

Nonbanks and Risk in Retail Payments: EU and U.S.

by

Terri Bradford,^{*} Fumiko Hayashi,^{*} Christian Hung,^{*} Simonetta Rosati,^{**}
Richard J. Sullivan,^{*} Zhu Wang,^{*} and Stuart E. Weiner^{*}

June 2008

Forthcoming in
*Managing Information Risk and the
Economics of Security*
Springer Publishing
Eric M. Johnson, ed.

JEL Classifications: G28, L51, E42

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 payment risks. Nonbanks play multiple roles along the entire payment processing chain. They are prominent in the United States and their presence is high and growing in Europe as well, although there are differences among the various countries and payments classes. Nonbanks' presence has shifted the locus of risks in retail payments towards greater relevance of operational and fraud risk. The paper reviews the main 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 Payments System Research Function.

^{**}European Central Bank Oversight Division.

The views expressed in this paper are those of the authors and do not necessarily reflect the views of the ECB, the Eurosystem, the Federal Reserve Bank of Kansas City, or the Federal Reserve System. A longer, more detailed version of this article is available in (ECB, FRBKC 2007b). This research has benefited from comments by participants at the Joint ECB-Bank of England Conference on Payment Systems and Financial Stability, Frankfurt, November 12-13, 2007, from seminar participants at the Banca d'Italia and the Reserve Bank of Australia, and from comments by anonymous referees for the WEIS 2008 conference.

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 2007a), we took a first step in documenting and analysing 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, 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.¹ This subsection provides a framework for documenting and analyzing these roles.

2.2 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

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

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” (EC 2006). 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 device 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.

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.

2.3 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.

Five broad payment types are considered 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,

³ ECB, FRBKC (2007a) 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.

credit transfers and direct debits, utilize agreements that credit or, with preauthorization, debit accounts. The fourth category, payment (credit and 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 or 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;
- *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 1.

2.4 Nonbank prevalence

2.4.1 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

Table 1: 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)

Table 1: Payment Activities (Cont.)

Primary Activity		Subactivity	
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.)

Table 1: Payment Activities (Cont.)

Primary Activity		Subactivity	
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 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 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, 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

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 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.

2.4.2 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. Results were obtained for 15 countries, 10 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 10 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 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

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

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

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 of 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.

A number of results emerge.

First, and most important, 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 (i) the growth of cashless payments; (ii) SEPA, and the resulting restructuring and consolidation ongoing within the payments processing outsourcing industry, and; (iii) the maturing of payments markets segments and substitution among payment classes favouring instruments whose growth is largely supported by nonbanks (cards and direct debits).

Second, nonbank presence varies significantly by country. In general, when considering nonbanks' importance across all payment instruments for each country, countries can be divided into three groups (ECB, FRBKC 2007a). In the 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 a 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 (such as 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.

And, fourth, irrespective of the role played in pre-transaction and other during-transaction activities, the settlement phase largely 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) and/or those who are allowed to hold payment settlement accounts. For e-money and other innovative payment solutions, settlement also remains largely dominated by banks, which is consistent with that innovation typically focusing on alternative means (such as Internet and mobile technology) to accessing traditional banking fund transfers services rather than offering fundamentally new payment instrument alternatives.⁶

⁶ See ECB (2005), 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

As an example of the detailed results obtained, the degree of nonbank participation in payment cards is presented in Table 2.⁷ In this table, moving from left to right, the degree of nonbank prevalence is shown for the surveyed countries accounting for the largest share of EU27 card payments to the countries accounting for the smallest share of EU27 card payments. Thus, the 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 (P), high (H), medium (M), low (L), or nonexistent (N) for that particular payment activity-payment type-country combination. Cells with parallel lines are not applicable, while cells in white indicate insufficient information to judge. The assessments are based on survey results, industry data, and other sources.

2.4.3 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 3 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 accounted for 4.4 percent,

does not modify the clearing and settlement phases of the payment cycle which are managed and regulated by banks.”

⁷ Tables for the other four broad payment types are shown in ECB, FRBKC (2007b).

Table 2: Nonbank Importance: EU: Payment Cards

% of 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	0.1	0.1	0.0
Pre-Transaction		FR	DE	NL	IT	PT	BE	FI	AT	CZ	SI	GR	CY	LT	LV	BG		
1	a		L	L	M	L	L	H	H	M	L	M			M	L		
	b		H	M	M	M	P	L	H	M	L	M	P	L	M	L		
2	a	H			P		L	P	H	M	L	M				M		
	b	P	H		P		P		H	M	L	H			H	L		
3	a	P	H	H		H	P	H	H		M	H	H	H	H			
	b	P	H	H	P		L		H	M	P	H		H		P		
	c		H		P		L		H	M		H		H				
	d				P		L		H	M		H		H				
4	a	P	H	H	P	H	P	P	H	M	M	H	P	P	P	H		
	b	P	H	H	P	H	P	P	H	M	M	H	P	P	H	H		
	c																	
5	a	P	H		P		P	M	H		L	P	P		L	M		
	b	P	H	H	P		P		H		H	P	M		P	H		
	c	H		H	P		P	M	H	M	H	H	P	P	P	H		
	d								H									
6	a	M	H	H	M	H	P		H		H		M		H			
	b	P	H	H	P		P		H		M		P		H			
	c	M		H		L			H	M	H							
7	a		H		P		P	H	H	M						M		
	a	M	H	M	P	H	P	P	H	M	L	H			M	M		
8	a		H	M	P	H	P	P	H	M	L				M			
	a		H	H	P	P	P	P	H	M	L	M			M			
9	a		H	H	P	P	P	P	H	M	M	M			M			
	a		H	H	P	P	P	P	H	M	M	M			M			

Notes: P=Prevalent, H=High, M=Medium, L=Low, N=Nonexistent
 Prevalent; High
 Medium, Low, Nonexistent
 Not applicable
 Not able to judge

Table 2: Nombank Importance: EU: Payment Cards (Cont.)

	FR	DE	NL	IT	PT	BE	FI	AT	CZ	SI	GR	CY	LT	LV	BG
During-Transaction – Stage 1															
10	a	M	H	H	P	H	P	H	M	P	H	P	P	H	H
	b	H	H	H	P	P		H	M	H	H	P	P	H	P
11	a	L	H	H	P	P	P	H	M	H	P	P	P	H	P
	b	M	H	H	P	P		H	M	H	P	P	P	H	P
	c	M	H	L	H		P	H	M	M	P	P	P	H	P
	d	M	H	L	M		L	H	M	L	H	P	H	M	H
12	a	M	H	H	P	P	L		M	M	H	P	H	L	
	b	M	H	H	P	P		H	M	L	H		L	L	L
	c	M	H	M	P	P	P	H	M	M	H	P	H	L	
13	a	M	H	L	H	P	M	H	M	M	H	P	H	M	M
	a	M		L	H	L		H	M	L	P	H	M	M	
14	a	L	H	L	H	L		L	M	L	P	H	M	M	
	a	L	H	L	H			L	M		P			L	
During-Transaction – Stage 2															
16	a	L		H	M	H	M	H	M	M	H	P	P	M	
	b	L		H	M	P	M	H	M	M	H	P	P	H	M
	c	L		H	M	P	M	H	M	H	P	P	P	H	P
	d		H	H				L		L					
	e	M	H	H			P		H	M			P	P	
17	a	L		H	H	M	M	H	M	M	P	P	H		P
	b	L		H	H	P		H	M	M	H	P			
	c	L	H	H	H	P		H	M	M	H	P	L	M	P
	d	L	H	H	H			H	M	M	H			H	

Notes: P=Prevalent; H=High; M=Medium; L=Low; N=Nonexistent

Prevalent; High

Medium; Low; Nonexistent

Not applicable

Not able to judge

Table 2: Nonbank Importance: EU: Payment Cards (Cont.)

	FR	DE	NL	IT	PT	BE	FI	AT	CZ	SI	GR	CY	LT	LV	BG
During-Transaction – Stage 2															
18	a	L	H	H		P	H	H	M	M					
	b	L	L	L		P	H	H	M	M					
	c	L				N	L	H	M	M	L			L	H
	d	L	L	L		N	L	H	M	M	L	P		L	H
	e			L											
Post-Transaction															
19	a	M	M	H		M		H	M	M	M	P		M	M
	b	M	L	H			L	H	M	M	M		M		L
20	a		H	P			L	H	M	M	M	P			
	a		H	M		M	L	H	M	M	M	P	M	L	
21	a		H	H		P		H	M	M	M	P	H		
	b		H	H		N		H	M	M	M	P			
	c		H	H		P		H	M	M	M	P			
22	a		H	P		N		H	M	M	M	P			
	b		H	P	H	P		H	M	M	M	P	H		H
23	a	L		P		M		L	M	M	M			L	

Notes: P=Prevalent, H=High, M=Medium, L=Low, N=Nonexistent

Prevalent, High

Medium, Low, Nonexistent

Not applicable

Not able to judge

Table 3: Nonbank Importance: United States

Payment Activity	Type of Payment and Share of Noncash Payments											
	Payment Cards 45.9%		Direct Debits 6.86%	Credit Transfer 6.03%	e-Cheque 4.41%	Prepaid Card		e-Money 0.00%				
	4-party Credit/Sig. Debit	PIN-Debit	3-party Credit	Automatic	One-time	Tempo/PayBy Touch		Open-Loop	Closed-Loop	Prepaid Card	PayCash	PayPal
Pre-Transaction												
1	a	P	P	P	P	P		P	P	P	P	P
	b	P	P			P		P	P	P	P	P
2	a	H	H			P						
	b	P	P	P	P	P		P	P	P	P	P
	a	P	P	P		P		P	P	P		P
3	b											
	c										P	P
	d											
4	a	H	H	H								
	b	P	P	P		P		P	P	P		
	c											
5	a	P	P	P	P	P		P	P	P	P	P
	b	P	P	P								
	c	P	P	P	P	P						
	d											
6	a	P	P	P	P	P		P	P	P	P	P
	b	P	P	P	P	P						
	c	P	P	P	P	P						
7	a	P	P	P								
8	a											
9	a	P	P	P	P	P		P	P	P	P	P





Notes: P=Prevalent, H=High, M=Medium, L=Low, N=Nonexistent
 Prevalent, High
 Medium, Low, Nonexistent
 Not applicable
 Not able to judge

Table 3: Nonbank Importance: United States (Cont.)

Payment Activity	Type of Payment and Share of Noncash Payments										
	Payment Cards 45.9%		Direct Debits 6.86%		Credit Transfer 6.03%	e-Cheque 4.41%	e-Money 0.00%			PayPal	
4-party Credit/Sig Debit	PIN-Debit	3-party Credit	Automatic	One-time			Tempo/PayBy Touch	Prepaid Card Open-Loop	Prepaid Card Closed-Loop		PayCash
During-Transaction – Stage 1											
10	a	P	P	P	P	P	P	P	P	P	P
	b	P	P	P	P	P	P	P	P	P	P
11	a	P	P	P	P	P	P	P	P	P	P
	b	P	P	P	P	P	P	P	P	P	P
	c	P	P	P	P	H	P	P	P	P	P
	d	H	H	H	H	P	H	H	P	P	P
12	a	P	P	P	P	P	P	P	P	P	P
	b	P	P	P	P	P	P	P	P	P	P
	c	P	P	P	P	P	P	P	P	P	P
13	a	H	H	H	H	P	P	P	P	P	P
14	a	H	H	H	H	P	P	P	P	P	P
15	a	H	M	P	M	M	M	M	M	P	P
During-Transaction – Stage 2											
16	a	P	P	P	P	P	P	P	P	P	P
	b	P	P	P	P	P	P	P	P	P	P
	c	P	P	P	P	P	P	P	P	P	P
	d										
	e										

Notes: P=Prevalent; H=High; M=Medium; L=Low; N=Nonexistent
 [Shaded Box] Prevalent; High
 [White Box] Medium; Low; Nonexistent
 [Horizontal Lines Box] Not applicable
 [Vertical Lines Box] Not able to judge

Table 3: Nonbank Importance: United States (Cont.)

Payment Activity	Type of Payment and Share of Noncash Payments										
	Payment Cards 45.9%		Direct Debits 6.86%		Credit Transfer 6.03%	e-Cheque 4.41%	Prepaid Card		e-Money 0.00%		
	4-party Credit/Sig Debit	PIN-Debit	3-party Credit	Automatic			One-time	Tempo/PayBy Touch	Open-Loop	Closed-Loop	Prepaid Card
During-Transaction – Stage 2											
17	a	P	P	P	H	H	P		H	P	
	b										
	c	P	P	P	P	P	P	P	P	P	P
	d										
18	a	N	N	N	N	N	N	N	N	N	N
	b	N	N	N	N	N	N	N	N	N	N
	c	P	P	P	P	P	P	P	P	P	P
	d	P	P	P	P	P	P	P	P	P	P
e											
Post-Transaction											
19	a	P	P	P	P	P	P	P	P	P	P
	b	P	P	P	P	P	P	P	P	P	P
20	a	P	P	P	P	P	P	P	P	P	P
	b	P	P	P	P	P	P	P	P	P	P
21	a	P	P	P	P	P	P	P	P	P	P
	b	P	P	P	P	P	P	P	P	P	P
22	a	P	P	P	P	P	P	P	P	P	P
	b										
23	a	P	L	P	L	L	L	L	L	L	P
	b	L	L	P	L	L	L	L	L	L	P

Notes: P=Prevalent; H=High; M=Medium; L=Low; N=Nonexistent
 [Grey Box] Prevalent; High
 [White Box] Medium; Low; Nonexistent
 [White Box with Dots] Not applicable
 [White Box with Dots] Not able to judge

and the e-money share was nearly negligible.⁸ Within some of these broader categories, in turn, are shown more specific payments instruments: three types of payment card transactions (four-party credit and signature debit (such as MasterCard and Visa), PIN-debit, and three-party credit (such as 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 3 is the high degree of “P” and “H” cells 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 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 is settlement activities that involve posting credits and debits to financial institutions’ commercial and central bank accounts—here banks dominate.⁹ Virtually everywhere else, nonbank presence relative to banks is high, and, indeed, prevalent.

The message from Table 3 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.

⁸ An e-cheque is created when a written cheque is either truncated and becomes an ACH payment at some point of cheque processing or is used as a device to capture information to create an ACH payment at the point of transaction.

⁹ This also is a principal finding of Bradford, Davies, and Weiner (2003).

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.¹⁰

- *Liquidity and credit risks*: 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).
- *Settlement agent risk*: the risk of failure of the entity (settlement agent) whose assets are used to settle payment obligations. This is a specific form of credit risk.
- *Operational risk*: the risk that deficiencies in information systems, internal controls, human errors, or management failures will result in unexpected losses (internal and external events).

Recent discussions of operational risk in payments point to subcategories that have grown in importance:

- *Malfunctions and related problems*: malfunctions that are the result of unintentional circumstances or events (e.g. a computer breakdown or a processing slowdown, or organisational deficiencies) or intentional circumstances or events (such as attack or misuse of information or procedures).
- *Data security risk*: unauthorized modification, destruction, or disclosure of data used in transactions or used to support transactions. Payment data need to be secured to prevent illicit use and to protect privacy.

¹⁰ The definitions used in this section derive from various sources: for definitions of risks in the context of payments clearing and settlement (credit risk, liquidity risk, operational risk, settlement risk, and systemic risk) see CPSS (2003) and the glossary annexed to ECB (2007b). On various aspects of settlement risk, see also Basel Committee on Banking Supervision (2000). On risks concerning, more specifically, retail payments (e.g. fraud risk, risk of a system-wide impact and reputational risk) see ECB (2007a) and CCBS (Handbook No.8).

- *Counterfeit and associated fraud*: the risk of financial loss for one of the parties involved in a payment transaction arising from wrongful or criminal deception where either the identity of the payer cannot be easily ascertained or the payee does not have a legitimate claim on the payer. Traditionally, the crime of counterfeiting applies to paper money 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.¹¹

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. For payment instruments that involve the use of specific hardware (such as card readers), fraud risk is relevant if the hardware can be compromised or altered for illicit purposes (such as skimming or cloning of cards). Data security risk is relevant for all activities involving the storage and transit of payment 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.

- *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

¹¹ A cheque that bears a false signature or has been altered is properly called forgery. For our purposes, we include forgery with counterfeit risk.

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). 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.¹² 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.

- *Risk of illicit use*: the risk of penalties if the failure to comply with required guidelines to curb illicit use of payments is discovered. 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. 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. 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.

There are a number of additional risks that are a concern in payments but are excluded from extensive discussion for various reasons. Principal among these is systemic risk (the risk that the failure of one participant in a transfer system, or in financial markets generally, to meet

¹² 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.

its required obligations will cause other participants or financial institutions to be unable to meet their obligations when due). We say little about systemic because there is a widely held perception that it is well controlled in retail payment systems. We say little about settlement risk (the risk that settlement in a transfer system does not take place as expected), for similar reasons.¹³ Finally, we limit discussion of some other risk categories, such as reputational, legal, and system wide risk, because they are of a general nature and so are often present whenever a disruption or problem in the payment system arises.

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 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, financial institutions may become subject to legal risks (if the responsibilities of the parties are not sufficiently clear or legally

¹³ Settlement agent risk is a variation of settlement risk. We include settlement agent risk because settlement agents are used principally in retail payment systems.

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.

In this section we look at the vulnerability of certain payment activities to specific categories of risk by using a matrix representation (Table 4). 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 the matrix we show liquidity risk, credit risk, and settlement agent credit risk. The matrix highlights with a shaded 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.

Table 4: Payment Activities and Selected Risks

Payment Activity	Liquidity and Credit				Operational				Compliance	Illicit use (AML, terrorist financing)
	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	Data security risk associated with fraud or violations of privacy responsibilities			
Pre-Transaction										
1		x				x		x	x	x
	x					x		x		x
2		x			x					
					x					
					x				x	
3					x				x	
					x					
4					x				x	
					x					
					x					
					x					
5					x				x	
					x					
					x					
					x					
6					x				x	
					x					
					x					
7					x				x	
					x					
8					x				x	

Note: Data security risk is associated with the online environment.

Table 4: Payment Activities and Selected Risks (Cont.)

Payment Activity	Type of Risk									
	Liquidity and Credit				Operational			Counterfeit and associated fraud	Compliance	Illicit use (AML, terrorist financing)
	Liquidity	Credit	Settlement agent credit risk	Malfunctioning and/or other operational problems	Data security risk associated with fraud or violations of privacy responsibilities					
Pre-Transaction										
9	a				x			x		x
During-Transaction – Stage 1										
10	a				x			x		x
	b				x			x		x
	a				x			x		x
	b				x			x		x
11	c	x			x			x		x
	d	x			x			x		x
	a	x			x			x		x
	b				x			x		x
12	c				x			x		x
	a							x		x
	b							x		x
13	a							x		x
	a	x			x					
	a									
14	a									
	a									
	a									
15	a									
	a									
	a									
	a									
	a									
During-Transaction – Stage 2										
16	a				x			x		x
	b				x			x		x
	c				x			x		x
	d				x			x		x
	e				x			x		x

Note: Data security risk is associated with the online environment.

Table 4: Payment Activities and Selected Risks (Cont.)

Payment Activity	Liquidity and Credit					Operational					Compliance	Illicit use (AML, terrorist financing)	
	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	Type of Risk						
During-Transaction – Stage 2													
17	a				x				x				
	b				x				x				
	c				x				x				
	d				x				x				
18	a	x	x		x								
	b	x	x	x	x								
	c	x	x	x	x								
	d	x	x	x	x								
	e	x	x	x	x								
Post-Transaction													
19	a				x							x	
	b				x							x	
20	a				x				x			x	
21	a				x				x				
	a								x				
22	b												
	c								x				
	a								x				x
23	a								x			x	

Notes: Shading of table cells indicate activities and components of settlement risk. Data security risk is associated with the online environment.

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 payee has already withdrawn the credited funds. In general, prepaid payment instruments entail a credit risk for the holder of the instrument vis-à-vis the issuer (such as in case of prepaid 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 4 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 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.

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 it.

The next-to-last column of Table 4 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, PIN-debit, signature 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 PCI data security standard.¹⁴ The standard was revised in January 2005 and the payments industry is in a transition phase to the new standard. Merchants and payment processors that participate in a card network are responsible for complying 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 4 is for risk associated with illicit use of payments. For example, in the United States, payment providers are required to use reliable forms of identifying consumers when they provide payment services and banks must monitor accounts and file reports for suspicious activity.¹⁵ In Europe not only banks but also other parties are required by the Third Anti Money Laundering Directive to comply with obligations concerning customer due

¹⁴ The standards were developed as collaboration between American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International.

¹⁵ As required by the Bank Secrecy Act (1970) and the USA PATRIOT Act (2001).

diligence, reporting of suspicious transactions, record keeping and statistical data, and to take other supporting measures, such as ensuring the proper training of personnel and the establishment of appropriate internal preventive policies and procedures.¹⁶

In Table 4 we associate the various payment activities with liquidity, credit and settlement risks, with operational risk and its main subcategories, 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.¹⁷ 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.¹⁸ The key to understanding the prominence of operational risk is the shift of payments toward electronic forms. The payment activities and subactivities listed in the table are dominated by processes that facilitate or depend upon

¹⁶ 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.

¹⁷ This serves as a reminder that the purpose of Table 4 is to help identify where risk occurs in the many activities that underlie payments, not their severity.

¹⁸ This method of containing risk in 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 2008)

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 toward operational risk.

In the light of the above results, do nonbanks raise special risk considerations? We address this question in the next section.

4 Impact of nonbanks on risk

4.1 Changing risk profile

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. This has added to the prominence of data security risk, fraud risk and counterfeit risk for e-money.

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. Another reason is that the accounts used by banks to settle reciprocal payment obligations are accounts held either one-with-another (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 methods to initiate payments. 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 (U.S. Department of Justice 2002). Since this incident, PayPal has been successful at improving its data security and fraud detection systems (Cox 2001; Garver 2005).

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

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 do materialize, as shown by several recent examples.

In 2005, the U.S. company CardSystems, Inc. experienced a breach of its computer system that exposed 40 million transaction records 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 breach occurred at the large retailer group TJX, which operates over 2,000 stores in various countries, including the UK and Ireland. The breach exposed more than 90 million card account 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). 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 1,000 UK customers from a Delhi call centre worker, for GBP 4.25 each, saying that both cards credit numbers and account passwords were for sale (McKenna 2005).

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).

In addition to outsourcing, similar risks may arise when banks sell payments services to nonbanks. Banks mitigate this risk with know-your-customer practices that allow banks to detect attempts to exploit payment services and carry out illicit activities. An example of bank liability for improper monitoring of payment services provision to a nonbank customer was reported in

the United States in 2003, when the Federal Trade Commission issued press releases explaining how it had closed down several companies (the Assail Telemarketing Network and affiliates) that engaged in fraudulent telemarketing activities. Assail used the ACH services of First Premier Bank; the bank admitted that it had failed to perform due diligence on the activities and legitimacy of its customers (but it did supply information to the investigative agencies); the bank later paid \$200,000 in fines as part of a wider settlement and agreed to vigorously engage in know-your-customer actions and ongoing monitoring of customer activity (Iowa Attorney General 2005).

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 concentrate processing for an entire retail payments market segment. Under these circumstances, nonbank presence may have implications at the system level. While concentration is 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 (McPhail 2003). For example, the international credit card system relies on very few cards schemes. A major disruption at a key player may have the potential to impair the ability of millions of customers in several countries to make card payments.

The above discussion points out that nonbank access to payment systems may entail some risks. Furthermore, such risks may be exacerbated by the trend toward electronic payments, as electronic payment networks require a high degree of simultaneous coordination among all participants, with an increased need for cooperation 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 were originally 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 established transmission networks such as SWIFT.

Nonbanks also bring new technology and perspectives that can significantly contribute to reducing risk in the payments system. 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. In addition, cooperation of payment service providers with Internet providers is key to combating payment fraud via IT systems in terms of promptly shutting down fraudster web sites and phishing sites. In general the payments industry 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 online 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.

4.2 Risk management

Management of risk in retail payments depends highly on efforts of bank and nonbank participants in the payment system. But limitations of incentives to control payment risk leads to both industry self-regulation and government regulation. In general, available measures of retail

payment risk show that risk in retail payments is well-controlled, but there are significant limits to data on payment risk, especially regarding the role of nonbanks in payments.

Self-interest will lead both bank and nonbank providers of payments to limit risks that they can control within their organization. They will also be aware that some risks will affect them from outside of their organizations and may take extra precautions to protect themselves from such contingencies. But the interrelated nature of payment networks, and the exposure to outside threats that are very difficult to anticipate, implies that self-interest may not be sufficient to protect the payment system.

As a result, industry self-regulation is significant in the payments industry. These efforts are typically conducted at the network level where rules and requirements are set regarding standards that participants must meet regarding controls and management of operational, data security, and other risks. The fact that the PCI standards have been strengthened recently shows that these standards evolve in an effort to meet new risks as payment technology advances.

Because successful payment systems depend to a large extent on public confidence, there is also a public policy interest in the safe and smooth functioning of the payment system. In most countries this leads to some regulatory requirements that influence risk management in payments. Banks are at the center of the payment systems and bank supervisors do look at the payments activities of banks (and any payment processing subsidiary affiliated with the bank) to ensure controls over payment risk are in place.

Regulatory treatment of payments services for nonbank payment providers and processors can vary more widely across various countries. In the European Union, for example, front-end payment services provided by nonbanks vary significantly from country to country (EC 2003) and 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 institutions in another country.¹⁹ The recently adopted Payment Services Directive changes this differential treatment. The Directive opens the market by allowing actors other than banks and e-money institutions to provide payment services. These new “payment institutions” are entitled to provide the payment services listed in annex to the Directive (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.

Similarly, regulatory safeguards regarding outsourcing by other nonbank providers of payment services are not harmonized at the EU level, but they will be once the Payment Services Directive comes into force: the Directive prescribes information requirements to the competent authorities and sets conditions and limits for outsourcing of “important operational activities.”²⁰ The Directive also specifies that the authorities supervising the payment institutions would be entitled to carry out on-site inspections also with any entity to which payment services activities are outsourced.

Similarly, bank and nonbank regulations differ for payment participants in the United States. Supervisors will look to see that financial institutions comply with requirements to keep sensitive information secure.²¹ There is no similar requirement for nonbanks participants in payments, although the Federal Trade Commission has filled this gap by enforcing data security

¹⁹ Comparative tables of the national regimes in place in the various Member States are available at ec.europa.eu/internal_market/payments/framework/comparison_en.htm.

²⁰ 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 (Article 11).

²¹ As required by the Gramm-Leach-Bliley Act of 1999.

standards for retailers and other organizations.²² In general there is no prudential supervision of nonbank payment providers, but a handful of larger nonbank payment providers are examined by federal financial institution supervisors under a technology service provider supervision program.²³ The actual protection this program provides for the payment system is uncertain because its primary purpose is to protect banks, not the payment system. Moreover, many payment providers are not overseen because they are not in an outsourcing relationship with a bank.

The important public policy questions are whether the effort toward risk management by individuals, banks and other payment providers is sufficient and whether the mix of individual effort, industry self-regulation, and regulatory oversight is adequate in the face of a payments industry that is increasingly dependent on nonbank organizations. Unfortunately, comprehensive data that bears on these questions is thin and generally does not parse out the role of nonbanks. Anecdotal examples point to criminal attacks on an increasingly large scale through IT technology (Anderson and others 2008) or to nonbank responsibility for data breaches, but most analysts would say that the actual level of fraud is low. For example, according to Visa Europe Annual Report 2006, the fraud to sales ratio was only 0.069 percent of total POS spending.

The UK 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. The UK is also an important case study because it is the first country to adopt EVM payment cards, which provide a higher level of security by using computer chips to add encryption and other features to payment authorization. UK card issuers began the rollout of EMV cards and associated infrastructure in late 2003 and the year 2007 is the first complete year

²² Examples include the retailer DSW, the credit agency ChoicePoint, and software vendor Guidance Software.

²³ Sullivan (2007). At year end 2004, 87 payments processors were supervised, while news reports suggest that there are roughly 500 companies that process credit card payments (Dash 2005).

where all card payments had been required to be used in retail and ATM transactions. Total fraud losses in 2007 on cards issued by UK financial institutions are 6 percent higher than in 2004 but the mix of fraud from various sources as well as the distribution of losses in and out of the UK changed substantially over this time period (APACS 2008). Losses due to lost or stolen cards and card ID theft fell by 50.9 percent, reflecting the fact that the card requires a PIN. Fraud at UK retailers and ATMs both declined by large margins. The reduction in fraud on lost or stolen cards is a significant accomplishment and UK issuers achieved a major goal of EMV deployment.

There was, however, an increase of 92.6 percent in fraud losses on card-not-present transactions (phone, internet, and mail order). Surprisingly, losses due to counterfeit cards rose by 11.3 percent, despite the difficulty of counterfeiting a smart card. This happened because the UK EMV cards carry all the information necessary to make them backwards compatible with magnetic stripe cards. If criminals intercept this information, they can create a counterfeit magnetic stripe card for use in locations outside of the UK where they are still accepted. And in fact, fraud outside of the UK rose by 124.5 percent from 2004 to 2007.

The only systematic information on payment risk that allows a comparison of banks and nonbanks concerns data breaches in the United States. Data breaches are widely reported as a problem for payments and may serve as a measure of data security risk that could potentially lead to payments fraud. From January 2005 to April 2007, nearly 154 million records were compromised in 541 publicly reported data breaches.²⁴ Nonbank payment processors accounted for only 2.5 percent of all data breaches but 26.5 percent of compromised records. Banks and other financial service companies accounted for 9.4 percent of incidents and 4.1 percent of records compromised over the entire period. A large number of data breaches have occurred in

²⁴ Sullivan (2007), based on publicly disclosed data breaches listed by the Privacy Rights Clearinghouse (www.privacyrights.org/).

education, retail, health care, and government sectors. These four sectors together account for 77 percent of data breaches and 67.2 percent of records compromised in this particular period.

While conclusions are tentative, it appears that actual payments fraud is well contained. The UK experience shows how difficult it is to upgrade payment security standards because criminals adjust their efforts to exploit security weaknesses. And while analysis of data breaches show that payment security should involve all payment participants, the impact of data breaches on payments fraud appears limited at this time.

Insufficient incentives to manage risk in the payments system may contribute to payment risk. 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 payments 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 toward 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 payments 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 compliance 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 payments system. 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 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, with the ultimate cost, in terms of both financial cost and reputational damage, borne in many cases 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 toward 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

- Anderson, Ross, Rainer Böhme, Richard Clayton, and Tyler Moore. "Security Economics and European Policy," paper presented at the Workshop on the Economics of Information Security, March 1, 2008.
- APACS. "Fraud Abroad Pushes Up Losses on UK Cards Following Two-year Fall," press release, March 12, 2008. Available at www.apacs.org.uk/2007Fraudfiguresrelease.html#.
- Basel Committee on Banking Supervision. Principles for the Management of Credit Risk, Bank for International Settlement, 2000. Available at www.bis.org/publ/bcbs54.htm.
- Bradford, Terri, Matt Davies, and Stuart E. Weiner. Nonbanks in the Payments System, Federal Reserve Bank of Kansas City, 2003. Available at www.kansascityfed.org/publicat/psr/BksJournArticles/NonBankPaper.pdf.
- Braun, Michele, Jamie McAndrews, William Roberds, and Richard J. Sullivan. "The Economics of Managing Risks in Emerging Retail Payments," Federal Reserve Bank of New York Economic Policy Review, forthcoming 2008. Available at www.newyorkfed.org/research/epr/forthcoming/0711brau.pdf.
- Centre for Central Bank Studies. Bank of England, Payment Systems, Handbooks in Central Banking no. 8, 1996. Available at www.bankofengland.co.uk/education/ccbs/handbooks/pdf/ccbshb08.pdf.
- Committee on Payment and Settlement Systems. A Glossary of terms used in Payment and Settlement Systems, Bank for International Settlement, March 2003. Available at www.bis.org/publ/cps00b.htm.
- Cox, Paul. "PayPal and FBI Team Up," Wall Street Journal, June 22, 2001.
- Dash, Eric. "Take a Number," The New York Times, July 30, 2005.
- European Central Bank. Report on retail payment innovations 2005, Frankfurt am Main, Germany, 2005. Available at epso.intrasoft.lu/papers/Report-Retail-payment-innovations-2005.pdf.
- _____. Consultation announcement: oversight framework for card payment schemes, press release, and Draft oversight framework for card payment schemes, May 3, 2007a. Available at www.ecb.int/press/pr/date/2007/html/pr070503.en.html.
- _____. Blue Book 2007, Payments and Securities Settlement Systems in the European Union, August 2007b.
- European Central Bank Oversight Division and Federal Reserve Bank of Kansas City Payments System Research Function. "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, 2007a. Available at kansascityfed.org/econres/PSR/PSRConferences/2007/pdf/Rosati_Weiner.pdf.

- _____. "Nonbanks and Risk in Retail Payments," Working paper 07-02, Federal Reserve Bank of Kansas City, 2007b. Available at www.kc.frb.org/Econres/PSR/RWP/NonbanksRWP07-02.pdf.
- European Commission. "Comparative Tables of National Rules," 2003. Available at ec.europa.eu/internal_market/payments/framework/comparison_en.htm.
- _____. "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, 2006.
- Garver, Rob. "eBay and Banking: Is PayPal a Serious Rival?" *American Banker*, November 15, 2005.
- Iowa Attorney General. "First Premier Bank Agrees to Deny Automatic Withdrawal Services to Telemarketing Scams," July 6, 2005. Available at www.iowa.gov/government/ag/latest_news/releases/july_2005/First_Premier.html.
- Kerber, Ross. "Court filing in TJX breach doubles toll," *Boston Globe*, October 24, 2007. Available at www.boston.com/business/articles/2007/10/24/court_filing_in_tjx_breach_doubles_toll/
- Littas, R. "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, March 8–9, 2006. Available at ec.europa.eu/internal_market/payments/docs/fraud/taix_seminar/littas1st.pdf.
- Margerit, V. "The Payment Services Directive," *Banque de France Bulletin*, August 2007.
- Masi, Paola. "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, 2004.
- McKenna, B. "Credit card details in the clear and up for sale in India," *Network Security*, July 2005.
- McPhail, Kim. "Managing Operational Risk in Payment, Clearing, and Settlement Systems," Working Paper 2003-2, Department of Banking Operations, Bank of Canada, February 2003. Available at www.bankofcanada.ca/en/res/wp/2003/wp03-2.pdf.
- Sullivan, Richard J. "Risk Management and Nonbank Participation in the U.S. Retail Payments System," *Federal Reserve Bank of Kansas City Economic Review* (second quarter), 2007, pp. 5-40. Available at kansascityfed.org/PUBLICAT/ECONREV/PDF/2q07sull.pdf.
- U.S. Department of Justice. "Russian Computer Hacker Sentenced to Three Years in Prison," October 4, 2002. Available at www.cybercrime.gov/gorshkovSent.htm.
- Visa Europe. Annual Report 2006, released 2007.