*Developing successful strategies and increasing profitability in a SEPA environment*”, presentation delivered at the EFMA Cards and Payments Conference 2007, 18 September, Paris.

McPhail, Kim. 2003. “Managing Operational Risk in Payment, Clearing, and Settlement Systems,” Working Paper 2003-2, Department of Banking Operations, Bank of Canada, February.

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.

Sarazin, C. (2006). Implementing the SEPA Cards Framework (SCF): Towards greater security for card payments. Presentation available at http://ec.europa.eu/internal_market/fpeg/meetings_en.htm

Sullivan, Richard J. (2007). “Risk Management and Nonbank Participation in the U.S. Retail Payments System.” Federal Reserve Bank of Kansas City *Economic Review* (second quarter), pp. 5-40.

Spong, Kenneth. (2000). *Banking Regulation: Its Purposes, Implementation, and Effects*. Kansas City: Federal Reserve Bank of Kansas City.

U.S. Department of Justice. 2002. “Russian Computer Hacker Sentenced to Three Years in Prison,” October 4, *www.cybercrime.gov/gorshkovSent.htm*.

Visa Europe. (2007). Annual Report 2006.

Vulpiani, Domenico. (2006). “Identity theft: Security and Social Impact,” speech delivered at the EC High Level “Maintaining the integrity of Identities and Payments -- Two challenges to fraud prevention, Brussels, 22-23 November 2006

Table 1: Broad Payment Types

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

Table 2: 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 or deployments of ATMs
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 (such as a 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 (such as 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 (such as 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 (payer)
During-Transaction Stage 1			
10	Communication connection for merchants	a	Provision of gateway to acquirer/payment processors
		b	Provision of gateway to various networks/check or ACH authorization vendors
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
		c	Provision of decision management/fraud screening/neutral network scoring system to card issuers for authorization
		d	Process to verify and confirm if payer has sufficient funds (or credit lines) available to cover the transaction amount
12	Fraud and risk management services to front-end customers (payees)	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
15	Ex-ante compliance services	a	Anti-money laundering and terrorist financing regulation such as 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 (such as MICR to ACH)
		e	Provision of sorting transactions by destination groups to financial institutions
17	Clearing	a	Transmission of clearing orders (credit transfers, direct debits, cards, cheques) to a financial institution
		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) (such as 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, such as support services for treasury and accounting
		b	to consumers
		c	to financial institutions
23	Ex-post compliance services	a	Compliance with anti-money laundering and terrorist financing regulation, such as reporting to authorities, back-feeding to ex-ante databases

Table 3: Nonbank Importance: EU: Payment Cards

	FR	DE*	NL	IT	PT	BE	FI	AT	CZ	SI	GR	CY	LT	LV	BG
% on country total	31.7%	15.0%	33.5%	30.5%	58.4%	36.8%	44.9%	11.2%	8.4%	39.6%	53.5%	30.3%	37.5%	22.7%	8.9%
% on EU27	22.7%	10.5%	6.3%	5.1%	3.5%	3.2%	2.7%	1.0%	0.3%	0.4%	0.3%	0.1%	0.1%	0.1%	0.0%

		FR	DE*	NL	IT	PT	BE	FI	AT	CZ	SI	GR	CY	LT	LV	BG
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															

* In Germany a number of nonbanks are bank-owned

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

Data Quality
- High
- Medium
- Low

Table 4: Nonbank Importance: EU: Credit Transfers

	DE*	FR	NL	IT	AT	FI	CZ	PT	LV	BG	LT	GR	SI	CY
% on country total	43.1%	18.9%	35.5%	31.5%	50.3%	49.4%	54.2%	7.8%	76.8%	86.1%	58.3%	11.6%	42.2%	8.6%
% on EU27	31.7%	14.2%	7.0%	5.6%	4.8%	3.1%	2.0%	0.5%	0.4%	0.2%	0.2%	0.1%	0.5%	0.0%

		DE*	FR	NL	IT	AT	FI	CZ	PT	LV	BG	LT	GR	SI	CY
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														

* In Germany a number of nonbanks are bank-owned

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

Data Quality
- High
- Medium
- Low

Table 5: Nonbank Importance: EU: Direct Debits

	DE	FR	NL	AT	IT	CZ	PT	FI	SI	BG	CY	GR	LT	LV
% on country total	40.6%	17.2%	27.9%	37.1%	12.8%	37.4%	12.4%	5.6%	16.8%	4.9%	13.5%	0.1%	2.7%	0.4%
% on EU27	36.6%	15.8%	6.7%	4.3%	2.8%	1.7%	0.5%	0.4%	0.2%	0.0%	0.0%	0.1%	0.0%	0.0%

		DE	FR	NL	AT	IT	CZ	PT	FI	SI	BG	CY	GR	LT	LV
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														

* In Germany a number of nonbanks are bank-owned

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

Data Quality
- High
- Medium
- Low

Table 6: Nonbank Importance: EU: E-Cheques

% on country total	31.1%	15.6%	21.0%	1.0%	47.6%	24.2%	0.4%	0.0%	0.0%	0.0%	0.1%	0.1%	1.4%
% on EU27	54.7%	6.5%	3.1%	1.7%	0.3%	0.3%	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%

		FR	IT	PT	DE*	CY	GR	AT	BG	CZ	LT	FI	LV	SI
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													

* In Germany a number of nonbanks are bank-owned

Importance
- Prevalent
- High
- Medium
- Low
- Nonexistent

- Not applicable
- Not able to judge

Data Quality
- High
- Medium
- Low

Table 7: Nonbank Importance: EU: E-Money

		NL	BE	DE*	FR	AT	IT	PT	LT	FI	BG	CY	CZ	GR	LV	SI
% on country total		3.0%	6.4%	0.3%	0.1%	1.0%	0.1%	0.1%	1.5%	0.1%	-	-	-	-	-	nav
% on EU27**		35.5%	34.8%	12.1%	5.9%	5.7%	0.9%	0.4%	0.3%	0.3%	-	-	-	-	-	nav
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															

* In Germany a number of nonbanks are bank-owned

**(% may be overestimated due to lack of data for e-money issued in the UK, which is not included in EU total)

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

Data Quality
- High
- Medium
- Low

Table 8: Nonbank Importance: United States

Payment Activity		Type of Payment and Share of Noncash Payments											
		Payment Cards 45.9%			Direct Debits 6.86%			Credit Transfers 6.03%	e-Cheques 4.41%	e-Money 0.00%			
		4-party Credit/ Sig. Debit	PIN-Debit	3-party Credit	Automatic	One-time	Tempo/ PayByTouch			Prepaid Card Open-Loop	Prepaid Card Closed-Loop	PayCash	PayPal
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

Data Quality
- High
- Medium
- Low

Table 9: Payment Activities and Selected Risks

Activity				Type of Risk							
				Liquidity and Credit			Operational				
Primary Activity		Subactivity		Liquidity	Credit	Settlement agent credit risk	Malfunctioning and/or other operational problems	Data security risk associated with fraud or violations of privacy responsibilities	Counterfeit and associated fraud	Compliance	Illicit use (AML, terrorist financing)
Pre-Transaction											
1	Customer acquisition	a	Registration and enrollment of customers as payers (consumers)		x			x		x	x
		b	Registration and enrollment for merchant accounts or deployers of ATMs	x	x			x		x	x
2	Services for issuer's front-end customer (payer) acquisition	a	Provision of credit evaluation/credit risk assessment tools		x		x	x			
		b	Application processing services				x	x			
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				x	x	x	x	
		b	Hardware and software production (such as a card reader) for usage with a consumer's online device (PC, mobile, handheld)				x	x		x	
		c	Provision of e-money wallet / access code to e-money values					x			
		d	Cheque manufacturing				x	x	x		
4	Provision of hardware to accept payment instruments/devices	a	Provision of ATM terminals (sell/lease; manage)				x	x		x	
		b	Provision of POS terminals				x	x		x	
		c	Provision of cheque readers/cheque POS terminals				x	x			
5	Provision of software to accept payment instruments/devices	a	Web hosting services				x	x		x	
		b	Provision of shopping cart software				x	x		x	
		c	Provision of software to connect payment gateway service providers				x	x		x	
		d	Provision of cheque verification software				x	x	x		
6	Provision of internet security-related technology/support	a	Certificate-authority services (such as PKI-based secure environments); provision of digital identity services for consumer authentication					x		x	
		b	Provision of online transaction security systems to front-end customers (payees, merchants...), and back-end customers (such as 3D-secured card transactions via internet)				x	x		x	
		c	Provision of e-signatures and other e-authorizations for payment authorization purposes				x	x		x	
7	Payment Card Industry (PCI) compliance services to merchants and/or payers	a						x		x	
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				x	x		x	
9	e-invoicing	a	Creation and delivery of electronic invoices to front-end customers (payer)				x	x		x	
During-Transaction Stage 1											
10	Communication connection for merchants	a	Provision of gateway to acquirer/payment processors				x	x		x	
		b	Provision of gateway to various networks/check or ACH authorization vendors				x	x		x	
11	Transaction authorization (fund verification)	a	Provision of network switch services; a back-end service				x	x		x	
		b	Provision of communication connection between networks and payment instrument issuers				x	x		x	
		c	Provision of decision management/fraud screening/neutral network scoring system to card issuers for authorization		x		x	x			
		d	Process to verify and confirm if payer has sufficient funds (or credit lines) available to cover the transaction amount		x		x	x		x	
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 authorization services		x			x		x	
		b	Identity authentication					x		x	
		c	Decision management/fraud screening/neutral network scoring system (hosted at third-party service providers)					x	x		
13	Fraud and risk management services to card issuers	a	Monitoring transactions and notifying cardholders of potential fraud, enabling them to take immediate action					x		x	
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	x	x		x	x			
15	Ex-ante Compliance services	a	Anti-money laundering and terrorist financing regulation such as controls to identify suspicious transactions (database, software, and so on)							x	x

Notes:
Data security risk is associated with the online environment.
Counterfeit and associated fraud is limited to physical payment instruments (checks and payment cards) used in an offline environment.

Table 9: Payment Activities and Selected Risks (Continued)

Activity				Type of Risk							
				Liquidity and Credit			Operational				
Primary Activity			Subactivity	Liquidity	Credit	Settlement agent credit risk	Malfunctioning and/or other operational problems	Data security risk associated with fraud or violations of privacy responsibilities	Counterfeit and associated fraud	Compliance	Illicit use (AML, terrorist financing)
During-Transaction Stage 2											
16	Preparation	a	Sorting merchant's sales information by payment instrument/network for clearing				x	x		x	
		b	Submission of sales information to each payment instrument network				x	x		x	
		c	Calculation of each network member's (either financial institution or processor) net position and transmission of net position information to each member				x	x			
		d	Provision of transformation services into other payment instrument formats (such as MICR to ACH)				x	x			
		e	Provision of sorting transactions by destination groups to financial institutions				x	x			
17	Clearing	a	Transmission of clearing orders (credit transfers, direct debits, cards, cheques) to a financial institution				x	x			
		b	Transmission of clearing orders to ACH operator				x	x			
		c	Distribution of advices showing the amounts and settlement dates				x	x			
		d	Clearing (different from an ACH)				x	x			
18	Settlement	a	Posting credit and debit at each financial institution's central bank account	x	x		x				
		b	Posting credit and debit at each financial institution's commercial bank account	x	x	x	x				
		c	Posting debit (credit in case of a return) to front-end payer account	x	x	x	x				
		d	Posting credit (debit in case of a return) to merchant (payee) account	x	x	x	x				
		e	Check settlement	x	x	x	x				
Post-Transaction											
19	Statement	a	Provide statement preparation/delivery services for front-end customers (payers) (such as mobile credit advice or online bank/card account statements)				x			x	
		b	Provision of statement/payment receipt notification services for merchants (payees)				x			x	
20	Reconciliation, incl. collection and receivable management services	a	Matching invoices and payments				x	x		x	
21	Retrieval	a	Provision of chargeback and dispute processing services				x	x			
22	Reporting and data analysis services	a	to merchants, such as support services for treasury and accounting					x			
		b	to consumers					x			
		c	to financial institutions					x			
23	Ex post Compliance services	a	Compliance with anti-money laundering and terrorist financing regulation, such as reporting to authorities, back-feeding to ex-ante databases					x		x	x

Notes:
Yellow shading of table cells indicate activities and components of settlement risk.
Data security risk is associated with the online environment.
Counterfeit and associated fraud is limited to physical payment instruments (checks and payment cards) used in an offline environment.

Table 10: Publicly Reported Data Breaches in the United States

January 2005 to April 2007

Sector of origin	Bank and financial services	Nonbank payment processor	Education	Retail	Health Care	Government	Other or unknown	Total
A: Number of incidents								
All incidents	51 9.4%	16 3.0%	149 27.5%	101 18.7%	51 9.4%	118 21.8%	55 10.2%	541
before 4/1/2006	16 11.5%	6 4.3%	58 41.7%	21 15.1%	14 10.1%	11 7.9%	13 9.4%	139
after 4/1/2006	35 8.7%	10 2.5%	91 22.6%	80 19.9%	37 9.2%	107 26.6%	42 10.4%	402
	B: Records compromised							
All records	6,352,711 4.1%	40,691,306 26.5%	4,961,749 3.2%	61,288,322 39.9%	1,244,716 0.8%	35,761,123 23.3%	3,393,818 2.2%	153,693,745
before 4/1/2006	5,725,850 10.7%	40,200,526 74.8%	2,491,827 4.6%	2,765,590 5.1%	391,300 0.7%	960,183 1.8%	1,227,330 2.3%	53,762,606 35.0%
after 4/1/2006	626,861 0.6%	490,780 0.5%	2,469,922 2.5%	58,522,732 58.6%	853,416 0.9%	34,800,940 34.8%	2,166,488 2.2%	99,931,139 65.0%

Notes: Data are based on information collected by the Privacy Rights Clearinghouse and accessed on their Website April 8, 2007. Classification by sector of origin and other calculations are by the authors.

Table 11: Public Regulation Relevant to Payment Risk Management in the United States

Area of Regulation	Description	Legal basis	Enforcement authority	Regulations or guidelines	Treatment of bank and nonbank organizations
Consumer protection	Liabilities and responsibilities in check and electronic funds transfers	State check laws; Electronic Funds Transfer Act of 1978	For checks, state legal authorities; for electronic funds transfer, federal agencies (financial institution supervisory agencies* or the Securities and Exchange Commission according to their jurisdiction) with the Federal Trade Commission covering retailers and others payment participants not covered by other agencies	For electronic funds transfer, the Federal Reserve Board's Regulation E specifies disclosure, payment authorization, transaction record, and dispute resolution requirements	Equal
Data security	Safeguarding and disclosing to customers the use of sensitive nonpublic customer information	Graham-Leach-Bliley Act of 1999; various federal and state laws concerning unfair and deceptive acts in business transactions	Federal financial institution supervisory agencies*; Federal Trade Commission	Federal Reserve Board's Regulation P and Regulation H (appendix D2)	Unequal between financial and nonfinancial organizations
Prudential supervision	Periodic examination and ongoing monitoring of the financial health and prudential operation of the institution	Various laws enabling supervision of financial institutions; The Bank Service Company Act of 1962; state laws covering money transmitters	Federal financial institution supervisory agencies*	State and federal guidance provided by supervisory agencies; Federal Reserve regulations covering payments, such as Regulations J (check collection) and CC (check funds availability)	Generally unequal with the possible exception of where banks outsource payment processing to nonbanks
Law enforcement	Efforts to counter trends in illegal data breaches, identity theft, and money laundering	USA Patriot Act of 2001; Bank Secrecy Act of 1970; state law	Federal Bureau of Investigation Cyber Operations group; Secret Service Electronic Crimes Task Force; Department of the Treasury Financial Crimes Enforcement Network; state and local law enforcement	Electronic Crimes Task Force website (www.fincen.gov/reg_guidance.html); FinCEN website (www.secretservice.gov/ectf.shtml)	Equal

*Federal financial institution supervisors include the Office of the Comptroller of the Currency, the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision and the National Credit Union Administration.

Table 12: Business Lines Offered by Supervised Technology Service Providers
Year end 2004

Business Line	All TSPs		Bank affiliation status			
			Independent		Bank affiliated	
	N	Percent	N	Percent	N	Percent
Core processing	68	54.6%	37	44.6%	31	73.8%
Any payments-related business line*	87	69.6%	55	66.3%	32	76.2%
Other business line**	21	16.8%	19	22.9%	2	4.8%
Total number of TSPs	125		83		42	

*ACH processing/services, ATM processing/services/network/switch, bill payment service, credit card issuance, credit and/or debit card merchant processing, credit card network/switch, check processing, check processing software vendor clearing and settlement, POS processing/services/network/switch, and wholesale payments.
**Retail e-banking/transactional website hosting, electronic record safekeeping, imaging, loan or mortgage processing/servicing, corporate e-banking/cash management, website hosting (informational), disaster recovery, investment processing, aggregation, asset/liability management, credit scoring, other emerging technologies, employee benefit account processing, asset management processing, bank image processor, debit card "services", Internet services, IRA "services", payroll "services", safe deposit, student loan processor, trust processing services, Visa "services."

Notes: Many TSPs are double counted because they offer core processing, payments, and/or other business lines. As a result, the sum of the number of TSPs in each category is greater than the total number of TSPs, and the sum of percentages is greater than 100 percent. Bank affiliation status is determined by a significant ownership position by one or more depository institution, whether run as corporations, limited partnerships or limited liability companies. An independent TSP has no significant ownership by a depository institution.