

Lydian Payments Journal

Volume 1 | Issue 3 | January 2010



In This Issue	Lydian Payments Journal
<p>2 What is Changing? Age, Economic Crises, and Shifting Patterns of Card Use Ronald J Mann</p>	<p>The Lydian Payments Journal publishes articles from thought leaders across the globe on one of the most important industries in the world — payments, the industry which makes trade, the source of all economic prosperity, possible.</p>
<p>6 Payment Card Interchange Fees and Merchant Service Charges- An International Comparison Fumiko Hayashi</p>	<p>Titled after the Kingdom of Lydia, a region that is now part of eastern Turkey and which is attributed with inventing coinage in 600 BC, the Lydian Payments Journal shapes and chronicles this important sector by focusing on a spectrum of topics: from policy issues such as competition, consumer protection, and interchange to disruptive innovation such as social lending, remittance products, and mobile commerce.</p>
<p>23 Cooperation Models for the Development of Mobile Payment Solutions Marc Bourreau and Marianne Verdier</p>	<p>This e-journal leverages the power of the Web to provide germane and timely thought leadership to a broad and relevant audience. The online format also works to fuel interaction between readers and authors, extending the dialogue beyond just the articles. Visit the Lydian Payments Journal online at www.pymnts.com/journal.</p>
<p>31 PCIDSS and the Legal Framework for Securing: An Update on Recent Developments and Policy Directions Edward Morse and Vasant Raval</p>	

For information about contributing to The Pymnts Journal, please contact editorial@pymnts.com



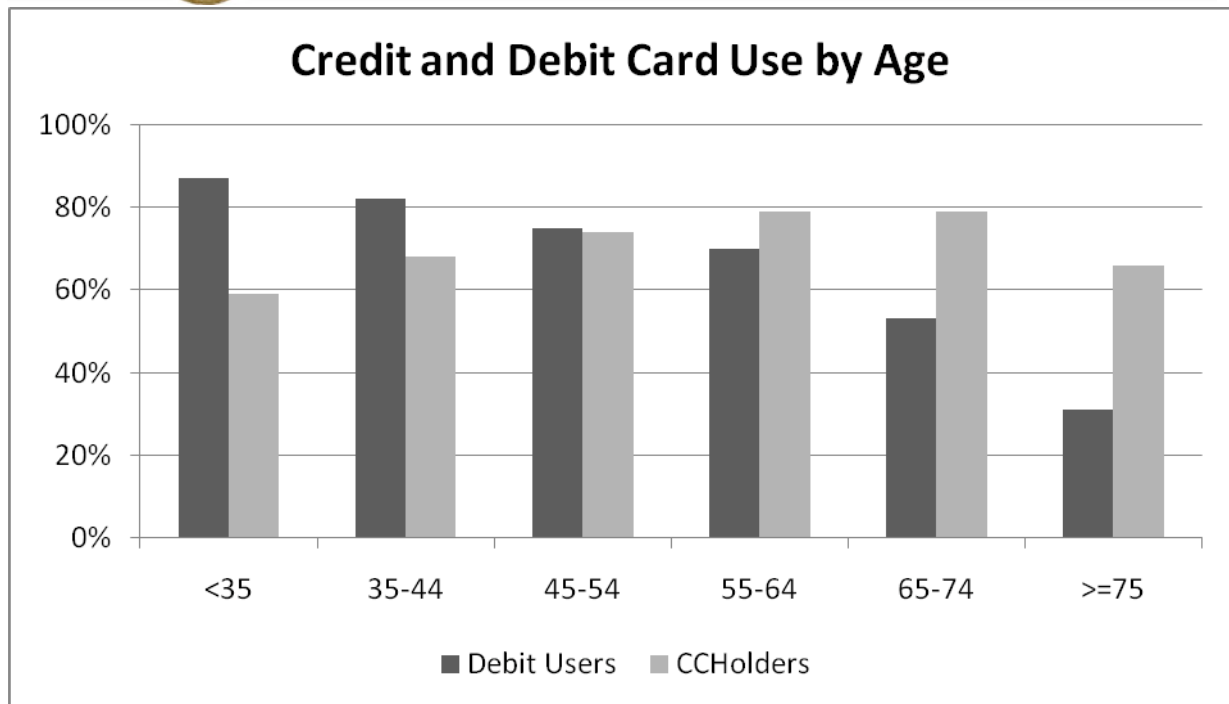
What is Changing? Age, Economic Crises, And Shifting Patterns of Card Use

Ronald J. Mann

Perhaps the most important long-term problem that the U.S. payments industry confronts is the possibility of a permanent shift away from credit card use. The last fifteen years have been characterized by routine use of credit cards as the dominant transaction vehicle, coupled with pervasive use of revolving credit to generate substantial interest revenues for the issuers sophisticated enough to remain competitive in that sector of the market. But the rapid growth of the debit card since the mid-1990s, accelerating in the last few years, has drawn the long-term stability of the credit card payment model into question. Will the debit card soon replace the credit card as the transaction vehicle of choice for American consumers? Or will the credit card instead return to prominence when the economy returns to normality in a few years?

On closer examination, the future of the credit card is an intriguing question. The problem is that the current decline of credit card spending rests on a combination of several effects, with distinct implications for the future of the product. It is useful to understand how those effects have worked together to alter usage patterns in recent years.

The most challenging issue relates to age. It is easy to see that routine credit card users are older than routine debit card users. For example, the figure below shows data from the Federal Reserve's 2007 Survey of Consumer Finance about how debit and credit card use change over the life course. As the figure displays, debit card use steadily declines with age, while credit card use rises through the life course to a peak at middle age and does not decline until cardholders reach 75 years of age.



One possibility is that the effect is generational: the high credit card users are the post-war Baby Boom generation, whose experience with the Great Depression was sufficiently remote to make a casual use of credit tolerable. A younger generation, observing the repeated economic crashes that resulted from the freewheeling behavior of their elders, might find routine credit more jarring. This perspective resonates with the reluctance of our parents and grandparents to carry revolving balances on credit cards: when you talk to people who remember the Great Depression, they have a deep aversion to debt, which they attribute to the scarring memories of the challenges of the 1930s.

An institutional parallel looks to the payments vehicles available at the maturity of different generations. When my generation first left home and took responsibility for separate household finances, the credit card was readily available but the debit card was not yet in any realistic way a practical choice. So another possibility is that the choice of a payment vehicle generally is made in youth and stays unchanged through the course of life; in that view, the earlier generation made the foolhardy choice of the credit card because it had no other available choice (except the check!).

Yet another possibility commonly suggested is that the effect is not generational, but age-related: perhaps debit cards are preferred by the young, while credit cards are preferred by the old. The 2007 data shown above cannot disprove this idea, because they show only a snapshot. It is difficult to reconcile, however, with the palpable aversion to credit cards shown by the Depression-era households. To me, it makes much more sense to view the current generation as consciously



rejecting the credit choices of their parents. They could use credit cards and not revolve, as their grandparents did, but in fact they seem to choose the safer precommitment strategy of avoiding credit cards entirely.

A second problem that confronts credit card issuers is the psychological effect of the current financial crisis. The discussion above suggests that the effects of the Great Depression left an entire generation reluctant to take the risks of easy credit, and that the rise of credit has coincided with the maturity of the first American generation that never experienced such a jarring event. If this story is true, how will the current crisis affect credit card usage? Will it cause a marked shift away from credit card usage as families seek “never again” to risk the exposure to calamity they faced in 2009? It is probably too soon to tell what the ultimate effect of this shift will be, but it is reasonable to expect a substantial shift toward products that emphasize consumer planning. The Blueprint products from JPMorgan Chase are exemplary.

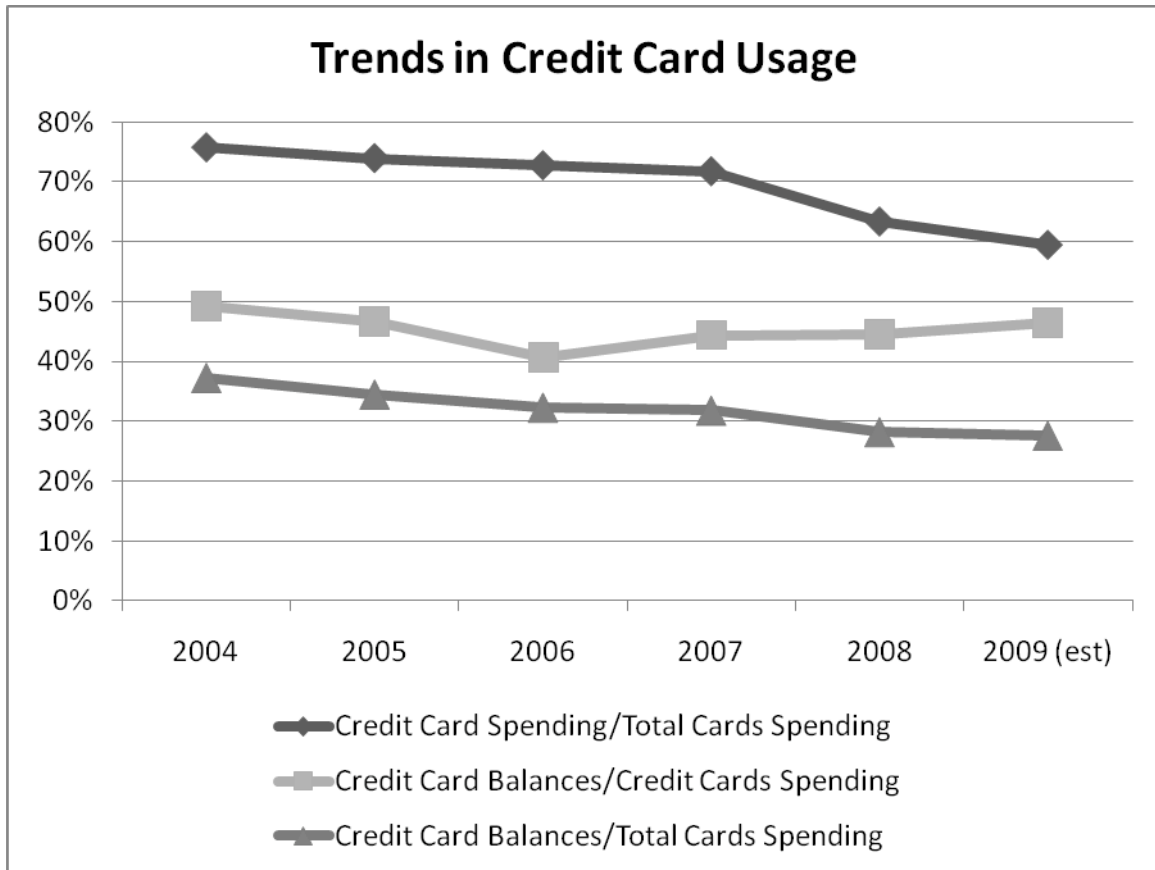
So what can data show us about these trends? For now, not as much as we would like. To understand the shifts well, we would need a longitudinal dataset that tracks particular households over time, to trace shifting patterns of payments use. Although nothing like that currently exists, the importance of payment cards to economic growth is motivating some important data-collection projects at places like the Boston Federal Reserve Board. For now, however, the most useful publicly available data comes from the Nilson Report.

The figure below uses Nilson Report data to show how credit card usage has been shifting over the last several years. The top line shows the ratio of credit card spending to overall payment card spending. Nothing about that line is surprising. It shows a steady decline in the share of spending on credit cards, accelerating since 2007, from 76% as recently as 2004 to only 59% during the first half of 2009. This is consistent with the received wisdom that credit card use is declining and also consistent with any of the explanations discussed above.

The second line shows the ratio of outstanding card balances to annual credit card spending – a simple metric useful for gauging the use of revolving credit on credit cards. This metric also was declining in the early part of the decade, but since 2006 it has been rising steadily, from 41% in 2006 to 47% during the first half of this year. Two explanations are apparent. One possibility is that those that are using credit cards have changed their behavior and begun to revolve more debt, not less. The more likely possibility, I think, is that the share of revolvers among credit card users is increasing as convenience users steadily abandon credit cards for debit cards. Under this explanation, those who use credit cards today are using them in much the same way as they did several years ago. It’s



just that the population is shifting over time to include a greater share of revolvers and a smaller share of convenience users.



The final line completes the story, showing the ratio of credit card balances to annual spending on all cards. This line, like the first one, shows a marked decline, losing about a quarter of its volume in the last five years (from 37% to 28%). This suggests that a shift of convenience users from credit cards to debit cards (which easily could explain the first two lines) is not the entire story. Here, I think, the most likely explanation is the generational one: a slow influx of new users, predominantly debit card users, is lowering the share of revolvers within the card industry as a whole, even as that share increases within the credit card sector standing alone.



Payment Card Interchange Fees and Merchant Service Charges – An International Comparison

Fumiko Hayashi¹

As payment cards have become an increasingly important electronic retail payment type in many countries, payment card fees, especially interchange fees, have become the source of a good deal of controversy. The interchange fee is used by card networks, such as MasterCard and Visa, to achieve a desired balance between merchants accepting and consumers holding and using their cards. Typically, merchants pay the interchange fee, which ultimately flows to the bank that issues the card the consumer uses. Recently, public authorities in many countries have intervened in or have initiated investigations in the payment card markets.² The United States is no exception. Congress is now considering bills regarding interchange fees and card networks' rules, such as no-surcharge rules and honor-all-cards rules, which impose contractual restrictions on merchants.

U.S. merchants are generally dissatisfied with the level at which the fee has been set. They argue that it does not make sense that the U.S. interchange fee is among the highest in the world despite the fact that the United States has the largest number of payment card transactions and the payment card industry exhibits economies of scale. They are also dissatisfied with the idea that the interchange fees fund payment card rewards received by some cardholders. Card networks respond to the argument by saying that although the U.S. interchange fee is among the highest, the total fee level on each transaction paid by merchants (i.e., the merchant service charge, hereafter MSC) is not necessarily higher. Overseas, merchants pay higher fees to acquirers and processors because acquirers assume more risk responsibility.³ Card networks also claim that the interchange fees are a

¹ Senior Economist, Federal Reserve Bank of Kansas City. E-mail: fumiko.hayashi@kc.frb.org. The views expressed in this article are those of the author and do not necessarily reflect those of the Federal Reserve Bank of Kansas City or the Federal Reserve System.

² Terri Bradford and Fumiko Hayashi, "Developments in Interchange Fees in the United States and Abroad," *Federal Reserve Bank of Kansas City Briefing*, April 2008.

³ Digital Transactions, "Merchants Urge That U.S. Follow Overseas Example on Interchange," *Digital Transaction News*, Sept. 17, 2009, available at <http://www.digitaltransactions.net/newsstory.cfm?newsid=2324>.



necessary tool to balance the merchants' card acceptance and the consumers' card adoption and usage.

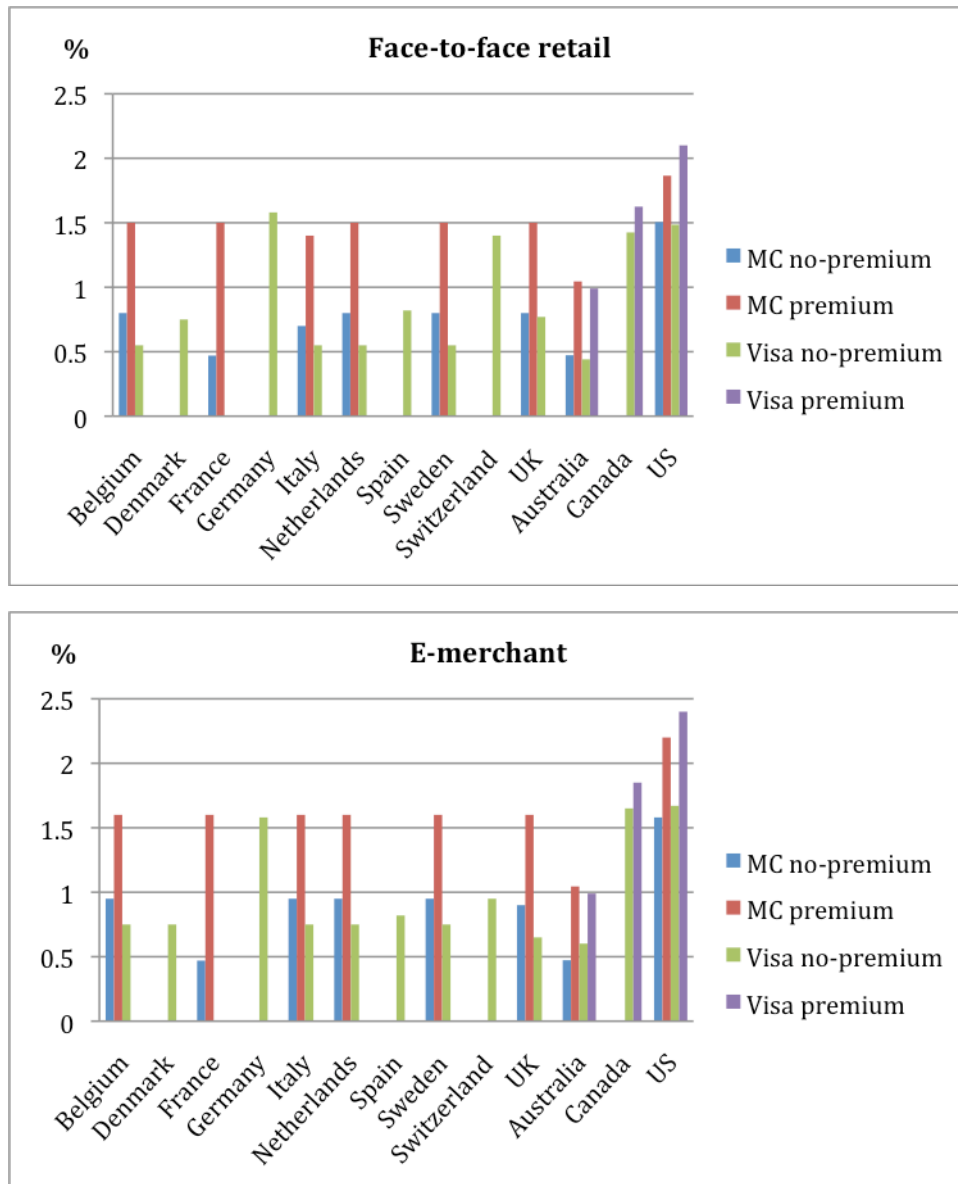
This article provides some empirical evidence in considering the arguments above. First, it compares interchange fees and MSCs for credit and debit cards in the United States and 12 other countries (Australia, Belgium, Canada, Denmark, France, Germany, Italy, the Netherlands, Spain, Sweden, Switzerland, and the United Kingdom) where the payment card industry is well established. Second, it discusses other factors that are important for interchange fee debate, including the total number of card transactions, cardholder fees, and card frauds.

Interchange Fee and MSC Comparison

Figure 1 compares credit card interchange fee rates (%) among 13 countries. The top panel shows interchange fee rates for face-to-face retail transactions, and the bottom panel shows those for e-merchant (i.e., online) transactions. In all countries where MasterCard interchange fee rates are reported in the figure, MasterCard interchange fee rates vary by reward features of the card. No-premium is the rate for the no- or the least-rewards cards and premium rate is for the highest-end rewards cards (World Signia in Europe, Premium in Australia, and World Elite in the U.S.). In contrast, according to the interchange fee schedules posted by Visa Europe, Visa does not have premium card interchange fees in all European countries where Visa interchange fee rates are reported in the figure. Visa sets different interchange fees for premium cards in Australia, Canada, and the United States.



Figure 1. Credit Card Interchange Fee Rates



Note: Spain, Canada, and the U.S. have multiple rates per category. The mid rate $(=(\text{lowest rate} + \text{highest rate})/2)$ is shown.

Sources: MasterCard and Visa

It is clear that the United States has the highest interchange fee rates among the 13 countries. The non-premium interchange fee rates in the U.S. are almost comparable to the premium interchange fee rates in Europe. Canada has the second highest interchange fee rates. The no-premium interchange fee rates in Canada are similar to those in the U.S., while the premium interchange fee rates in Canada are much lower than those in the U.S.



Another interesting finding from the figure is that e-merchants are not necessarily charged much higher interchange fees than face-to-face retailers. The interchange fee rate difference between e-merchants and face-to-face retailers is about 0.1% to 0.3%. It is considered that online transactions are much riskier than face-to-face (card present) transactions. Whether interchange fee rate differences reflect the risk differences between e-merchants and face-to-face retailers or differences among the 13 countries will be discussed later in this article.

Unlike credit card interchange fees, debit card interchange fees are difficult to compare across the 13 countries. As Table 1 presents, some schemes use fixed fees, and other schemes use proportional fees with or without a cap. Thus, ranking of the countries based on the debit card interchange fee levels varies depending on transaction value. In addition, in some countries, the domestic scheme is mainly used and the international schemes (MasterCard and Visa) are only used by foreigners. Thus, even if the international schemes set relatively high debit card interchange fee rates, the average debit card interchange fees the merchants actually pay may not be as high. Five countries (Belgium, Denmark, Germany, the Netherlands, and Canada) have a national debit card scheme with zero interchange fees. In Australia, interchange fees of EFTPOS, a national debit card scheme, are paid by card issuers to merchant acquirers. In Sweden, Switzerland, and the UK, MasterCard and Visa have replaced the domestic card scheme(s).

Table 1. Debit Card Interchange Fee Schedules (Face-to-Face Retail)

	Domestic scheme(s)	MasterCard	Visa
Belgium	0 EUR	0.056 EUR	0.26 EUR
Denmark	0 DKK	N/A	0.3% or 4 DKK
France*	0.21% + 0.1067 EUR + α	0.40% + 0.05 EUR	N/A
Germany	0 EUR	0.24% + 0.05 EUR	0.3% or 1.58%
Italy	N/A	0.35% + 0.05 EUR	0.26 EUR
Netherlands	0 EUR	0.40% + 0.05 EUR	0.26 EUR
Spain	N/A	N/A	0.24, 0.25, or 0.43 EUR
Sweden**	N/A	N/A	N/A
Switzerland**	N/A	0.40% + 0.05 EUR	0.26 EUR
UK**	N/A	0.08 GBP	0.08 GBP
Australia	-0.04 AUD	0.10 AUD	0.088 AUD



Canada	0 CAD	N/A	0.15% + 0.05 CAD
US***	0.55~0.75% + 0.05~0.15 USD	0.70~1.05% + 0.15 USD	0.62~1.03% + 0.13~0.15 USD

* α = risk associated for payment guarantee. Information on French domestic scheme interchange fee is from Judgment (Case A 318/02 Servired Interchange Fees) by the Spanish Competition Court. The document (in Spanish) is available at http://www.cncompetencia.es/Administracion/GestionDocumental/tabid/76/Default.aspx?EntryId=31216&Command=Core_Download&Method=attachment.

** In Sweden, Switzerland, and the UK, MasterCard and Visa have replaced the domestic scheme(s).
*** In the United States, MasterCard and Visa's rates are signature debit rates. Their PIN debit rates are considered as domestic schemes.

Sources: MasterCard, Visa, Reserve Bank of Australia, and *European Payment Cards Yearbook*.

The average debit card transaction value significantly varies by country (Table 2). The United States has the lowest value (\$39.11) among the 12 countries, followed by Canada. Switzerland has the highest value (\$134.91), which is more than three times higher than the United States.

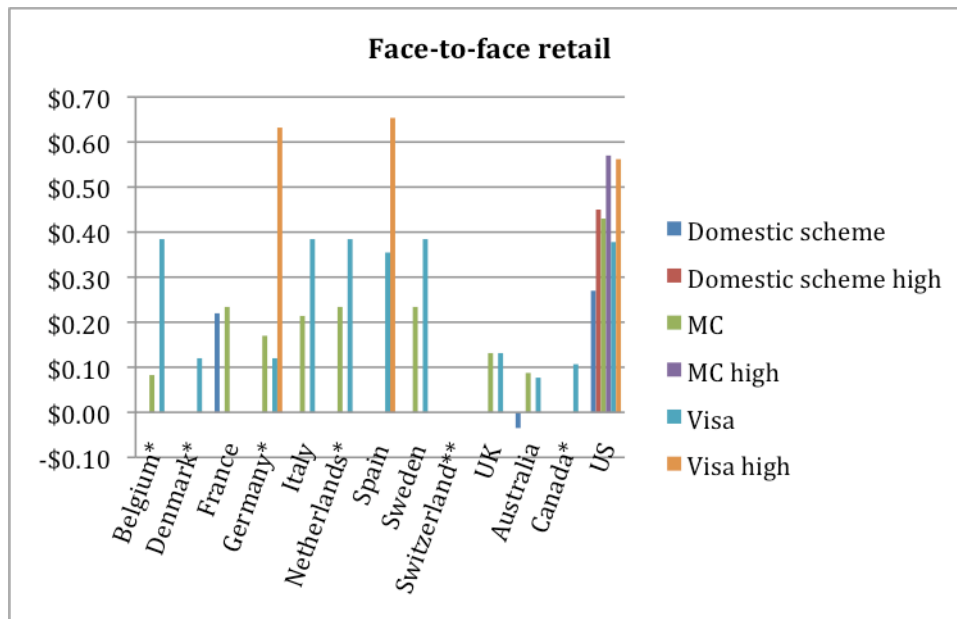
Table 2. Average Debit Card Transaction Value (2007)

	US\$ equivalent
Belgium	68.96
Denmark	74.36
France	N/A
Germany	88.35
Italy	126.98
Netherlands	59.26
Spain	68.01
Sweden	64.11
Switzerland	134.91
UK	91.27
Australia	60.20
Canada	42.33
US	39.11

Sources: Bank for International Settlements, European Central Bank, and Reserve Bank of Australia.



Figure 2. Debit Card Interchange Fees for a US\$40-equivalent Transaction



*The domestic debit scheme has zero interchange fees.

** In Switzerland, recently (March 25, 2009) the Competition Commission opened a preliminary investigation into Maestro’s introduction of an interchange fee. Maestro’s interchange fees in Switzerland are not available.

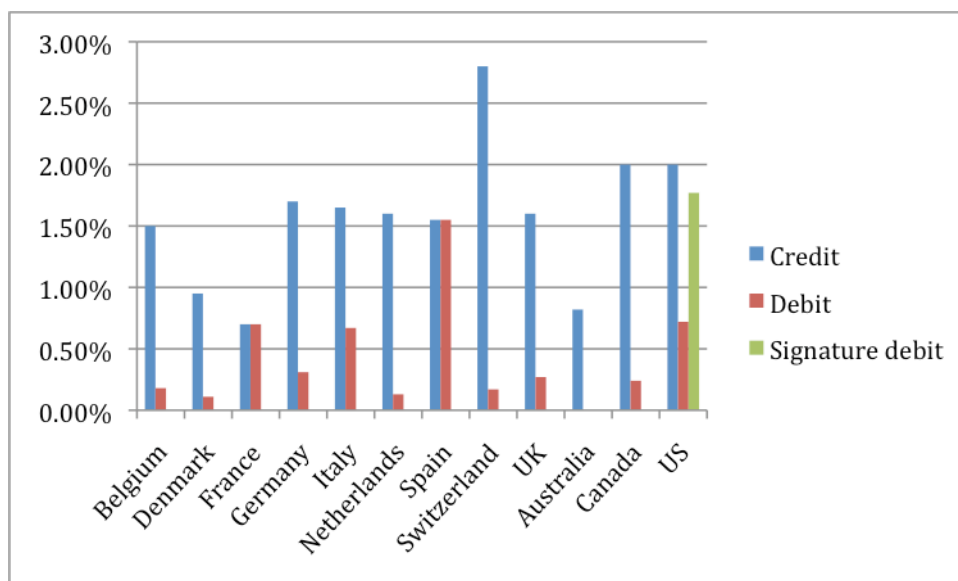
Figure 2 shows debit card interchange fees for a US\$40-equivalent transaction. In general, the United States has the highest debit card interchange fees. Two exceptions are Visa’s highest interchange fee rates in Germany and in Spain. In Germany, the interchange fee rate for V-Pay, Visa’s new European debit product based on EMV chip technology, is much lower (0.3%) compared with the interchange fee rate for a traditional immediate debit product (1.58%). In Spain, Visa’s interchange fee difference is based on merchant size. Merchants who generate the smallest transaction value (0-100 million euros) are charged the highest interchange fee (0.43 euros), while merchants who generate the highest transaction value (500 million euros or over) are charged the lowest interchange fee (0.24 euros).

In the United States, interchange fees for PIN debit transactions are generally lower than those for MasterCard and Visa’s signature debit card transactions. But, compared with PIN debit interchange fees in the other countries, the U.S. PIN debit interchange fees are higher.



Figures 1 and 2 provide evidence that the United States has the highest interchange fees for both credit and debit cards among the 13 countries, where adoption and usage of payment cards are well advanced. Does the United States have the highest MSCs among these 13 countries? Figure 3 compares MSC rates across 12 countries (Sweden’s data is not available). The MSC includes fees paid to the acquirer, to the network, and to the issuer. Switzerland’s credit card MSC rate is the highest (2.8%), but the rate does not fully reflect the interchange fee regulation that was implemented in Switzerland in 2005.⁴ Following Switzerland, Canada and the U.S. have the second highest MSC rate for credit cards (2%). For debit cards, the MSC rate for the U.S. signature debits is the highest, followed by Spain. The third place is shared among the U.S. PIN debit, France, and Italy. Thus, U.S. merchants may not pay the highest MSC rates but they likely pay the second highest MSC rates for both credit and debit cards among the 12 countries.

Figure 3. Merchant Service Charge Rates



Notes: All figures are 2006, except for Denmark (2004), Australia (2009), and the U.S. (2008). Australia’s debit card rate may potentially be negative, because EFTPOS interchange fees received by acquirers are shared with major merchants. The U.S credit card rate is MasterCard and Visa only. Sources: Peter Jones and Chris Jones, “Explaining Differing European MCS Levels,” *Papeles de Economia Espanola*, (2006); Reserve Bank of Australia; Carlos Arango and Varya Taylor, “Merchants’ Costs of Accepting Means of Payment: Is Cash the Least Costly?” *Bank of Canada Review* (Winter

⁴ In December 2005, the agreement was reached between the Swiss Competition Commission and credit card issuers to reduce credit card interchange fees from 1.65-1.70% to 1.30-1.35% within the next three years.



2008-2009); The Nilson Report, "Merchant Processing Fees," 936 (October 2009). For this figure, the author estimated the signature debit MSC rate, based on Visa and MasterCard's PIN and signature debit shares; Jeremy Dixon, "Credit Crunch: Dispute Over Interchange Fees Rages On," *YCM* (March/April 2009), available at http://www.conveniencecentral.ca/200903/pdf/Credit_Crunch.pdf.

Factors that Affect Interchange Fees and MSCs

Economies of Scale and Card Network Competition

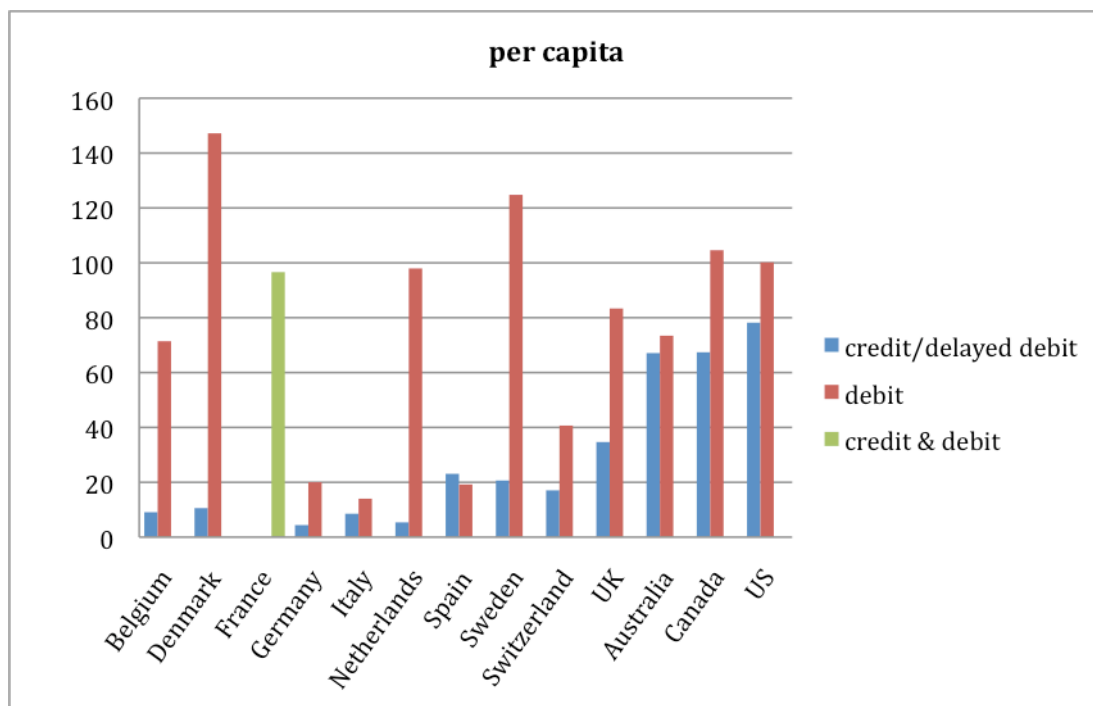
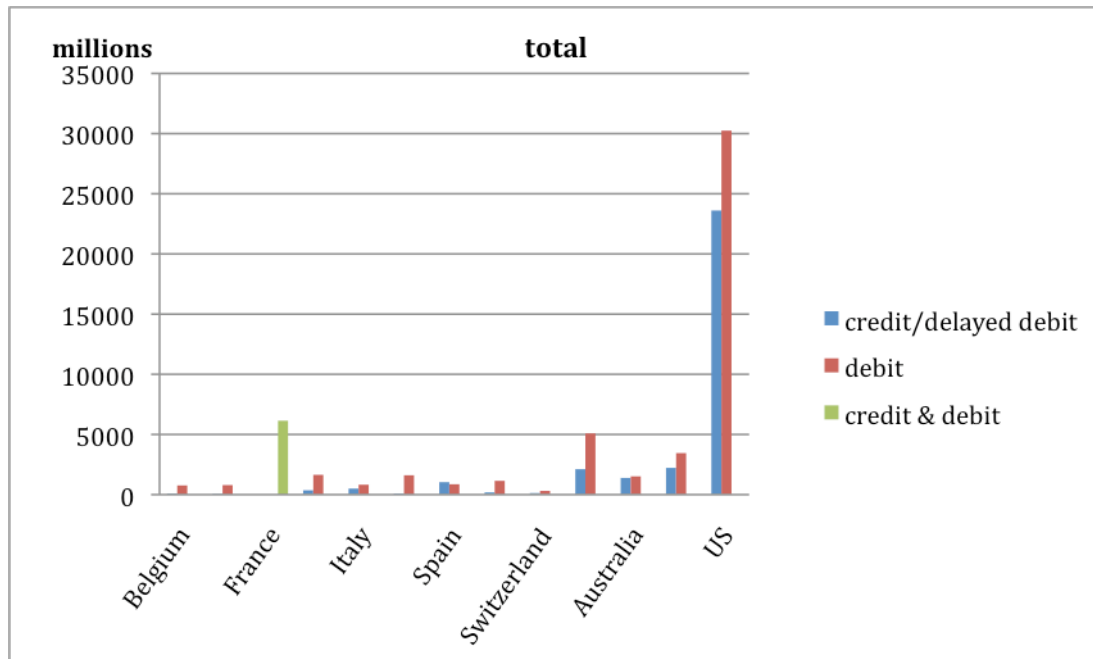
U.S. merchants question why U.S. interchange fees are among the highest in the world despite the fact that the U.S. has the largest number of card transactions. As the top panel of Figure 4 shows, the United States has the largest number of transactions for both credit and debit cards. The number of U.S. card transactions is about 7.5 times greater than that of the second largest country, the UK. Switzerland has the smallest number of transactions – less than 1% of the U.S. card transactions. The second panel shows the number of credit and debit card transactions per capita. Again, the U.S. has the largest number of credit card transactions per capita. In contrast, in terms of the number of debit card transactions per capita, the U.S. is fourth among the 13 countries.

Although the numbers of card networks, processors, acquirers, and card issuers in the U.S. are larger than those in any other countries, each U.S. player, especially a larger one, is likely processing enough transaction volume to take advantage of economies of scale. Thus, if the fundamentals of card transactions, such as transaction processing and clearing technologies and risks are the same across these 13 countries, each card transaction in the U.S. should not require more resources than a transaction in any other country.⁵

⁵ Jones and Jones (2006) listed factors that explain the differences in Europe's MSC rates. Those include service packages provided by acquirers (e.g., only telecommunication services or other services, such as terminal and terminal maintenance), settlement periods, and different cross-border/intra-European transaction flows.



Figure 4. The Number of Payment Card Transactions (2007)



Sources: Bank for International Settlements, European Central Bank, and Reserve Bank of Australia.

However, this does not necessarily imply that interchange fees or MSCs in the U.S. should be as low as those in other countries. Literature on two-sided markets suggests that if card service providers



(i.e., card networks, acquirers, and card issuers) do not have market power, then the sum of the two fees – one is paid by merchants and one is paid by cardholders – should be close to the cost.⁶ Thus, the higher interchange fees or merchant service charges do not necessarily result from the market power of card service providers; rather they might imply lower cardholder fees.

Cardholder Fees

Despite the importance of cardholder fees for efficiency of the payment card markets, information on cardholder fees is not well documented. This is partly because the cardholder fee structure is more complex than the merchant fee structure. For credit cards, an annual fee is typically charged by card issuers (Canada and the U.S. are exceptions); per transaction fee is very rare, but a negative per-transaction fee, i.e., rewards, is given for some transactions. For debit cards, in some cases, a per-transaction fee is assessed (e.g., PIN fee in the U.S.) or a negative per-transaction fee is given (e.g., some signature debit transactions in the U.S.). In another case, debit card transactions are free until a certain number of transactions per month. In other cases, debit card transactions are free but cardholders may need to pay a monthly fee to maintain the account. Tables 3 and 4 summarize cardholder fees in Europe, Australia, Canada, and the United States.

Table 3. Credit Card Cardholder Fees

	Per card	Per transaction	Others
Europe (2004)	24 euros* – annual average for 23 EU Member States.	No per transaction fee is charged in 19 of the 25 countries. In six countries, the fee varies from 0.1% to 0.7% of the transaction value.	In 20 countries, card issuance fee is charged. The average fee is 14 euros.*
Australia (2009)	AU\$85 for standard card and AU\$140 for gold rewards card annual fee.	Per transaction fee is not charged. The reward value is, on average, 0.59% of transaction value.	
Canada	No annual fees for some cards,		

⁶ See, for example, Sujit Chakravorti, “Externalities in Payment Card Networks: Theory and Evidence,” (presented at *The Changing Retail Payments Landscape: What Role for Central Banks?* Federal Reserve Bank of Kansas City International Payments Conference, Kansas City, MO, November 2009), available at <http://www.kansascityfed.org/econres/psr/psrconferences/2009/pdf/Chakravorti.10.30.09.pdf>.



(2009)	even for rewards cards.*		
US (2005)	About 87% of general purpose credit cards held by consumers do not charge annual fees. About 15% of co-branded rewards cards charge annual fees, but the majority of annual fees** are less than \$100.	Per transaction fee is not charged. The reward value is, on average, 1% of transaction value.	

* Only for MasterCard and Visa.

**Only for Discover, MasterCard, and Visa. The author visited top 10 U.S. credit card issuers' websites to check the annual fees charged by those issuers in October, 2009.

Sources: European Commission Directorate-General for Competition, "Report on the Retail Banking Sector Inquiry," Commission Staff Working Document, January 31, 2007; Reserve Bank of Australia, Payment System Board, Annual Report 2009; Visa Research Services, "2005 Payment Method Factbook: Visa Payment Panel Study."

Table 4. Debit Card Cardholder Fees

	Per card	Per transaction	Others
Europe (2004)	Annualized fees per card are, on average, 10 euros for MasterCard, 11 euros for Visa, and 9 euros for domestic schemes.	No per transaction fee is charged in 17 of the 25 countries. ⁷ In eight countries, the fee varies from 0.1% to 0.75% of the transaction value.	In 13 countries, card issuance fee is charged. The average fee is 6 euros.
Australia (2009)	A flat account-keeping fee of around AU\$4 per month.	An unlimited number of free electronic transactions, including EFTPOS and scheme debit.	
Canada (2004)	The majority of accounts provided by the largest Canadian Banks charge a monthly account fee, ranging from Can\$3.5 to Can\$35.	After a certain number of free transactions (10 to unlimited, depending on the account), a per-transaction fee is charged for debit transactions. The fee ranges from Can\$0.5 to Can\$0.6.	
US (2008)	The majority of accounts can avoid monthly fees if they carry more than the minimum balance. For noninterest checking accounts, the minimum balance is \$483.75 and the monthly fee is \$1.93, on average. For interest-bearing accounts, the minimum is \$3462 and the monthly fee is	Only 0.6% of cardholders are affected by a PIN fee, a per transaction fee charged for PIN-based debit transactions. The fee is averaged \$0.53. About 50% of card issuers offer debit rewards programs. The value of rewards is 0.25% of the transaction value.	The average overdraft (or nonsufficient fund) fee is \$28.95. Multiple overdraft fees can be charged in a day or a month.

⁷ Per-transaction fees are uncommon in Belgium, Denmark, France, the Netherlands, and Sweden, and the UK.



	\$11.97, on average.		
--	----------------------	--	--

Sources: European Commission Directorate-General for Competition, “Report on the Retail Banking Sector Inquiry,” Commission Staff Working Document, January 31, 2007; Reserve Bank of Australia, Payment System Board, Annual Report 2009; Dove Consulting, “Debit in Canada: An Overview of the Canadian Debit System and Comparison with the U.S. Model,” (February 2004) (This white paper was prepared by Dove Consulting and commissioned by Pulse EFT Association.); Laura Bruce, “2008 Checking Study: Banking Fees Continue to Soar,” Bankrate.com, October 27, 2008, available at <http://www.bankrate.com/brm/news/chk/chkstudy/20081027-checking-study-a1.asp>; Oliver Wyman, Pulse EFT Network, “2008 Debit Issuer Study,” April, 2008 (detailed summary available at http://findarticles.com/p/articles/mi_m0EIN/is_2008_April_29/ai_n25361372/?tag=content;col1) and “2009 Debit Issuer Study,” June, 2009 (news release available at https://www.pulsenetwork.com/public/upload/storage/file250/file/2009-Debit_Issuer_Study_Release.pdf).

U.S. cardholders likely pay lower cardholder fees or receive higher levels of rewards than cardholders in the other countries. In the United States, fixed fees (i.e., annual credit card fees and monthly checking account fees) are not very common for both credit and debit cards. Although some banks charge a per-transaction fee for PIN-based debit card transactions, only a small percentage (0.6%) of cardholders are affected by such a fee.⁸ U.S. cardholders receive rewards for their use of credit cards and (signature-based) debit cards. In contrast, fixed fees are common outside the United States (except Canada for credit cards). Generally, per transaction fees are not used in Europe and Australia. In Canada, cardholders pay a per-transaction fee for some debit card transactions. Credit card rewards are provided in Europe, Australia, and Canada, but details, such as the average levels of rewards and what percentage of transaction value/volume are made by reward cards, are not well documented. In general, debit card rewards are not provided outside the United States.

Do the lower cardholder fees in the U.S. offset the higher merchant fees? In other words, is the sum of the cardholder fee and merchant fee lower in the U.S.? For debit cards, the sum of the two fees is likely the highest in the United States;⁹ while for credit cards, the sum of the two fees in the U.S.

⁸ Pulse EFT Network, “2009 Debit Issuer Study.”

⁹ Even if the U.S. signature debit cards provide rewards of 0.25% of the transaction value on average, the sum of the two fees is still around 1.5%, while for the U.S. PIN debit, the sum of the two fees is around 0.7%.



might be lower than that in some European countries.¹⁰ Interestingly, the sum of the two fees for credit cards is still higher than that for PIN debit cards in the United States.

Unless significant technological inefficiencies or fraud risks exist in the U.S. debit card markets, or debit cards are profit-losing businesses in some other countries, the higher sum of the two fees for the U.S. debit cards may suggest some market power of the U.S. debit card service providers.

In contrast to debit cards, it is difficult to interpret the sum of the two fees for the U.S. credit cards. It is possible that the U.S. credit card service providers have some market power. The lower sum of the two fees for the U.S. credit cards than that of some European countries' credit cards may imply that the U.S. credit card service providers take advantage of significant economies of scale but they may still earn a profit margin. It is also possible that the U.S. credit card service providers have less market power. The higher sum of the two fees for the U.S. credit cards than for the U.S. (PIN) debit cards may simply imply credit cards require many more resources than (PIN) debit cards.¹¹

Even if the sum of the two fees for the U.S. credit cards is close to the resource costs, this does not necessarily imply that the U.S. credit card market is efficient. As two-sided markets literature suggests, efficiency also depends on the fee structure – how to split the total fees between merchants and cardholders. Thus, too much transfer to credit card cardholders through rewards

¹⁰ If U.S. credit cards provide rewards of 1% of the transaction value on average, then the sum of the two fees is around 1%, which is lower than credit card MSCs in some European countries.

¹¹ Cost studies conducted by the central banks of Australia, Belgium, the Netherlands, Norway, and Sweden found that a credit card transaction uses more resources than a debit card transaction. Hans Brits and Carlo Winder, "Payments are No Free Lunch," *De Nederlandsche Bank Occasional Studies*, 3(2), 2005, available at http://www.dnb.nl/binaries/Occstud32%20web_tcm46-146645.pdf; National Bank of Belgium, "Costs, Advantages and Drawbacks of the Various Means of Payment," *National Bank of Belgium Economic Review*, (2006): 41-47, available at http://www.nbb.be/doc/TS/Publications/EconomicReview/2006/ecorevI2006_H3.pdf; Mats Bergman, Gabriella Guibourg, and Bjorn Segendorf, "The Costs of Paying – Private and Social Costs of Cash and Card," Sveriges Riksbank Working Paper Series 212, September, 2007, available at http://www.riksbank.se/upload/Dokument_riksbank/Kat_publicerat/WorkingPapers/WP212.pdf; Carl Schwartz, Justin Fabo, Owen Baily, and Louise Carter, "Payment Costs in Australia," *Proceedings of Payments System Review Conference November 29, 2007*, Reserve Bank of Australia, pp. 88-138, available at <http://www.rba.gov.au/payments-system/resources/publications/payments-au/paymts-sys-rev-conf/2007/7-payment-costs.pdf>; Olaf Gresvik and Harald Haare, "Costs in the Payment System," *Norges Bank, Economic Bulletin* 80 (2009): 16-27, available at <http://www.norges-bank.no/upload/76227/costs%20in%20the%20payment%20system.pdf>.



programs might cause inefficiency, especially when a credit card transaction requires more resources than a transaction using other payment methods, such as PIN debit cards.¹² Also, if the transfer is made to very limited group of consumers – for instance, if the majority of rewards are received by high income earners – then the fee structure may potentially create a redistributive issue.

Frauds

Fraud risk is another factor that likely affects interchange fees and MSCs. It is more likely that not just fraud losses but also costs for fraud prevention and detection affect interchange fees and MSCs. It is difficult to pin down the exact costs associated with payment card fraud, especially the fraud prevention and detection costs. Statistics on payment card fraud losses are becoming available in many countries, while only fraud losses for card issuers are available in the United States (Table 5).

The fraud loss rate varies by country. Italy has the highest loss rate (22 basis points), followed by the UK (10.1 basis points). Five countries listed in the table (Belgium, Netherlands, Spain, Sweden, and Australia) have *total* loss rates that are lower than *card issuers'* loss rate in the United States (5.0 basis points). In some countries, more detailed statistics are available. For example, fraud loss rates for credit versus debit are available in Australia, Netherlands and the UK; in these countries, the loss rate for debit is much smaller – debit loss rates are about one-fifth (Australia), one-eighth (Netherlands) and one-third (UK) of credit loss rates. Types of transactions, such as card-present versus card-not-present and domestic versus international, also affect fraud loss rates. In France, the domestic loss rate on face-to-face and unattended payment terminal automatic payments was 1.5 basis points, while the domestic loss rate on payments at a distance (online, mail, and telephone

¹² More costly payment methods do not necessarily imply they are less efficient, if those payment methods generate more benefits to society than less costly payment methods. Efficiency should be measured by net benefit (i.e., benefits minus costs).



order) was 25.2 basis points, and international loss rates were much higher across all types of card transactions in 2008.¹³

Table 5. Fraud Loss Rates

(unit: basis point)

	Total loss	Issuer loss	Note
Belgium (2004)	2.0		debit cards with chip & PIN
Denmark	N/A	N/A	
France (2008)	5.6		domestically issued cards
Germany	N/A	N/A	
Italy (2007)	22		credit card only
Netherlands (2008)	4.5		domestically issued cards
Spain (2008)	2.5		domestically issued cards
Sweden (2008)	3.0		domestically issued cards
Switzerland	N/A	N/A	
UK (2008)	10.1		domestically issued cards
Australia (2008)	3.2		credit and debit cards
Canada (2008)	6.2		debit card only
US (2006)	N/A	5.0	credit and debit cards

Sources: Phillip Myers, “Getting a Fair Deal on Card Payments in the Chip and PIN Era,” European Retail Round Table (presentation at FMI Market Techniques, Washington D.C., February 15, 2005), available at http://www.fmi.org/facts_figs/conference_pdfs/Retail_Payments_Trends_1.pdf; Welch (2009); ACI Worldwide, “Stopping Card Fraud in its Tracks” (2009), available at <http://www.aciworldwide.com/downloads/CardFraudGuide.pdf>; Visa Europe, “Payment Security Report Sweden” (2009), available at http://www.visa.se/press/payment_security_report_sweden.pdf; Australian Payments Clearing Association, “Fraud Perpetrated on Australian Issued Payment Instruments,” available at http://www.apca.com.au/Public/apca01_live.nsf/WebPageDisplay/FraudStats_2009A_Summary?openDocument; Interac, “2008 Statistics,” available at <http://www.interac.ca/media/stats.php>; The Nilson Report, “Credit Card Fraud – U.S.,” 876 (March, 2007); Pulse EFT Network (2008).

Generally, information on how the fraud losses are shared among payment card industry participants – consumers, merchants, and card service providers (card issuers, card networks and acquirers) – is not available. An exception is France. In France, the fraud losses are distributed across cardholders (2.6%), merchants (53.5%), and issuers and acquirers (43.9%).¹⁴

¹³ Peter Welch, “Inside Fraud,” (supplement), *Payments Card & Mobile* (October 2009), available at http://www.paymentscardsandmobile.com/issues/PCM_FRAUD_Supplement_1109.pdf.

¹⁴ Observatory for Payment Card Security, “2008 Annual Report of the Observatory for Payment Card Security,” (2008), available at http://www.banque-france.fr/observatoire/telechar/gb/2008/rapport_an_2008_gb.pdf.



Although the fraud loss rates vary by country, by card type (credit vs. debit), and by transaction type, fraud losses may only explain a very small portion of interchange fees or MSCs. It is quite possible that card issuers, networks, and acquirers spend tremendous amounts on preventing and detecting payment card frauds. However, due to a lack of data, whether these costs explain a large portion of interchange fees or MSCs is not known. According to Sullivan (2008), U.S. banks spent an estimated \$3.1 billion to prevent payments fraud in 2006.¹⁵ The amount is equivalent to 0.1% (or 10 basis points) of payment card transaction value in the U.S. in 2006.¹⁶

Summary

This article first made international comparisons of interchange fees and MSCs and then discussed the factors that likely affect interchange fees and MSCs. Overall, the U.S. merchants pay higher interchange fees and MSCs for credit and debit card transactions than their counterparts in the other 12 countries considered in this article. However, U.S. cardholders likely pay lower cardholder fees or receive higher levels of rewards than their counterparts. The sum of the two fees – the merchant fee and cardholder fee (which can be negative to reflect rewards) – is likely the highest in the U.S. for debit cards, while for credit cards, the sum of the two fees in the U.S. might be lower than that in some European countries. Nevertheless, the sum of the two fees in the U.S. for credit cards is still higher than that for PIN-debit cards. Given the volume of card transactions in the U.S., this higher sum of the two fees for debit cards may imply higher markups for the U.S. debit card issuers, card networks, or acquirers, unless technological inefficiencies or higher fraud risks exist in the U.S. A potentially lower sum of the two fees for the U.S. credit cards than that for some European countries' credit cards may not necessarily imply efficiency of the U.S. credit cards; the U.S. credit card fee structure – higher merchant fees and negative cardholder fees – may potentially create

¹⁵ Richard Sullivan, "Can Smart Cards Reduce Payments Fraud and Identity Theft?" *Federal Reserve Bank of Kansas City Economic Review* (3rd quarter, 2008). A part of this \$3.1 billion may be used for preventing frauds of other payment methods, such as checks and ACH.

¹⁶ Merchants also incur costs associated with fraud prevention. The costs for merchants to comply with Payment Card Industry Data Security Standards (PCI DSS) were estimated from \$2.6 billion to \$5.5 billion in 2006. Sullivan, "Can Smart Cards Reduce Payments" (2008).



inefficiency in the U.S. payments system. Due to the lack of data on costs for fraud prevention and detection incurred by card service providers, whether fraud risks explain interchange fees and MSCs is still unanswered, but fraud losses may explain only a small portion of interchange fees and MSCs.



Cooperation Models for the Development of Mobile Payment Solutions

Marc Bourreau¹⁷ and Marianne Verdier¹⁸

Introduction

The technological advances in the field of near-field contactless communications (NFC) and the development of sophisticated mobile applications have enabled mobile phones to become a potential means of payment. In 2009, more than two-thirds of the population worldwide was equipped with a mobile phone.¹⁹ In developed countries, where the market for mobile telephony is mature, mobile payments are seen as a potential source of revenue by mobile operators, who are trying to diversify their services. In developing countries, where mobile telephony is also widely adopted, mobile payments are seen by the governments as an opportunity to improve access to banking services for the unbanked population. Overall, according to a study from Arthur D. Little, so-called “mobile payments” will represent a transaction volume of \$250 billion in 2012.²⁰ The growing importance of remittances also builds a case for the development of mobile payments. According to the World Bank, the market for remittances totaled \$433 billion in 2008.²¹ Remittances are money transfers made by migrant workers, who send a part of their revenue to their family or their acquaintances in their country of origin. They are mainly person-to-person money transfers, from developed countries to emerging countries, which can be processed through mobile networks or through traditional financial institutions such as Western Union.

However, though mobile payments have attracted a lot of attention, they have so far developed slowly, except in a few countries. For instance, the success of NTT DoCoMo, which launched a contactless payment solution in Japan, is often cited as prime example of the potential upheaval that mobile phones can create in the payments landscape of developed countries. The

¹⁷ Telecom ParisTech, Paris, France.

¹⁸ EconomiX, Université Paris Ouest La Défense, France.

¹⁹ International Telecommunication Union, “The World in 2009: ICT Facts and Figures,” 2009, available at http://www.itu.int/net/TELECOM/World/2009/newsroom/pdf/stats_ict200910.pdf

²⁰ Arthur D. Little, “Global M-Payment Report Update – 2009,” available at <http://www.adl.com/reports.html?view=389>.

²¹ Development Prospects Group, World Bank, “Migration and Development Brief 11,” (November 3, 2009), available at <http://siteresources.worldbank.org/>.



launch of the M-Pesa service by Vodafone in Kenya, which reached a total of 7.5 million subscribers in 2009, has also generated hopes to reduce financial exclusion in developing countries. However, a close analysis of these cases reveals that success stories cannot be easily generalized. The failure of the solution developed by Postfinance in Switzerland and the slow development of M-Pesa in Tanzania demonstrate that several ingredients are needed for mobile payments to succeed: standardization, incentives for consumers and merchants to adopt, and incentives for banks and mobile network operators to invest in the technology. In developed countries, the absence of these factors is often cited to account for the slow development of mobile payments.

In this paper, we examine the case of mobile payments in developed countries, as incentives to adopt mobile payment solutions seem to be fairly different in developing countries, and therefore we believe it would require a separate analysis. We propose to study the cooperation models for the development of mobile payment solutions. Do the players (banks, MNOs, nonbanks) have incentives to cooperate? What could happen if they decide to compete to provide mobile payment solutions? First, we start by defining mobile payments. Then, we analyze the potential path of development for mobile payment solutions. Afterwards, we study the various cooperation models between the players that are involved in mobile payments. Finally, we address the regulatory issues.

Definition of Mobile Payments

Mobile payments are generally defined as the process of two parties exchanging money using a mobile device in return for goods and services.²² This definition has the advantage of being simple enough to capture a wide array of technological possibilities. For instance, the mobile device can either be a mobile phone, a computer, a PDA, or even a wireless sticker that can be attached to any object, such as a ring or a key. The transaction can either be remote (SMS-based for instance) or processed locally via contactless technologies such as Near Field Communication or RFID. However, this definition may be potentially confusing, as the mobile device is not necessarily a means of payment. For instance, Vodafone in the United Kingdom has developed a payment solution that uses mobile phones to initiate and authenticate card payments. The purchases are charged directly to the payment cards of the users who have preregistered to the service. Hence, a broad definition needs to include the cases in which the payment process involves a mobile device that is not automatically used as a means of payment. Another problem is that the usual definition does not take into account the money transfers that can be processed through mobile devices, without any exchange of goods or services, such as person-to-person money transfers and remittances.

²² See the definition of the Mobile Payment Forum (2002) cited in F.S. Waris, F.M. Mubarik and L-F Pau, "Mobile Payments in the Netherlands: Adoption Bottlenecks and Opportunities, or... Throw Out Your Wallets", ERIS Report N° ERS-2006-012-LIS, 2006



Therefore, in this paper, we decide to focus on “mobile money transfers,” which we broadly define as transfers of money between two parties involving a mobile device. Mobile money transfers can be either remote, in-store, prepaid, or postpaid through reverse billing. In this paper, we also choose to focus on the case of mobile money transfers in developed countries.

The Potential Path of Development for Mobile Payment Solutions

An historical perspective on the development of payment card systems in developed countries can be useful to better understand the factors of success for the adoption of electronic payment systems. Payment cards were first introduced in the 1950s by closed platforms, such as Diners Club or individual banks, which managed to develop an important acceptance network for their customers. Afterwards, some banks decided to create interbank joint ventures, which enabled them to agree on common standards and increase their acceptance networks. The most important joint ventures, which later became Visa (1975) and MasterCard (1979), have a global reach and are now used and accepted in many different parts of the world. Recently, in 2006, these companies transformed their organizational structures to become publicly traded. The example of payment card systems shows that at least two ingredients are essential to the development of electronic payment systems for mass markets. First, the players must cooperate for the development of common standards, or specify the conditions for interoperability. Building a joint venture can considerably reduce the costs of incompatibility between different standards. However, as we will argue in the next section of the paper, the cooperation for the development of mobile payment services seems to be much more complicated than in the case of payment cards. Second, the players must develop an important acceptance network. Usually, the economic literature stresses the “two-sided” nature of retail payment systems.²³ Retail payment systems are indeed characterized by membership and usage externalities between two distinct groups of users, the consumers and the merchants. The more consumers adopt a payment instrument, the more the merchants will be willing to accept it, and vice versa. By taking advantage of network effects, joint ventures can increase the probability of success of each service provider who tries to affiliate consumers and merchants.

²³ See J-C Rochet and J. Tirole, “Two-Sided Markets: A Progress Report,” *RAND Journal of Economics* 37(2): 103-122 (2006) and M. Verdier, “Retail Payment Systems: What Do We Learn From Two-sided Markets?” *Communications & Strategies* 61 (2006): 37-51.



However, one should note that the problems for the adoption of mobile payment services are very different from the problems that the players faced for the diffusion of payment cards in developed countries. Consumers and merchants in developed countries are already well equipped with payment cards, a widely-used and accepted electronic payment solution. Hence, if they were to replace the use of payment cards, mobile payment services would have to provide sufficient additional value to be adopted by consumers and merchants. For instance, Ondrus et al. (2009) explain the failure of the mobile payment solution developed by PostFinance in Switzerland by the lack of value added to the existing payment card solution.²⁴ On the merchant side, for in-store payments, the incentives to adopt mobile payment solutions depend on the costs of upgrading the existing payment terminal, the level of security, and the potential additional benefits generated by the service, such as mobile couponing. For remote payments, such as e-commerce payments, merchants may find it valuable to add an additional payment option to their website, as cyber merchants who offer multiple payment instruments to their consumers tend to convert more visitors into customers.²⁵ On the consumer side, the mobile phones can potentially have a competitive edge over payment cards, as they can be used as an interactive device, in which the consumer can store information. However, consumers are often used to being delivered payment instruments for free, either in a bundle with their bank account, or by merchants who try to increase user stickiness. Hence, if the service is to be provided by a nonbank, the provider will have to find a way of recouping its costs of investment in infrastructure and security, which is not necessarily eased by the presence of low cost services. Another option for mobile payment service providers would be to target niche markets, in which payment cards are absent. Such markets could include person-to-person money transfers, or payment services at a low cost or a low risk for the unbanked or “underbanked.” The reasons why some people do not use existing electronic payment instruments are varied; for instance, if a consumer values privacy, he will not necessarily adopt mobile payments more easily than payment cards.

Cooperation Models for the Development of Mobile Payment Solutions

In this section, we study different cooperation models between the key players that could be involved in mobile payment solutions. We can view a mobile payment solution as based on three key inputs: i) a mobile phone, ii) a bank account, and iii) an acceptance network. Each of these inputs is

²⁴ J. Ondrus, K. Lyytinen, and Y. Pigneur, “Why Mobile Payments Fail? Towards a Dynamic and Multi-perspective Explanation,” working paper (2009).

²⁵ Cybersource, “The Insider’s Guide to eCommerce Payment,” study available at http://www.cybersource.com/news_and_events/view.php?page_id=1272.



to some extent controlled by a key player. Mobile network operators (MNOs) and mobile phone manufacturers have control over the design and distribution of mobile phones, as the former commercialize the phones at subsidized prices in their commercial agencies and own the SIM card while the latter produce the phones. Banks have control over their consumers' accounts. And, finally, payment systems like Visa or Mastercard have control over large acceptance networks.

Though these key players have some control over the three key inputs of a mobile phone solution, we argue that they can be bypassed. First, a solution can be developed without the cooperation of MNOs and mobile phone manufacturers, as the payment application can be resident on a separate SD card, for instance. Another example is the payment solution developed by the start up Square, which has been launched by the former CEO of Twitter. This solution is based on a plastic device that plugs into the mobile headphone jack, hence, it is completely independent of MNOs or manufacturers.²⁶ Second, the mobile payment solution could be based on the payment card of the consumers, in which case the provider does not need the cooperation of the banks to have access to the consumers' bank accounts. For instance, Obopay allows consumers to add money to their Obopay account with their debit or credit cards, and then send money to relatives or merchants with their mobile. Though Obopay proposes its service to banks, it has been developed without their cooperation. Third, a mobile payment service provider could develop a solution without a large acceptance network (like Visa or Mastercard) if it decides to target a niche market. For instance, the provider could limit the acceptance of its payment solution to vending machines (like Mobilkom A1 in Austria) or to a few affiliated merchants (like Obopay, which targets mainly P2P transfers but proposes merchants to affiliate to the system at no fee).

Since each of the three key players (banks, mobile network operators or mobile phone manufacturers, and large acceptance networks) could be bypassed or not for the development of a mobile payment solution, we have a priori six different possible combinations. The table below gives some examples for five combinations. The last combination corresponds to a situation where the mobile payment provider owns a bank or is a bank but bypasses the MNOs and the acceptance network. We consider that this combination is not relevant, as banks have strong incentives to develop a mass market solution, which requires cooperation with the acceptance network.

²⁶ See, for instance, Mark Milian, "Twitter Creator Wants to Give Away Square, His Credit Card Payment Gadget", *Los Angeles Times*, December 2, 2009.



	Cooperation with a...		
	Bank	Mobile network operator or mobile phone manufacturer	Large acceptance network
Light model	No	No	No
<i>Example</i>	This corresponds to the Obopay service in the U.S., where consumers use their payment cards to add money on their Obopay account, and can use any mobile phone.		
Mobile-centric model	No	Yes	No
<i>Example</i>	This model corresponds to the initial mobile prepaid solution proposed by NTT DoCoMo in Japan.		
Bank-centric model	Yes	No	Yes
<i>Example</i>	In this model, banks develop a mass market mobile payment solution without the cooperation of MNOs and mobile phone manufacturers.		
Partial integration model	Yes	Yes	No
<i>Example</i>	This model corresponds to the payment solution developed by Mobikom in Austria: the incumbent mobile operator Mobikom acquired a bank (A1) and restricted its mobile payment solutions to vending machines.		
Full integration model	Yes	Yes	Yes
<i>Example</i>	This model corresponds to different potential or existing situations: vertical integration over the value chain (one example is the mobile operator NTT DoCoMo in Japan, which acquired a bank and a large retailer); joint ventures between banks and MNOs; etc.		

These different models involve different degrees and forms of cooperation. Benefits of cooperation are cost-sharing and taking advantage of complementarities between different players. Banks have gained a great deal of experience in operating mass-market payment systems, which might be critical for a wide adoption of a mobile payment solution. They also have experience in risk and fraud management that other players, like MNOs, do not have. In contrast, MNOs have strong partnerships with mobile phone manufacturers which might help to develop payment-enabled mobile handsets. Costs of cooperation are twofold. First, partners will have to share not only costs but also revenues. For instance, in case of a cooperation between banks and MNOs, if mobile payment adds little value



relative to existing payment solutions (e.g., payments by card), this may impede the constitution of a partnership. Second, like in any joint venture, there are costs of coordination. As they have different objectives and interests for the development of mobile payments, we think that the costs of cooperation between banks and MNOs are probably high. The literature on research joint ventures (RJVs) indeed suggests that asymmetries between members of an RJV make the RJV less likely to succeed.²⁷

Finally, the incentives of the different players to develop mobile payments differ. If they develop a mobile payment solution, MNOs would be new entrants in the payment industry. In contrast, banks are incumbents in the payment market, and therefore would view mobile payments as an improvement over other payment solutions that they commercialize (like payment cards). Therefore, banks would face a "replacement effect" for the development of mobile payments. Hence, their incentives to develop mobile payments might be lower than the incentives of MNOs, except that they could have high preemption incentives to protect their market share from an entry threat.

Some Regulatory Issues

Finally, the cooperation models for the development of mobile payments could be impacted by the regulation of nonbank players. Bradford et al. identify several risks to the presence of nonbanks in payment systems: operational risk, settlement risk, legal risk, reputational risk, and systemic risk.²⁸ The provision of mobile payment solutions could increase the presence of nonbanks in retail payment systems, and thus, could require a regulatory intervention to limit the potential risks involved for the economy. So far, in developed countries, regulators have often tolerated the use of mobile phones for small transactions without requiring any banking license. However, this situation could be called into question if the volume of mobile payments were to become important. In Europe, the payment service directive offers to the new entrants the possibility to adopt the status of "payment service provider," which means that mobile payment service providers will be supervised by the relevant national regulatory authority. In France, for instance, the national supervisor (the CECEI) stated precisely that MNOs must apply for the right to enter the payments market, and it specified minimum capital requirements. If the MNOs were to issue electronic money,

²⁷ See, for instance: L. Röller, M. Tombak, and M. Siebert, "Why Firms Form Research Joint Ventures: Theory and Evidence," WZB discussion paper, FS IV 97 - 6r (1997).

²⁸ T. Bradford, F. Hayashi, S. Rosati, R-J. Sullivan, Z. Wang, and S.E. Weiner, "Nonbanks and Risk in Retail Payments," Social Science Research Network (2008), available at <http://ssrn.com/abstract=1201882>.



they would fall into the regulations of electronic money institutions. Some economic areas and countries such as Europe, Japan, and the Philippines have decided to design a specific status for e-money institutions. In other countries, there are still many regulatory loopholes that could slow down the adoption of mobile payments, either because the consumers may not trust nonbanks for payments, or because some companies may decide not to run the risk of investing in technologies that do not comply with the regulatory rules (compliance risk).

Conclusion

In this paper, we have argued that there are three key inputs for the development of mobile money transfers: bank accounts, mobile phones and large acceptance networks, with each of these inputs being somehow controlled by a key player (banks, MNOs or mobile phone manufacturers, and payment systems). A mobile money transfer solution could either involve cooperation with or bypass of these key players. Hence, we define five different cooperation models and we give some examples for each of these models.

However, the competition that could emerge within each model and between the various models remains to be seen. One could be tempted to argue that the light model is easier to implement to target niche markets, but that prospects for mass adoption of mobile payments are higher with the full integration model.

Finally, we focused on developed countries. However, many interesting questions are raised by the development of mobile payments in developing countries, which would deserve further attention. An interesting question would be to examine under which conditions mobile payments can really improve access to banking services in countries where a large share of the population is unbanked.



PCIDSS and the Legal Framework for Security: An Update on Recent Developments and Policy Directions

Edward A. Morse* and Vasant Raval^f

I. Introduction

Consumer risks associated with unauthorized payment card usage have largely been assumed by others within the payment card matrix, leaving consumers mostly immune from financial liability. But related risks from unauthorized access to personal information remain as an important area of concern for consumers, who face potential costs outside the realm of control of payment card system participants. For the most part, the security measures imposed within the payment card matrix have been the product of private ordering, with Payment Card Industry Data Security Standards (PCIDSS) emerging as a pervasive standard. Compliance measures emerging around PCIDSS have also been the product of private ordering, and these measures have taken into account both prudential and technological limitations associated with the payment card matrix and its constituent members.

Private ordering for security is reinforced by important economic interests within the payment card industry, where security measures translate into customer trust, which is essential to the functionality of the payment card matrix and the profitability of participants. In a prior article, we have explored these economic motivations favoring private ordering as a solution to consumer concerns involving payment card data security, along with threats to that framework through legislation and litigation.²⁹ This essay provides an update, focusing on recent developments in litigation and legislative fronts that may shape outcomes affecting PCIDSS as well as developments

* Professor of Law, Creighton University School of Law.

^f Professor of Accounting, Creighton University College of Business Administration.

²⁹ Edward A. Morse and Vasant Raval, "PCIDSS: Payment Card Industry Data Security Standards in Context," 24 *Computer Law & Security Report* 540 (Elsevier 2008), available online at <http://ssrn.com/abstract=1303122>.



within the PCIDSS model. Despite the likelihood of increased government intervention, private ordering can be expected to remain central to the development of appropriately nested security measures that will lead to continued trust and participation in the payment card system. As we discuss below, trust, and not absolute security per se, should be the ultimate benchmark for moving forward with enhancements to this system.

II. Legal Intervention: Significant Litigation and Proposed Legislation

Litigation and proposed legislation have impacted security measures within the payment card matrix in the past year. Despite assurances of conformity with PCIDSS, security standards are not foolproof. When breaches occur, private litigants, state attorneys general, and legislators have become involved. Although consumers have found it difficult to prove compensable losses for the purpose of bringing claims against merchants with security breaches, issuing banks have been more successful in extracting settlements from those merchants. State attorneys general have also achieved successful settlements, despite uncertainty in the legal framework for liability. Some of the significant cases, as well as proposed legislative interventions, are discussed below.

A. Litigation

The massive security breach within The TJX Companies – affecting more than 45 million credit and debit card accounts – provided an important wake-up call for payment card industry participants. This breach continues to impact the scrutiny of data security standards and compliance with those standards. Issuing banks who incurred significant costs as a consequence of the breach, including the costs of replacing customer cards, sought relief through litigation, and some consumer groups also joined in the fray. This litigation, involving as many as 18 cases, has gradually been



resolved through settlements.³⁰ All totaled, The TJX Companies have paid more than \$130 million in cash, along with an estimated \$177 million in consumer discounts and payments for credit monitoring services for consumers affected by the breach.³¹ It also settled claims brought by state attorneys general of 41 states, in which TJX agreed to payments of more than \$9 million as well as the imposition of additional data security requirements, despite the fact that the company “firmly believes that it did not violate any consumer protection or data security laws.”³²

While the disclaimer of wrongdoing is a standard litany in settlement announcements, the truth of the matter here is that TJX might have won had it chosen to continue litigating these claims. Within the cases that made it to judgment on preliminary matters, TJX and its co-defendant Fifth Third Bank, the processing bank for its credit card transactions, came out quite favorably. Claims for negligence and breach of contract were dismissed by the trial court,³³ and earlier this year they were affirmed in the First Circuit.³⁴

The negligence claims failed on account of the so-called economic loss doctrine, which holds that “purely economic losses are unrecoverable in tort and strict liability actions in the absence of personal injury or property damage.”³⁵ Although one of the claimants argued that it had property damage through the fact that payment card information was rendered worthless, this was rejected as a cognizable form of injury based on Massachusetts law.³⁶ Consumers seeking tort recoveries would also face barriers from these doctrines, as well as the additional problem of showing a compensable loss based solely on data breach, which is a critical prerequisite to standing to maintain

³⁰ See “TJX, Financial Institution Plaintiffs Settle Claims in Breach of 46 Million Credit Cards,” 14 *BNA Electronic Commerce and Law Report* 1296 (September 16, 2009).

³¹ See *id.* This total includes \$40 million to banks in December 2007, \$24 million to banks in April 2008, and \$70 million in connection with a consumer class action settlement in September 2007.

³² See Press Release, “The TJX Companies, Inc. Announces Settlement with Attorneys General Regarding 2005/2006 Cyber Intrusions” (June 23, 2009), available at http://www.businesswire.com/portal/site/tjx/?ndmViewId=news_view&newsId=20090623006073&newsLang=en

³³ *In re TJX Companies Retail Security Breach Litigation*, 524 F.Supp.2d 83 (2007).

³⁴ *In re TJX Companies Retail Security Breach Litigation*, 564 F.3d 489 (1st Cir. 2009).

³⁵ *Id.*, 565 F.3d at 498 (quoting *Aldrich v. ADD, Inc.*, 437 Mass. 213, 222 (2002)). For further discussion of the economic loss doctrine, see *Morse & Raval*, *supra* note 1, at 548.

³⁶ *Id.*



a claim.³⁷ Thus, these tort-based claims seem to include serious barriers that protect the industry from liability that might otherwise induce greater attention to breaches.

As for the contract claims, the claimants failed to show that they were covered by relevant contractual language. Security requirements were included in relevant contracts between TXJ and its processing bank, as well as in the card processing agreements with Mastercard and Visa.³⁸ However, the claimants were not parties to these contracts, and relevant state law did not support the claimants' position that they were intended to be third party beneficiaries of those contracts; indeed, the contracts expressly limited their obligations and benefits to the contracting parties, thus excluding others from this status.³⁹ Here, too, contract law serves as a protection from third-party liability.

The First Circuit allowed some other claims to go forward, including a claim based on "negligent misrepresentation," which allows recovery in tort based on failing to exercise reasonable care or competence in obtaining or communicating information to others, which falsely guides them in their business transactions. However, the court also questioned whether proof could be adduced for this claim, cautioning that "[i]t would almost surely stretch Massachusetts law too far to say that merely doing credit card transactions with issuing banks, whether directly (Fifth Third) or indirectly (TJX) is a representation implied by conduct to third parties that defendants were complying with detailed security specifications of Visa and Mastercard."⁴⁰ Although the First Circuit allowed further

³⁷ For additional discussion of the standing problem, see Morse & Raval, *supra*, at 548. Consumers seeking redress for damages based solely on their time and effort in response to the data breach at Hannaford Brothers Grocery have had this question certified to the Maine Supreme Judicial Court, owing to uncertainties in state law on this point. See *In re Hannaford Bros. Co. Customer Data Security Breach*, ___ F. Supp. 2d, 2009 WL 4145416 (D. Me. November 24, 2009).

³⁸ For further discussion of the web of contractual relationships within the payment card network, see Morse & Raval, *supra*, at 551-52.

³⁹ See *In Re TJX Companies Retail Securities Breach Litigation*, 564 F.3d at 489.

⁴⁰ *Id.* at 494.



proof to be offered at trial, it also noted, “The present claim thus survives, but on life support.”⁴¹

Thus, if this claim had gone forward, it does not seem to present a very serious threat.

A final claim that did survive involved a state law provision allowing claims for “unfair” or “deceptive” trade practices. This claim is linked closely to Section 5 of the Federal Trade Commission Act, which provides authority to the FTC to address unfair or deceptive practices.⁴² In this case, TJX had been the subject of a consent decree from the FTC with regard to this security breach.⁴³ Although the category of “unfair” conduct is admittedly vague, the court found that FTC precedent and factors serve to offset this vagueness.⁴⁴ Here, if appropriate facts are proven, “a court using these general FTC criteria might well find in the present case inexcusable and protracted reckless conduct, aggravated by failure to give prompt notice when lapses were discovered internally, and causing very widespread and serious harm to other companies and to innumerable consumers” that would give rise to relief under this provision.⁴⁵

Of course, The TJX Companies could not have known these outcomes for sure at the time of settlement. Litigation portends significant business disruptions, which must be taken into account in assessing whether settlement is prudent. Moreover, the “unfair” trade practice claim under state law presents an environment of significant legal uncertainty, which a prudent decisionmaker may well choose to avoid. But coming out of this litigation, we are left with considerable uncertainty from the judicial sector as to what standard of behavior is required with regard to data security and the basis for a successful claim.

Nevertheless, economic costs of nearly \$300 million from a security breach caused by criminal conduct surely causes corporate officers to take notice. But what action is appropriate? And how does existing law provide the answer to this question? As other breaches have rolled

⁴¹ Id. at 495.

⁴² For an explanation of the role of FTC enforcement actions, see Morse & Raval, *supra*, at 545-46.

⁴³ See *In the Matter of TJX Companies, Inc.*, File No. 072-3055.

⁴⁴ *In re TJX Companies Retail Security Breach Litigation*, 564 F.3d at 497.

⁴⁵ Id. at 496.



through the media, shareholders have also taken notice. When a significant stock price decline occurs in connection with the announcement of a data security breach, is corporate management responsible for notifying shareholders of these risks? A study released last spring by Hiscox, an insurance firm based in Bermuda that sells, among other things, “hacker insurance,” suggests that a significant number of firms are not disclosing these risks in their SEC filings.⁴⁶ Moreover, among the firms surveyed with obligations to be PCIDSS compliant, more than one third of these firms were not compliant.⁴⁷

Three points are particularly relevant in this regard. First, it appears that state law is the primary foundation for developing these claims. When an international payment network is involved, merely deciding which state’s laws should apply presents a significant problem. For example, in the TJX litigation, Fifth Third Bank, the payment card processor, did its work outside of Massachusetts. Should its conduct conform to Massachusetts law?⁴⁸ Second, even if we know which laws apply, should the regulation of important interstate activities be relegated to a patchwork of state regulation? Third, if laws are to provide not only the source of standards, but also allocate the costs of failing to meet those standards, will legal solutions developed through the courts adequately define the standards and efficiently allocate the costs? If so, will the standards remain current, in

⁴⁶ See *id.* A recent class action lawsuit by shareholders seeking to hold the management of a Heartland Payments Systems, Inc., a large bank card payment processing company, accountable for inadequate disclosures relating to the state of its computer network security was dismissed on the ground that the company’s disclosures were not misleading and did not omit relevant information related to the breach. See *In re Heartland Payment Systems, Inc. Securities Litigation*, Civ. No. 09-1043 (D. N.J. 12/07/09); see also “Court Rejects Shareholder Class Action Over Heartland Payment Systems Breach,” 14 *BNA Electronic Commerce & Law Report* 1776 (December 16, 2009). However, this nonpublished decision may not be the last word on whether the prospect of shareholder claims will provide an additional impetus for management to engage in security efforts.

⁴⁷ Hiscox, “Data privacy and corporate America: who’s recognizing the risk” (April 2009); “Many Firms Fail to tell SEC of Risk to Finances, Reputation from Data Breaches,” 14 *BNA Electronic Commerce & Law Report* 562 (April 22, 2009).

⁴⁸ The First Circuit certainly thought so. See *id.* at 498 (rejecting claims for exemption from unfair practices claims based on the fact that none of the processing occurred primarily or substantially within Massachusetts; noting that “communicating to and from TJX’s servers in Massachusetts is part of the causal chain.”)



pace with information technology? Needless to say, there are certainly grounds for skepticism on these points. The law as a sole source of a holistic solution appears far from reality.

B. Proposed Legislation

Data security breaches have received attention from legislatures at both state and federal levels. Most states have enacted legislation that requires public disclosure of data security breaches, which applies not only to payment card information, but also to a broad range of other personal information.⁴⁹ Such efforts have had a salutary effect on bringing out the consequences of inadequate security, as well as allowing the affected individuals to take appropriate corrective action. However, those efforts provide, at best, a patchwork solution, raising significant potential conflicts for businesses engaged in multistate business operations.

To date, only Minnesota has enacted any legislation to address the problem of who bears costs associated with the breach of security within the payment card system. Minnesota law provides a statutory basis for recovery to the issuing banks, effective beginning August 1, 2008, for a breach of security in violation of the statutory security standards.⁵⁰ The recovery may include costs incurred in order to protect the information or cardholders, cancellation and reissuance of payment cards or other access devices, notification costs, as well as the costs of unauthorized transactions.⁵¹ The standard for liability, however, reflects a rather weak standard, which would include retaining customer data more than 48 hours after the transaction has been authorized.⁵² Of course, this falls short of PCIDSS compliance. As one commentator has noted, a PCIDSS compliant merchant would certainly meet the standard and avoid liability under the statute despite the fact that a security breach occurred, but a merchant that complied with Minnesota's laws may not necessarily be PCIDSS compliant.⁵³ Significantly, this legislation fails to provide a realistic standard for proper commercial

⁴⁹ See Morse & Raval, *supra*, at 546-47.

⁵⁰ See Minn. Stat. Ann. § 325E.64(3).

⁵¹ See *id.*

⁵² See *id.* § 325E.64(2)

⁵³ See James T. Graves, Note, "Minnesota's PCI Law: A Small Step on the Path to a Statutory Duty of Data Security Due Care," 34 *Wm Mitchell L. Rev.* 1115, 1135-36 (2008).



behavior. Instead, it imposes liability only for a subset of commercial behavior that might be regarded as highly improper. This ultimately adds little to the solution of the question of defining a broader standard for behavior which might result in shifting costs.

Congress has also looked at the matter of data security for payment cards, with a particular focus on whether the matter of self-regulation through PCIDSS is enough. A bill has recently passed the House, HR 2221, the Data Accountability and Trust Act, which addresses several aspects of the data security breach problem. First, it provides a federal rule for notification of data security breaches, thus resolving the problem of potentially competing state demands.⁵⁴ Second, it delegates authority to the FTC to promulgate regulations within one year “to require each person engaged in interstate commerce that owns or possesses data containing personal information, or contract to have any third party entity maintain such data for such person, to establish and implement policies and procedures regarding information security practices”⁵⁵ The Act specifically preempts state information security laws, thereby ensuring a single federal source for compliance.⁵⁶

As for enforcement, the Act does not provide a private cause of action. The FTC and state attorneys general are both empowered to enforce these rules, including the imposition of civil penalties and fines, not to exceed a total of \$5 million.⁵⁷ Thus, the matter of whether consumers, issuing banks, or shareholders may bring claims for damages is not resolved here.

Also unresolved by this bill, of course, is the content of the policies and procedures that must be maintained in order to avoid these penalties. Building upon what has already been accomplished in the payment card industry would seem to be a likely point for departure. Although PCIDSS is subject to criticism as not providing enough security, focusing on the products of private ordering here may become, at the least, an important starting point.

⁵⁴ HR 2221, § 3.

⁵⁵ *Id.* § 2(a)(1).

⁵⁶ *See id.* § 6.

⁵⁷ *See id.* § 4.



III. PCIDSS: Private Ordering at Work

The Payment Card Industry (PCI) Data Security Standards (DSS) emerged out of the payment card industry's business needs. Initially, such standards in various forms were set in motion by each card issuer. Given the inherent risks of the payment card industry, the realization that a patchwork of diverse standards will not work became apparent. Furthermore, with less than a dozen major card brands controlling over 90% of the card industry, players realized that cooperation in this arena would be an effective approach for the industry as a whole. Consequently, the industry, with limited participation from other stakeholders, put together a set of requirements, called standards. As we noted earlier, these standards have the force of economic utility, which cannot be easily ignored. It is through contractual commitment that a waterfall of participants in the industry, from individual retailer to merchant banks to the card brands, should honor their commitment to compliance with these requirements.

In October 2008, the PCI Security Standards Council released Version 1.2 of the standards.⁵⁸ The revisions focus on clarifications and explanations, and on removing redundant sub-requirements. Of the numerous changes made, the Council lists the following four as enhancements:

- Requirement 4.1.1 now emphasizes the use of strong encryption technologies for wireless networks.
- Requirement 5.2 now provides for separate testing procedures to verify that all anti-virus software is current, actively running, and capable of generating logs.

⁵⁸ PCI Security Standards Council, Payment Card Data Security Standard, Summary of Changes form PCI DSS Version 1.1 to 1.2, October 2008.



The four separate procedures refer to verification of the policy, software installation, system components, and logs.

- Form for attestation of compliance for onsite assessments – merchants, has been added (Appendix D).
- Form for attestation of compliance for onsite assessments – service providers, has been added (Appendix E).

The new version essentially provides clarification through granularity and clears up some of the language to make meaning more precise.

A. Are We Secure Yet?

Is the Payment Card Industry secure? Despite some progress in the industry-led governance in this domain, compromises occur. As the web gains increasingly larger share of payment card transactions, both in number of transactions and the aggregate amount worldwide, the risks of such compromises will continue to frustrate the industry and its stakeholders, including consumers. The 2009 Data Breach Report issued by Verizon Business analyzed 90 confirmed breaches in 2008 affecting 285 million records.⁵⁹ Their previous report, covering years 2004 through 2007, reported a four-year aggregate of 230 million transactions compromised during the period.

A striking statistic in the 2009 Verizon Business report is this: 81% of victims were not Payment Card Industry (PCI) compliant.⁶⁰ The issue is not the spirit of the PCIDSS standards, but rather the execution by participants of the process of remaining compliant. Penalties and litigation, not to mention the government's reach to stop the breaches, persist past such incidents, but with only marginal systemic improvements in the sense that, when a weakness is exposed, sophisticated actors will seek to address that weakness. But that is

⁵⁹ Verizon Business, 2009 Data Breach Investigations Report, www.verizonbusiness.com.

⁶⁰ *Op.Cit.*, page 3.



surely not the end of the persistent battle to prevent criminal exploitation of weakness.

Litigation results, such as the settlements discussed above, merely reallocate losses, albeit with significant additional transaction costs.

B. Core Issue: Security or Online Trust?

The market mechanisms in the payment card transactions environment appears to thrive on the consumer trust. As we indicated earlier, a major chunk of the consumer comfort in online financial transactions seems to lie in the protection afforded to them, that they will be compensated for financial losses they incur. However, there are other consumer costs also. For example, Listerman and Romesberg report that it takes an identity theft victim an average of 58 to 231 hours of personal time to deal with all of the correcting and legal issues.⁶¹ And even Ben Baranke is not exempt from this, as evident in a compromise that hit his wallet recently.⁶²

Consumers don't necessarily want, or desire, perfect security. They need to trust the system in order for them to be able to transact on an ongoing basis. Trust can only be asked of the customer, not provided by the merchants. Therefore, it is important to recognize that the industry would be prudent to work with a surrogate – secured systems – to seek online trust. Thus, since online trust seems to be a somewhat uncontrollable phenomenon, the PCI seeks to generate consumer trust through security. Imperfect as it is, the security could lead to consumer trust, thus sustaining the market mechanism for thriving consumer activity.

We scoured the PCIDSS Version 1.2 for the terms “trust,” “trusted system,” and “security.” Whereas there are numerous references to *security*, there is no mention of *trusted system(s)* in the entire standard. Requirement 1, Install and maintain a firewall

⁶¹ R.A. Listerman and J. Romesberg, “Are We Safe Yet?” *Strategic Finance* (July 2009): 27 -33.

⁶² Michael Isikoff, “Bernanke Victimized by Identity Theft Ring”, *Newsweek*, August 25, 2009, available at <http://www.newsweek.com/id/213696>



configuration to protect cardholder data, is preceded by a heading, Build and Maintain a Secure Network. The preamble to specific sub-requirements within Requirement 1 talks about trusted and untrusted networks but ultimately switches to the comfort zone of security without laying a bridge between security and trust. And perhaps this is as it should be, when we are speaking of technical standards. But the ultimate goal remains a trusted system, in which customers are not afraid to spend and merchants are not afraid to participate. If threats are too great, consumers will keep their cards in their pockets. But if merchants or other participants face potentially crippling losses from a reallocation of costs, their participation is at stake, too.

IV. The Way Forward

The payment card transactions environment is complex. If we look at it carefully, it involves issues of pricing and resource allocation (or reallocation), consumer loyalty, online trust, global reach of the industry, customer information protection, and business value structuring across a network of value adding participants. Numerous stakeholders are in the mix, with different motives and goals.

Policy analysis that focuses solely on security will undoubtedly reach the conclusion that the current model of self-regulation is not achieving this goal. Congressional hearings this past spring rehearsed a litany of breaches, including Hannaford Brothers, TJX, Heartland Payment Systems, and others, which typically involved gaps in PCIDSS compliance.⁶³ The self-regulation model implicitly recognizes that security is not, and will never be, an achievable goal. The network includes participants with broad ranges of technological

⁶³ See "House Panel Asks Whether Self-Regulation is Effective Against Credit Card Cybercrime," 14 *BNA Electronic Commerce & Law Report* 490 (April 8, 2009). Statements from these hearings in the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology on March 31, 2009, can be accessed at <http://hsc.house.gov/hearings/index.asp?ID=185>



sophistication and economic wherewithal to implement security measures and bear the costs of monitoring compliance with those measures. These pragmatic limitations, coupled with the inherent ingenuity of humans (a trait unfortunately shared by hackers, too), ensure that security failures will occur in any payment system.

Apart from fines that may be imposed, the self-regulation model effectively allocates costs within the system to merchants (for chargebacks) and to issuing banks (for reissuing cards). These participants, in turn, are likely to export those costs to their customers, albeit discreetly through pricing of their products and services. Intervention through either legislation or through litigation to reallocate losses within this model may reflect political preferences for some participants over others, but such interventions inject new transaction costs into the mix. And to the extent government seeks additional protections for consumers, those reallocations may prove temporary to the extent that customers are likely to become the ultimate cost bearers for any system.

Reallocations need to be based on clear and cognizable standards for security obligations, which are lacking within the legal system but which are present, more or less, within the system of self-regulation. Although the Minnesota law discussed above may achieve clarity by defining minimal standards that are far below the expected level of behavior, such an approach is unlikely to induce trust. However, a more robust approach presents significant new challenges. Whether the FTC can achieve this feat in one year, as directed by HR 2221, is doubtful. Whatever they do achieve is likely to be subject to the same criticisms of PCIDSS – those standards will not necessarily achieve security either, and it is far from clear that whatever they do achieve will enhance trust in this system.

Disclosure laws, on the other hand, may serve an important role in protecting consumers from a false sense of trust. This kind of intervention is likely to enhance the



effectiveness of self-regulation through reinforcing market-based incentives toward preserving security and addressing shortcomings. To the extent HR 2221 helps move us toward common standards for disclosure, thereby avoiding uncertainty and conflicts that emerge from a patchwork of state laws, this is a positive development. Disclosure requirements also reinforce trust by precipitating offers of assistance such as credit monitoring, which are emerging as expected and customary practices by firms who experience security breaches. Disclosure also provides a valuable signal to other participants, including consumers, that they have obligations to be vigilant. We all have personal information circulating in networks, which makes us vulnerable. As we have used technology to address other technology problems, such as spam, private monitoring systems have emerged to help address threats. Efforts by the FTC to impose monitoring obligations on financial services providers may also assist consumers in this process.

Government should tread lightly in this dynamic area. Although it is tempting to make points with voters through expressing the good intention of protecting consumers from the errors of others, consumers are likely to become the ultimate cost bearers. Adding more technical security standards in an environment in which existing standards are often not in compliance leads to justifiable skepticism as to whether this approach will benefit consumers. And if compliance costs increase significantly, the cure may be worse than the disease.

Courts should also exercise restraint in expanding legal doctrines that would require cost-shifting among participants in the payment card marketplace. The current scheme diffuses costs in a manner that avoids significant transaction costs and the threat of crippling liabilities from a security failure that are admittedly difficult to prevent ex ante. Threats of liability may devote more resources to compliance, but the realities of the marketplace



suggest limits that courts are ill-equipped to consider. If the costs associated with security risks are too high, merchants may also choose to withdraw. Those who think this is not possible should consider the practices of merchants today with regard to personal checks. For many, the costs and risks of this payment medium are simply too great. Locating an ATM in the store instead of taking checks or payment cards is an emerging option we have observed in some retail locations, but this may present new risks, including tax-enforcement issues that lurk in a cash-based economy.

We can do better at keeping customer data secure. The industry knows this, too, as it will continue the process of self-examination. But the broader concept of trust, in which security plays a complementary role along with other values, including cost-effective utility, deserves greater attention by policymakers considering intervention and refinements in the payment card system.