Can Smart Cards Reduce Payments Fraud and Identity Theft?

By Richard J. Sullivan

In the United States, when a consumer presents a payment to a merchant, the merchant typically makes a request for authorization before accepting the payment. Personal information, such as an account number, address, or telephone number, is often enough to initiate a payment. A serious weakness of this system is that criminals who obtain the correct personal information can impersonate an honest consumer and commit payments fraud.

A key to improving security—and reducing payments fraud—might be payment smart cards. Payment smart cards have an embedded computer chip that encrypts messages to aid authorization. If properly configured, payment smart cards could provide direct benefits to consumers, merchants, banks, and others. These groups would be less vulnerable to the effects of fraud and the cost of fraud prevention would fall. Smart cards could also provide indirect benefits to society by allowing a more efficient payments system. Smart cards have already been adopted in other countries, allowing a more secure payments process and a more efficient payments system.

Richard J. Sullivan is a senior economist at the Federal Reserve Bank of Kansas City. This article is on the bank's website at ***www.KansasCityFed.org****.*

This article explores why smart cards have the potential to provide strong payment authorization and thus put a substantial dent into the problems of payments fraud and identity theft. But adopting smart cards in the United States faces some significant challenges. First, the industry must adopt payment smart cards and their new security standards. Second, card issuers and others in the payments industry must agree on the specific forms of security protocols used in smart cards. In both steps the industry must overcome market incentives that can impede the adoption of payment smart cards or limit the strength of their security.

Section I reviews the costs of payments fraud and describes how payments fraud is related to identity theft. It then illustrates how card payments in the United States are currently authorized. Section II explains how smart cards work and how they can improve payment authorization. It also describes weaknesses that can remain even with the use of smart cards. The next two sections discuss the economic challenges that smart cards face in the United States. Section III examines the incentives for adopting payment smart cards and for upgrading payment security standards. Section IV examines the market processes that determine the security standard used in payment smart cards. The final section offers some concluding thoughts.

I. PAYMENTS FRAUD, IDENTITY THEFT, AND PAYMENT AUTHORIZATION

Payment fraud is costly to all payment participants and has indirect costs that affect all members of society. Identity theft often leads to payment fraud, which is made possible because the authorization process fails to identify a fraudulent transaction. Before looking closely at how payment smart cards can improve the security of payment authorization, it is useful to consider several basic questions. What are the costs of payments fraud and how are they distributed? How is payments fraud related to identity theft? And, what is the purpose of payment authorization and how does it work?

The costs of payments fraud

The exact costs of payments fraud are difficult to pin down because the data on costs are not consistently reliable. Still, a review of selected

data helps show the magnitude of the problem and who pays the costs. Clearly, the costs are spread across many members of society.

Losses from payments fraud are shouldered by banks, merchants, and consumers. Bank losses total about $2.89 billion per year (Table 1, panel A).[1] The largest share of bank losses are on credit cards, followed by losses on checks, debit cards, and ACH payments. Fraud losses for retail merchants total about $15.6 billion per year, with most losses due to bad checks.[2] Reflecting the growing importance of Internet retailing, merchant losses from credit card fraud at websites are now larger than those at brick-and-mortar locations.[3] Finally, in 2007 out-of-pocket losses to consumers from identity theft are estimated at $5.6 billion.[4]

The high costs of preventing payments fraud and of complying with regulatory and network security standards are similar to the estimates of the actual losses due to fraud (Table 1, panel B). In 2006, banks spent an estimated $3.1 billion to prevent payments fraud, while merchant spending may have reached $5.0 billion. Recently, several card networks (Visa, MasterCard, Discover, American Express, and JCB) have harmonized and updated their security standards for merchants and service providers who accept or process transactions made with their payment cards. These standards, known as the Payment Card Industry Data Security Standards (PCI DSS), began a phased implementation process in 2005. The costs for merchants to comply with PCI DSS standards have been significant, with estimates ranging from $2.6 billion to $5.5 billion in 2006.[5]

The indirect costs of payments fraud include the costs of local and national law enforcement, barriers to online commerce and its benefits, barriers to adoption of electronic payments and its efficiencies, and potential loss of confidence in payments. For example, many consumers are wary of revealing personal information and so avoid Internet shopping. One estimate suggests that the share of consumers who shop on the Internet, currently estimated at 66 percent, would rise to 73 percent if consumers did not fear disclosing personal or credit card information (Horrigan). Similarly, many consumers avoid electronic payments out of concerns for privacy and security (Benton and others). The current transition away from less efficient check payments would be quicker if consumers had less concern over the electronic payment security.

Table 1

SELECTED MEASURES OF THE ANNUAL COSTS OF PAYMENTS FRAUD IN THE UNITED STATES

A. Fraud Losses

	Payment type	Losses ($billions)	Period
Banks	Credit cards	1.240	2006
	Checks	.969	2006
	Debit cards	.626	2005
	ACH	.065	2005
	Subtotal	2.89	
Merchants	Checks at retail locations	10	2006
	Credit cards at online retailers	3.6	2007
	Debit and credit cards at brick-and-mortar retailers	2	2006
	Subtotal	15.6	
Consumers	All payment losses due to ID theft	5.6	2007

Sources: ABA; Fabian; Pulse; "Credit Card Fraud;" Bills; Mott 2007a; Meacham; Javelin 2008b.

B. Costs of Prevention and Compliance with Security Standards

	Prevention/Compliance	Costs ($billions)	Period
Banks	Prevention for all types of payment	3.1	2006
Merchants	Prevention for all types of payment	1.1 to 5	2006
	Compliance with debit and credit card security standards	2 to 5.5	2006

Sources: Kusovski; Mott 2007b, "What's the Industry Cost;" "A Deeper Dive."

Thus, the direct costs of payments fraud are spread across banks, merchants, consumers, and others, while the indirect costs, such as failure to obtain the complete benefits of Internet retailing and electronic payments, affect the entire economy. But payments fraud is not new and society has worked over time to limit the costs. What is new is a surge in identity theft as a source of payments fraud (Schreft).

Identity theft

Identity theft occurs when one individual misuses another individual's personal information to commit fraud (President's Task Force on Identity Theft). In 2007, an estimated 8.1 million people in the United States were victims of identity theft, with total losses estimated at $41 billion (Javelin 2008b). Although both the total number of victims and the proportion of the U.S. population suffering from identity theft have declined in each year from 2003 to 2007, it remains a major public policy concern.

The most common type of identity theft, existing account fraud, occurs when a payment card or checkbook is lost or stolen and a criminal uses the card or forges a signature on a check. It can also occur using only the information on a credit card or check for Internet purchases or by creating counterfeit checks or payment cards. A second type of identity theft, called new account fraud, occurs when a criminal obtains personal information on an individual and impersonates the individual to create a new payment account, such as a checking or a credit card account.[6]

Identity theft and payments fraud are not always the same. Some payments fraud, such as changing the dollar amount on an existing check, is not related to identity theft. Conversely, not all identity theft results in payments fraud. Medical identity theft is a significant problem (Yip). And, a recent study of 517 identity theft cases investigated by the Secret Service revealed that substantial shares of the cases were related to fraudulent applications for loans or concealment of identity from authorities (Gordon and others). The same study, however, calculated that 78 percent of the crimes used a victim's identity to obtain cash or credit cards.

Identity theft and associated payments fraud start with lost or stolen payment instruments or surreptitiously obtained bits of information. Often the information is not difficult to obtain, such as by employees or other insiders at locations that store the data. Outsiders can

get it by picking through trash (Acohido and Swartz). Another source is hacking into online databases or intercepting payment messages. In the 12-month period from April 2007 to March 2008, for example, more than 300 data breaches in the United States exposed at least 24 million records of personal information that could potentially be used to commit payments fraud.[7]

Payments fraud can then occur if these bits of information are used to obtain cash or goods. Criminals can obtain cash by making counterfeit cards and using them at an ATM (Dove Consulting 2007). They can obtain goods with stolen or counterfeit payment cards at brick-and-mortar retailers or with the few pieces of information needed for an Internet purchase. Success in each of these cases depends on the criminal's ability to thwart payment authorization schemes that otherwise prevent fraudulent payments.[8]

Payment authorization

Payment authorization attempts to ensure that a person making a purchase uses a valid payment instrument that is properly attached to the associated payment account.[9] It can make a merchant or other payee more comfortable accepting the payment instrument. It assures the payer that unauthorized individuals cannot easily use the payment instrument. And an effective authorization system makes a payment instrument more likely to be widely used.

A transaction is authorized if three tasks are completed satisfactorily (Ward). First, the payment instrument and other hardware are authenticated. Second, the identity of the payer is verified. Third, details of the transaction must satisfy risk parameters set by the merchant and the card issuer.

Specific methods of authorization depend on the payment instrument. This article reviews authorization for debit and credit card payments in some detail because they are growing rapidly in the United States and because, as electronic forms of payment, they are an increasingly important target for payments fraud.[10]

Card payment authorization differs depending on how the consumer verifies their identity: with a signature (as with credit cards and some debit cards) or with a personal identification number (or PIN, used with some debit cards). Authorization also differs in that the debit

or credit card may or may not be present during the transaction. The card is usually present for purchases in brick-and-mortar retailers but not present for Internet or telephone orders.

In card-present transactions, a consumer uses the card at a point of sale, and the merchant can authenticate the card by inspecting for counterfeits. For signature cards, the merchant can verify the identity of the cardholder by inspecting the signature on the payment ticket against the signature on the back of the card. For PIN debit, the consumer's successful entry of the payment card's PIN verifies the cardholder's identity.

The transaction information is then sent over the payment network.[11] A processor can confirm that the card is valid and that the value of transaction is below a limit set by the card issuer. It can also check to see if there is a sufficient balance in the cardholder's bank account (for debit cards) or if there is a sufficient line of credit (for credit cards) to cover the payment. To further guard against fraud, card issuers may employ supplementary analysis to identify transactions that are out of the ordinary for the cardholder. Risk parameters used in the analysis might include the location of the transaction, the number and value of recent transactions, the specific merchant where the transaction is taking place, and so on.

Card-not-present transactions are most commonly conducted with signature payment cards. The merchant cannot inspect the card or verify a signature. It can use certain rules to limit risk, such as accepting an order only if the customer's shipping address matches the address associated with the payment card. To confirm that the consumer actually possesses the card in card-not-present transactions, the merchant can ask the customer to provide security codes that are imprinted on the card and check to see if the card account number is consistent with the security code.[12] Card networks have strict rules prohibiting retention and storage of the security codes to help ensure they are not easily accessible to unauthorized individuals.

Some methods used to authorize a card in card-present transactions, such as card validity, transaction limits, and sufficient account balances, are also used in card-not-present transactions. Supplementary authorization methods can also be used. The card can be further authenticated by a protocol called 3D Secure.[13] Both merchant and cardholder must

enroll in the program. The cardholder registers his or her payment card with their card issuer and chooses a 3D Secure PIN. A transaction at an enrolled merchant has an extra step that requires entry of the PIN, thus providing further assurance that only the appropriate cardholder is using the payment card.

With a properly authorized card-present transaction, the merchant bears little risk that it will not get the funds from the transaction. An authorized debit card transaction provides strong assurance that funds for payment are in the customer's account and that they will be properly transferred to the merchant. With a credit card transaction, the merchant gets a payment guarantee from the card issuer and, if the transaction turns out to be fraudulent, the card issuer bears the cost. Fraud risk is higher for card-not-present transactions and, as a result, the merchant will pay higher transactions fees.[14] In addition, the merchant does not generally get a payment guarantee with a properly authorized transaction.[15]

Most cards payments, and many other payments, can be authorized in the United States based solely on information.[16] At first, authorization relied mainly on the card account number and transaction information. To further fight against fraud, card issuers have expanded the information set they rely on to authorize a transaction, such as the location of the transaction and the transaction history of the cardholder. In some Internet payment systems, such as online banking, customers must provide personal information to populate answers to challenge questions. This information can be extensive and diverse, such as the customer's city of birth or the manufacturer of the first car he or she owned.[17]

This information-intensive method of payment authorization has required a widening set of personal information and an expanding computing and communications system to keep up with criminal efforts to commit fraud. Moreover, it provides an incentive for criminals to gather stores of information, either through public sources or by stealing information from private sources. Such information is valuable to criminals because payment authorization in the United States can allow payments fraud.

II. SMART CARDS AND THE SECURITY OF PAYMENT AUTHORIZATION

Payment smart cards hold the promise to improve the security of payment authorization and help reduce the costs of identity theft and payments fraud. Smart cards allow a range of security options and some issuers have implemented the strongest upgrades, while others have not. This section first reviews the most commonly deployed payment smart card, which is based on the EMV standard. It then describes an alternative, the X9.59 standard, which offers several features that can help in the fight against identity theft. The section ends with a review of security weaknesses that can remain even with payment smart cards.

EMV smart cards

EMV smart cards have powerful chips that allow advanced capabilities, such as encryption and generation of digital signatures (box).[18] EMV smart cards are based on the EMV standard, which was initially developed by the Mastercard, Visa, and JCB payment networks, which sponsor the standard, and is currently maintained by EMVCo LLC.[19] The standard was issued in 1996 and has subsequently been revised and supplemented. EMV cards require use of a PIN by the cardholder for each transaction and thus are often called "chip and PIN" cards. Using advanced security features on EMV cards would be considered strong payment authentication, but it is not clear how extensively these advanced features are used.

EMV payment cards are being adopted in a large number of countries worldwide (Finextra). The United Kingdom is notable for its commitment to this payment card, with the rollout beginning in late 2003 and all ATM and point-of-sale transactions in the UK required to use EMV cards in April 2006.[20] The entire European Union has targeted the end of 2010 for conversion to EMV cards. Canada and Mexico are also adopting EMV cards.

An EMV card is inserted into a merchant's terminal or into an ATM. The first step in the authorization process involves authenticating the card (Murdoch). Two common card authentication techniques are static data authentication (SDA) and dynamic data authentication (DDA).

ENCRYPTION AND DIGITAL SIGNATURES

The most advanced method of modern encryption uses a pair of matched keys, one to encrypt and one to decrypt (Anderson). If one key encrypts a message, the other must be used to decrypt, and vice versa. Because both keys are required for encryption and decryption, this method is called asymmetric encryption. The matched pair is unique so that one pair of keys will not work with another pair of keys.

If one of the keys is kept secret, a digital signature can be created. The secret key can be securely coded on a payment card and used to create an encrypted message. If the card issuer successfully decrypts the message using the matching key, then it can be sure that the message was sent using the card.

This particular use of encryption creates a "digital signature" because it is a message that is unique to a particular pair of encryption keys, similar to how handwritten signatures are unique to individuals. For this to work, the pair of keys must be assigned to particular individuals or devices, and the secret key must be used by only that individual or device. The assignment must be recorded and the information made available to users.

There are various ways that such assignment can be organized. A public key infrastructure (PKI) can be created where one or more organizations called *certificate authorities* can create and assign pairs of keys. One of the keys is kept secret and the other is made public. The certificate authority creates a certificate that identifies the individual or device using a pair of keys and discloses the public key. For the certificate to be trusted, the certificate authority must attest to the validity of the assignment and to the identity of the individual or device to which the encryption keys are assigned. As such, certificate authorities in a PKI must be well established and trustworthy.

An alternative method of organizing key assignments is for an organization to serve as its own certificate authority and use digital certificates for its internal purposes. For example, a bank may create and assign pairs of keys for each payment card it issues. The private key is encoded securely on the card, and the public key is stored on an internal computer database. When the card is used at an ATM or at a cash register, the card creates a digital signature that can be used to ensure the card issuer the signature was created by the payment card.

Under SDA, a digital signature using encrypted static information from the card is decrypted at the merchant's terminal to verify the card. Under DDA, a code unique to the transaction is encrypted on the card to create a digital signature. The signature is then decrypted at the merchant's terminal to verify the card.

The consumer enters a PIN to initiate the process that verifies the cardholder. The terminal sends the PIN to the card in clear text under SDA or encrypted under DDA. If the correct PIN has been entered, the transaction proceeds.

The next step authorizes the transaction. Depending on limits set by the card issuer, such as the value of the transaction and other risk parameters, the transaction may be authorized offline or online. Transactions considered low risk may be authorized offline by letting the decision be made at the terminal. Higher-risk transactions require online authorization, whereby an encoded message using the unique information for the transaction is sent to the card issuer (or its processor). The issuer decrypts the message and, if acceptable, sends a message authorizing the transaction.

Card issuers must decide whether to use SDA or DDA. The computer chips on SDA cards are less costly because encryption is not conducted on the card, but SDA is less secure than DDA. The static card verification under SDA is vulnerable because the authorization message can be copied and reused in another transaction.[21] PIN numbers are exposed as they are transmitted from terminal to card (Drimer and others). The PIN, along with other card information, can be used to create counterfeit magnetic stripe versions of the card. Another vulnerability on some SDA cards allows hackers to reprogram risk parameters to make the card accept any form of verification, such as a false PIN (a so-called "yes" card), allowing a stolen card to be used for fraud.

The UK, where a mix of SDA and DDA cards were issued, provides an early case study of the effect of the stronger payment authentication available on EMV cards. Total fraud losses in 2007 were actually 6 percent higher than in 2004, but the mix of fraud from various sources as well as the distribution of losses in and out of the UK changed substantially over this period (Table 2).

Losses due to lost or stolen cards and card ID theft fell 50.9 percent, reflecting the smart card's PIN requirement. Fraud declined by

Table 2

CREDIT AND DEBIT CARD FRAUD LOSSES ON UK-ISSUED CARDS

Fraud Type	2004 (£millions)	2007 (£millions)	Percent Change
TOTAL	504.8	535.2	6.0
Subcategories:			
Card-not-present fraud via phone, Internet, and mail order	150.8	290.5	92.6
Counterfeit (skimmed/cloned) card fraud	129.7	144.3	11.3
Fraud on lost or stolen cards	114.4	56.2	-50.9
Card ID theft (Account takeover and new accounts)	36.9	34.1	-7.6
Cards stolen from mail	72.9	10.2	-86.0
Contained within the total:			
Card present fraud in face-to-face UK retail transactions	218.8	73.0	-66.6
UK cash machine fraud	74.6	35.0	-53.1
Domestic/International split of total figure:			
UK fraud	412.3	327.6	-20.5
Fraud abroad	92.5	207.6	124.4

Note: Distribution of EMV cards began in October 2003. Use of EMV cards became mandatory on February 14, 2006.
Source: APACS.

large margins at both UK retailers and ATMs. The reduction in fraud on lost or stolen cards was significant, proving that UK issuers achieved a major goal of EMV deployment.

At the same time, fraud losses on card-not-present transactions increased 92.6 percent (phone, Internet, and mail order). Surprisingly, losses due to counterfeit cards rose 11.3 percent, despite the difficulty of counterfeiting a smart card. This happened in part because in the UK EMV cards carry all the information necessary to make them backwards compatible with magnetic stripe cards. If criminals intercept this information, they can create a counterfeit magnetic stripe card for use outside of the UK, where such cards are still accepted. In fact, fraud outside of the UK soared 124.5 percent from 2004 to 2007.

The United States, where magnetic stripe cards are standard, was the top destination in 2007 for fraud on UK payment cards (Balaban).

X9.59 standard

In the 1990s, a group was formed to assess payment authorization methods and develop a standard to secure all forms of electronic payments. The standard was approved for field testing in 2002, but so far has not been embraced by payment networks. The standard has potential to provide simplified, but strong, payment authorization. Equally important, it takes the incentive away from criminals to gather personal information for the purpose of committing payments fraud.

In an X9.59 transaction, the consumer presents a payment card to a merchant and enters a PIN to initiate the authorization process.[22] The consumer's bank and the merchant's bank verify the consumer and merchant using digital signatures. Authorization requests include a unique identifier for each transaction. The payment message is delivered to consumer and merchant banks using payment routing codes (PRCs). Sensitive information is encrypted, but only a few message elements are necessary for authentication, allowing a relatively compact message.

The X9.59 standard has a number of advantages. It does not require a public key infrastructure because banks act as certificate authorities by issuing encryption keys and assigning digital certificates to the accounts of both consumers and merchants.[23] Transaction-level identifiers prevent improper reuse of authorization messages. PRCs are to be used only for transactions that deliver strong authentication messages over the entire payment network. This limitation prevents card counterfeiting because, to be accepted, the PRC must be digitally signed, which requires a noncounterfeit card. PIN and possession of the card are strong factors of authentication that verify the cardholder, while the merchant's digital signature verifies the card terminal.[24] The type of encryption used does require a sophisticated chip on the card, and the standard simplifies the processing to the point that relatively modest processing power is needed.

Many of the strategies inherent in the X9.59 standard are being used in EMV cards, such as the requirement to use a PIN to verify the cardholder. But the X9.59 standard offers strong end-to-end security on low-cost chip cards without the need for a complex public key

infrastructure and with a drastically reduced need to harden the security of every element of a payment system (Wheeler). Most important, the standard eliminates personal information from payment authorization. Even if a criminal breaks into a database to obtain the PRC, the bank account number, name, and address of an accountholder, the information cannot be used in an X9.59 transaction because the criminal would not have the card. As a result, the motivation to perpetrate payments fraud from this form of identity theft is drastically reduced.

Smart card security weaknesses

EMV smart cards have had mixed results in the UK, due to several remaining security weaknesses. Some of the weaknesses have been demonstrated by computer experts.[25] In 2007, computer experts tested two of the most common EMV card readers in use in the UK at retail points-of-sale (Drimer and others). Despite satisfying EMV security standards, researchers found that both types of terminals had vulnerabilities. They successfully modified the terminals with a paper clip or needle, attached a recording device, and found that many EMV cards used SDA, allowing information exchanged between the card and the terminal to be captured without being detected. The information, which included a PIN code, would allow criminals to counterfeit a magnetic stripe version of the card or use the information in card-not-present transactions.

It is not known to what extent these vulnerabilities are being exploited, but they demonstrate that smart card hardware alone does not guarantee secure authentication. Choices, such as the use of static or dynamic data authentication to verify EMV cards, underscore the importance of security protocols. Insecure card readers illustrate how the entire line of communication for payment authorization must be protected.

More broadly, current strategy for authorization methods used in EMV cards adds encryption and digital signatures to an existing authorization model. To make this system work at the highest level of security, the payment card, card issuer, and merchant terminal must each have digital certificates. These in turn must be supported by a public key infrastructure. The complex infrastructure and trust relationships required to support this infrastructure have been seriously questioned by computer security experts (Ellison and Schneier). The messaging

volume becomes larger and more complex because messages may be required to verify each certificate. Message size is affected because encrypted messages are larger.

These concerns are less important with the X9.59 standard. Another important benefit of X9.59's reduced reliance on public information for authorization is that it greatly reduces the need for, and cost of, PCI DSS-mandated upgrading of security of the entire payments infrastructure.

But the full benefits of both the X9.59 and the EMV standards will not be realized as long as support remains for legacy payment systems. In particular, magnetic stripe cards and the current methods of conducting Internet transactions are vulnerable. These weaknesses attract even more criminal activity if security in other elements of the payments system is fortified.

III. ECONOMIC INCENTIVES FOR ADOPTING PAYMENT SMART CARDS

Both the EMV and X9.59 are feasible technologies that could reduce payments fraud, but neither technology has been adopted for payments in the United States. Lack of adoption may be related to how the market can limit incentives to adopt payment smart cards. Market incentives are tied to private benefits and costs, which can hold up adoption of payment smart cards even if their social benefits are greater than adoption costs. Limited incentives for adoption are related to the network nature of the payments system, support for legacy payment systems, and disruptions to business and consumer interests.

For issuers to adopt the payment smart cards, its private benefits must outweigh its costs. The cost of smart cards themselves has fallen considerably because computer chips are much less costly today than in the past, and the cost will continue to fall. Another significant cost involves upgrading the point-of-sale payment terminals and associated software. This type of cost could be minimized by requiring upgrades over an extended period (such as five years), so that installing a smart-card enabled payment terminal would be part of a normal equipment upgrade cycle. While trends in adoption costs are favorable, card issuers in the United States have not yet chosen to deploy payment smart cards.

Limited incentives for upgrading security of U.S. card payments remain significant because it is difficult to coordinate security efforts in a network market. First, payment participants' choices are driven

mainly by private costs and benefits. For example, the share of new account fraud resulting from identity theft has declined in recent years as the financial industry has more carefully verified the identity of consumers who apply for an account (Javelin 2008a). Because the cost of new account fraud is largely borne by financial institutions, it should be expected that they put considerable effort toward its reduction.[26] In general it is unlikely that the distribution of the costs of security upgrades will match the distribution of its benefits for banks, merchants, consumers, and government, which limits the extent to which individual incentives can control payments fraud. Moreover, if improvements to security standards for one element of the payment network reduce fraud elsewhere, one group of payment participants may "free ride" on the security upgrades of others.

Second, the spillover effects of security failures on the payment network can have an adverse impact on incentives to upgrade security. For example, the large 2006 data breach at TJX Companies, Inc., led to payments fraud that affected consumers and caused losses at card issuers. Card issuers also bore the expense of reissuing some payment cards. Although TJX faced considerable expense of it own, and reached settlements that reimbursed cardholders and card issuers (Aplin), it is not always clear that payment participants who are responsible for security breaches face the full cost of the consequential damage (Becket and Sapsford).[27] Moreover, implementation of the EMV standard has prompted some card networks to shift liability for fraud from card issuers to other payment participants, which can reduce the incentive of card issuers to limit fraud (Anderson and others). This has broad consequences because card networks and issuers have a great degree of control over security protocols in payment authorization.

The continued use of legacy payment instruments is a similar coordination problem. There is always a transition period when a payment network upgrades its technology so that payment options with weaker security coexist with those that have stronger security. As the UK experience shows, increased security of one form of payment may simply shift payments fraud to other payment options with weaker security. Subsidies and deadlines for adoption can help to reduce the length of the transition period. Perhaps more difficult is a commitment to abandon legacy payment options altogether.

Another challenge is that the revenue generated from payment services can be significant for some payment providers, and a change in payment security standards can affect those revenue streams. For example, estimates show that banks make more revenue from signature debit compared to PIN debit.[28] Because the EMV and X9.59 standards would essentially eliminate signature debit, bank revenue for payment services could be reduced.

Use of smart cards for payments will also require some adjustment of consumer habits. Consumers would lose the option of using a signature for payments, and card issuers are typically reluctant to limit consumer choices.[29] Consumer experience with Internet commerce would also change because payment smart cards might be required for Internet transactions.[30]

A long-term strategy must address security weaknesses by improving authorization of all types of payments.[31] Legacy payment instruments may need to be phased out so that over time payments will migrate to forms with strong authorization security. But new authorization protocols should avoid excessive disruption to business interests and significant customer inconvenience or they will not be adopted.

IV. THE ECONOMICS OF SECURITY STANDARDS

Economic forces related to upgrading technical standards can also slow adoption of payment smart cards. The replacement of older technical standards with new ones has been studied extensively by economists. The studies relevant to payments fall into two groups. The first concerns the network nature of payment systems, which may produce a potential bias away from common security standards and a tendency to entrench inferior security standards. The second group considers the process by which security standards are developed. To be successful, the standard setting process in payments must enourage consensus, have limited scope, and be carefully designed.

Network industries and standards entrenchment

One purpose of a security standard is to ensure compatibility. For example, the EMV standard must be used with a compatible card reader. In the United States, most payment card readers are not compatible. A payment network establishes its own security features, which can make

its payment instrument either compatible or incompatible with the hardware and communications systems of other payment networks.

Compatibility alone, however, may not ensure a move toward a stronger payment authentication standard. In markets where network externalities and economies of scale are strong, the industry is likely to emerge as an oligopoly (few firms) where there is one dominant firm. A dominant firm with loyal customers will likely be uninterested in establishing a common security standard, despite the efficiencies and enhanced social welfare that might accompany a common standard, because the firm may perceive a competitive advantage to incompatibility (Wiseman). If the benefits of standardization are strong enough, we may observe a coalition form to establish standards, as has happened with EMV. But gaining consensus can be difficult.

Economic analysis suggests that in the early stages of a network industry competing firms must quickly establish a base of customers in the race to become dominant. For example, below-cost pricing is a viable short-term strategy. But it also becomes possible that the firm that succeeds and becomes dominant in the industry does not have the best technology.

In the case of payments, the leader that emerges may not have the best security features.[32] Payment instruments have multiple features, and consumer adoption decisions will weigh all of the features. The network aspect of payments implies a strong benefit from widespread use. That is, if many others are using a particular payment option, then a consumer may decide to use it as well because it is more likely to be widely accepted.[33] Consumers may understand that one payment option has better security features than another, but nevertheless may adopt the payment option with inferior security if it is widely used.

An inferior security standard can be difficult to displace in a network market once it is in place. Customers decide to adopt a new product based on the number of others that use the product and the perceived benefits of shifting to a new product (Greenstein and Stango). Thus, a large installed base of an existing product is a barrier to adopting a new product with a superior technology. In the payments market, the larger the number of consumers and merchants using a particular security standard, the higher the perceived security benefit must be to justify a switch.

Standards development

Instead of market competition, a formal development process at the industry level can determine security standards. There are several such processes for payments in the United States. One is where an organization (or sponsor) has close control over the payments system and takes the lead in determining the standards for the system, such as in the Fedwire payments system or in credit card networks. An alternative is standard setting organizations (SSOs).

In the U.S. payments system there are two types of SSOs. Industry-based SSOs are voluntary and their memberships are drawn from a specific payment system, such as the National Automated Clearing House Association (NACHA), which oversees standards development and maintenance for the ACH system.[34] The second type of SSO is independent of specific payment systems. In the United States, the American National Standards Institute (ANSI) accredited the X9 committee for financial standards in 1984.[35] The X9 process is voluntary and depends on members of industry contributing resources to standards development.

A number of factors determine whether standards development will be successful. As mentioned above, consensus can be difficult to reach if firms perceive incompatibility as a competitive advantage. Some payments providers may have developed security technology independently and in some instances may have obtained patents and trade secrets they seek to exploit. Thus, intellectual property is a potential barrier to developing standards in the financial industry (Hunt and others).

The degree of control of the sponsor also plays a role in standards development. A sponsor with strong control over decisions can develop a standard more quickly than the decentralized process typical of an SSO. However, a closely controlled process may not succeed in generating a standard that gains consensus by those affected. Actual security depends not only on the features of the standard but also the degree to which it is implemented and followed. As a result, there may be a trade-off between speed of development and compliance with the standard.

Because some common interests in payments security exist, an SSO could usefully coordinate the development of payment security standards. To be successful, research suggests that the scope of the standard needs to be carefully defined, addressing a common business need but avoiding business processes that are closely tied to competitive advantage (Steinfeld

and others). The governance structure of the SSO must manage competing interests. Its success would depend on voluntary but open participation, limited costs of participation, clear rules for decision making that foster consensus, and a philosophy of participation that is based on self-interest but recognizes the common interest.

Participation in the SSO by a broad cross-section of the industry is valuable, but commitment of significant members of the industry is essential. The process also needs to encourage adoption of the standards, and it helps if actual participants act as change agents within their own organization through communication and education. Adoption is facilitated by standards that are well-defined, complete, and flexible. Follow-up may be needed for standards maintenance which may require a formal, ongoing organization.

Vested interests can make the work of SSOs difficult (Greenstein and Stango). The costs and benefits of adopting a standard will vary across affected parties, and as a consequence, some participants may delay or impede progress. A clear policy toward applicable intellectual property can avoid roadblocks and misunderstanding. Options such as compelling licenses for intellectual property can help the SSO reach consensus more quickly.

In short, both the network structure of the payments system and the difficulty of developing security standards can present barriers to improving payment authorization. The implication for payment smart cards is clear: Even if the societal benefits justify their cost, payment smart cards with strong authorization security may be adopted slowly.

V. SUMMARY AND CONCLUSION

Today there is great public concern about identity theft both because of its direct costs to victims and its invasion of privacy. From a public policy perspective, identity theft is a concern because it attacks the payment system and could undermine confidence in it. Market forces have generally worked well at limiting risk in retail payments and may be sufficient to answer the challenge of identity theft. But market forces depend on adequate incentives, and these incentives are increasingly unclear. Identity theft, for example, can occur because a consumer lends a payment card to an irresponsible friend, a card processor suffers a data breach, an Internet merchant does not use 3D Secure, or

card issuers accept weak authorization protocols. Identity theft blurs the line between responsibility for, and control of, payments fraud. Consequently, trends in payments fraud and identity theft need to be carefully monitored to ensure that it does not threaten the integrity of the payments system.

Payment providers are finding solutions to payments fraud and identity theft. Many of these efforts aim to bolster security of the payments network, but the results do not significantly change the basic underlying model of payment authorization. As a result, a costly effort is under way to harden the security of payment information when it is in transit and where it is stored. Authorization has shifted to more real-time data, which requires a complex and expensive infrastructure. Data requirements are increasingly intensive, especially for supplementary authorization. As long as authorization is information intensive, criminals have incentive to gather and exploit information to commit payments fraud.

The EMV standard relies on smart cards and can potentially introduce significant upgrades, such as two-factor cardholder verification—a smart card and a PIN—to fortify authorization security. However, the strongest security configuration is not always used, and EMV perpetuates the information-intensive method of payment authorization. The X9.59 payment security standard also uses two-factor authentication but relies less on personal information. Adoption of this standard would reduce the fear of exposing personal information on the Internet because it reduces the ability to use the information for payments fraud.

The use of smart cards to improve payment authorization methods faces significant challenges. The distribution of costs and benefits across payment participants determines the private incentives to improve methods of payment authorization, but the outcome of those efforts is not necessarily best from society's point of view. The tendency for criminals to shift their efforts toward areas of weakness implies that security in all types of payments needs to be fortified. But the view that security is a means to gaining competitive advantage reduces the willingness of payment providers to participate in developing a strong, common security standard. The complex network structure of payments makes coordination of standards development difficult. And even if there is consensus to develop a common, more secure authorization process, the

standard setting process must be well organized and pursued properly to avoid failure.

Smart cards have the potential to provide strong payment authorization and thus put a substantial dent into the problem of identity theft and payments fraud. The falling costs of infrastructure are tilting the cost-benefit calculation in favor of adopting payment smart cards in the United States. But some significant challenges must be overcome before smart card deployment can substantially improve the security of payment authorization.

ENDNOTES

[1]The most reliable statistics in Table 1 are the fraud losses for banks, consumers, and Internet merchants. Least reliable is the cost of PCI DSS compliance for merchants, but they are based on reports from industry experts.

[2]Non-retail losses to payments fraud by industrial and non-commercial firms are fairly minimal (AFP survey).

[3]This grossly understates the burden of fraud losses borne by Internet merchants. Credit card losses as a percent of sales are 1.4 percent for Internet retailers and under 0.05 percent for brick-and-mortar merchants. (Internet losses and rates of fraud are taken from CyberSource. The brick-and-mortar estimate is the $2 billion in losses shown in Table 1 divided by the $4.03 trillion estimate of total retail sales for 2006 (U.S. Census Bureau)).

[4]This estimate is the consumer portion of the costs of identity fraud reported in a recent survey (Javelin 2008a). An estimate of the cost of identity fraud to businesses would then be $35.4 billion (the $41.0 billion minus $5.6 billion). This estimate of business losses is problematic because the sum of all reported payments fraud losses in Table 2 is only $18.5 billion. Consumers may report the gross value of fraud that they experience, but businesses avoid a portion of those costs by preventing some fraud losses or by recovering funds after the fraud is discovered. The out-of-pocket losses reported by consumers is likely more credible because it represents their personal experience.

[5]It is unclear whether this represents an initial cost of upgrading security or whether this will be an ongoing cost.

[6]Existing account fraud represents an estimated 74 percent of all identity theft (Javelin 2008a). According to a 2004 survey, the median cost of existing credit card identity theft was $750 compared to $3,000 for new account fraud (Javelin 2005). One reason for the difference is that it takes longer to become aware of new account fraud so that the criminal has more time to run up charges.

[7]Data breach statistics calculated from publicly announced data breaches published by the Privacy Rights Clearinghouse *www.privacyrights.org/ar/ChronDataBreaches.htm.*

[8]A worldwide underground market for information useful for payments fraud has developed in the last few years (Anderson and others 2008).

[9]Another important phase of payment risk management is the verification of new customer identity and other information before issuing a payment instrument. This article focuses on transaction-level authorization.

[10]Sometime between 2003 and 2006, the number of card payment transactions surpassed check transactions in U.S. retail payments (Federal Reserve System).

[11]The example presented here uses *online* authorization where communication with a payment processor is used for immediate, real-time access to information. *Offline* authorization occurs without such communication, but as with online authorization the card issuer sets risk parameters that a transaction must

satisfy before it is authorized, such as inspection of the payment card and screens that check of consistency of information stored on the card. Offline authorization serves as a fall-back option when card readers malfunction, lines of communication are unavailable or if the card processor's system is down. Offline authorization is also less expensive and is sometimes used for low-value, low-risk transactions.

[12]Visa and MasterCard call these card verification values (CVV) and card verification codes (CVC).

[13]Visa's program is called Verified-by-Visa, MasterCard's is SecureCode, and JBC International is J/Secure.

[14]One analyst reports that 49 percent of transactional fraud is from card-not-present transactions (Green).

[15]If an authorized transaction turns out to be fraudulent, then the merchant's bank will "chargeback" the transaction. That is, it will recover the funds for the payment from the merchant's account. The merchant, rather than the card issuing bank, bears the risk of payment card fraud. As a result, managing chargebacks is becoming routine among Internet merchants and can be a significant expense (CyberSource). The merchant can transfer this risk to the card issuing bank if it participates in a 3D Secure program.

[16]Some payments, such as check and ACH, can be authorized using a bank routing number, a consumer account number, and other relevant information.

[17]Concern for security led bank supervisors to require stronger security in Internet banking and payments (Board of Governors), and as a result many financial institutions have used these challenge and response systems.

[18]Recently, contactless payment cards have been deployed in the United States that communicate with readers via radio frequency signals. These cards could be called smart cards because they use electronic chips for radio communication. However, the cards are essentially the same as magnetic stripe cards in the way they are authenticated and the associated payment is authorized and will therefore not be discussed in this article.

[19]EMV is named after the original sponsors of the standard, Europay, Mastercard, and Visa. Europay was later absorbed by MasterCard. JCB joined the standard in 2004. For more information, visit *www.emvco.com*.

[20]Visit *www.chipandpin.co.uk* for more information on the UK chip and PIN program.

[21]This weakness is referred to as a "replay attack."

[22]This description is based on a particular implementation of X9.59 called the account authority digital signatures (AADS) and used at brick-and-mortar retailers. The X9.59 standard is adaptable to other implementations. See *www.garlic.com/~lynn* for more information on X9.59 and AADS.

[23]Certificate authorities attest that specific encryption keys are assigned to specific individuals, and a public key infrastructure supports the use and integrity of digital signatures. Box 1 explains these terms in more detail.

[24]Factors of authentication are independent means of verifying an individual or device. In general, more factors imply stronger security.

[25]Contactless cards in the U.S. also have some security weaknesses. In 2006, computer scientists put together a contactless card reader and tapped it with unopened envelopes that contained contactless payment cards issues by U.S. banks (Schwartz). The investigators could read the cardholder's name, card number, and the card's expiration date. Tests revealed that 20 cards—each issued in 2006—all failed at least one method of attack. In at least one instance, the card information was used to conduct a transaction. Card issuers and networks claim implementation of contactless cards is secure, but reports of skimming vulnerability of U.S. bank-issued contactless cards have been published as late as February 2008 (Vamosi).

[26]Another possible indication that card issuer anti-fraud efforts do not place the highest priority on protecting cardholders is that the average out-of-pocket cost per identity theft victim rose in 2007 to $691, up 25 percent from the $554 average reported in 2006 (Javelin 2008b).

[27]Economists refer to the disconnect between costs and responsibility as an externality.

[28]This is true even after adjustments for higher fraud losses of signature over PIN debit. Revenue for signature debit is estimated to be 65 basis points higher than PIN debit (Pulse), while the differential for fraud losses is about 4 basis points (Star Systems 2005).

[29]This inconvenience may be limited because surveys suggest that since 2001 consumers have preferred PIN to signature debit (Star Systems 2006; Dove Consulting 2005; Boyer). Consumer inconvenience is further limited by the trend towards eliminating the requirement for either a signature or a PIN in low-value payments.

[30]To enable these transactions, consumer computers might need be equipped with smart card readers.

[31]Protocols have already been designed to adapt EMV and X9.59 standards for Internet payments (Levi and Koç; Khu-Smith and Mitchell).

[32]This is not necessarily an example of market failure. If the market has incomplete information—for example, is unable to anticipate future threats—then security standards may be put into place that become inadequate at some time in the future.

[33]Economists refer to the consumer benefit from widespread use a usage externality.

[34]NACHA develops both technical standards (such as ACH message formats) as well as standards for business practices that aim at managing risk.

[35]A significant part of the committee's work concerns security, but it also determines standards for the formats of electronic payment messages, the formats for paper checks, payment processing, and electronic credit records. Consult the X9 committee website (*www.X9.org/home)* for more information. ANSI is a subgroup of the International Standards Organization (ISO).

REFERENCES

Acohido, Byron, and Jon Swartz. 2008. *Zero Day Threat: The Shocking Truth of How Banks and Credit Bureaus Help Cyber Crooks Steal Your Money and Identity.* Somerville, Mass.: Union Square Press.

American Bankers Association. 2007. "Attempted Check Fraud Doubles to $12.2 Billion According to ABA Survey," news release, November 27, *www.aba.com/Press+Room/ 112707Deposit+FraudSurvey.htm.*

Anderson, Ross. 2001. "Cryptography," *Security Engineering.* New York: John Wiley, chapter 5.

_____, Mike Bond, and Steven J. Murdoch. No date. "Chip and Spin," *www.chipandspin.co.uk/spin.pdf.*

_____, Rainer Böhme, Richard Clayton, and Tyler Moore. 2008. "Security Economics and European Policy," paper presented at Workshop on the Economics of Information Security, *weis2008.econinfosec.org/papers/MooreSecurity.pdf.*

APACS. 2008. "Fraud Abroad Pushes Up Losses on UK Cards Following Two-Year Fall," press release, March 12, *www.apacs.org.uk/2007Fraudfiguresrelease.html#.*

Aplin, Donald G. 2008. "TJX Announces Settlement with MasterCard," *BNA Banking Daily*, April 3.

Association for Financial Professionals. 2007. "2007 AFP Payments Fraud Survey," March, *www.afponline.org/pub/pdf/2007PaymentsFraudSurvey.pdf.*

Balaban, Dan. 2008. "Losses Mount as Fraudsters Evade UK Chip Card Protections," *Cars & Payments*, July, pp. 14-18.

Becket, Paul, and Jathon Sapsford. 2003. "Signature Problems: As Credit Card Theft Grows, a Tussle Over Paying to Stop It," *Wall Street Journal*, May 1, p. A1.

Benton, Marques, Krista Blair, Marianne Crowe, and Scott Schuh. 2007. "The Boston Fed Study of Consumer Behavior and Payment Choice: A Survey of Federal Reserve System Employees," Federal Reserve Bank of Boston, Public Policy Discussion Paper 07-01, February 14, *www.bos.frb.org/economic/ppdp/2007/ppdp0701.pdf.*

Bills, Steve. 2006. "Shifting Payment Patterns Altering Fraud Landscape," *American Banker*, April 6.

Board of Governors of the Federal Reserve System. 2005. "Interagency Guidance on Authentication in an Internet Banking Environment," Supervision and Regulation, letter SR 05-19, October 13, *www.federalreserve.gov/boarddocs/SRLETTERS/2005 /sr0519.htm.*

Boyer, Megan. 2008. "Public Picks PIN Over Signature in Payment-Preferences Survey," *American Banker*, February 21, p. 1.

CyberSource. 2008. "9th Annual Online Fraud Report," download through *www.cybersource.com/cgi-bin/pages/prep.cgi?page=/promo/FraudReport2008NA/index17.html.*

Dove Consulting. 2005. 2005/2006 *Study of Consumer Payment Preferences.*

_____. 2007. "Highlights from the 2007 Debit Issuer Study," On Payments Issue #18, *www.doveconsulting.com/onpayments/onpaymentsweb.html.*

Drimer, Saar, Steven J. Murdoch, and Ross Anderson. 2008. "Thinking Inside the Box: System-Level Failures of Tamper Proofing," University of Cambridge Computer Laboratory, Technical Report No. 711, February, *www.cl.cam.ac.uk/techreports/UCAM-CL-TR-711.pdf.*

Ellison, Carl, and Bruce Schneier. 2000. "Ten Risks of PKI: What You're Not Being Told about Public Key Infrastructure," Computer Security Journal, vol. 16, no. 1, *www.schneier.com/paper-pki.pdf.*

Fabian, Thecia. 2007. "ABA Survey Finds Rapid Check Scam Rise," BNA Banking Daily, November 28.

Federal Reserve System. 2007. "The 2007 Federal Reserve Payments Study," December 10, *www.frbservices.org/files/communications/pdf/research/2007_payments _study.pdf.*

Finextra. 2008. "MasterCard Passes 300 Million Mark for EMV Cards Shipped," Finextra.com, March 6, *www.finextra.com/fullpr.asp?id=20267.*

Gordon, Gary R., Donald J. Rebenovich, Kyung-Seok Choo, and Judith B. Gordon. 2007. "Identity Fraud Trends and Patterns: Building a Data-Based Foundation for Proactive Enforcement," Utica College, Center for Identity Management and Information Protection, October.

Green, Mark. 2008. "Divided We Fall: Fighting Payments Fraud Together," presentation at 2008 Payments Conference sponsored by Federal Reserve Bank of Chicago, *Payments Fraud: Perception Versus Reality*, *www.chicagofed.org/news and_conferences/conferences_and_ events/files/2008_ payments_greene.pdf.*

Greenstein, Shane, and Victor Stango. 2007. "Introduction," in S. Greenstein and V. Stango, eds., *Standards and Public Policy*. Cambridge: Cambridge University Press, pp. 1-17.

Horrigan, John B. 2008. "Online Shopping: Internet Users Like the Convenience But Worry About the Security of Their Financial Information," Pew Internet and American Life Project, February 13, *www.pewinternet.org/pdfs/PIP_Online%20Shopping.pdf.*

Hunt, Robert M., S. Simojoki, And T. Takalo. 2007. "Intellectual Property Rights and Standard Setting in Financial Services: The Case of the Single European Payments Area," Federal Reserve Bank of Philadelphia, Working Paper 07-20, August, *www.philadelphiafed.org/files/wps/2007/wp07-20.pdf.*

Javelin Strategy and Research. 2008a. "2008 Identity Fraud Survey Report Excerpts for Card Issuers," *www.javelinstrategy.com/uploads/803 1.R_2008IdentityFraudSurveyReportforIssuers_ Brochure.pdf.*

_____. 2008b. "New Research Confirms Identity Fraud Is On Decline," press release, *www.javelinstrategy.com/2008/02/11/new-research-confirms-identity-fraud-is-on-decline/.*

_____. 2005. "2005 Identity Fraud Survey Report," January.

Khu-Smith, Vorapranee, and Chris J. Mitchell. 2002. "Using EMV Cards to Protect E-commerce Transations," in K. Bauknecht, A Min Tjoa, and G. Quirchmayr, eds., *E-Commerce and Web Technologies: Proceeding of the Third Annual Conference*. Berlin: Springer, pp. 388-99.

Kusovski, Boris. 2008. "'Competitive' Fraud Landscape Review," presentation to Financial Services Technology Consortium, March. *www.fstc.org/docs/email/FSTC%20Presentation%20IBM%20Fraud% 20Overview.pdf.*

Levi, Albert, and Ç. Kaya Koç. 2001. "CONSEPP: CONvenient and Secure Electronic Payment Protocol Based on X9.59," *Proceedings, 17th Annual Computer Security Applications Conference*. Los Alamitos, Calif.: IEEE Computer Society Press, pp. 286-95.

Meacham, Jennifer D. 2008. "Credit Card Fraud: How Big Is the Problem?" *Practical eCommerce*, April 23, *www.practicalecommerce.com/articles/720/Credit-Card-Fraud:-How-Big-Is-The-Problem?/.*

Mott, Steve. 2007a. "Why POS Merchants Don't Buy into Payment Security," *Digital Transactions News*, *www.digitaltransactions.net/newsstory.cfm?newsid=1503.*

_____. 2007b. "When It Comes to Online Security, It's All About the Money," *Digital Transactions News*, www.digitaltransactions.net/newsstory.cfm?newsid=1515.

Murdoch, Seven J. 2007. "EMV Flaws and Fixes: Vulnerabilities in Smart Card Payment Systems," COSIC seminar, June 11, *www.cl.cam.ac.uk/~sjm217/talks/leuven07emv.pdf.*

Nilson Report. 2007. "Credit Card Fraud-U.S.," *Nilson Report* 876, March, pp. 1, 9.

Payments News. 2008. "A Deeper Dive into the Cost of PCI Compliance," *Payments News*, May 16, *www.paymentsnews.com/ 2008/05/more-on-the-cos.html.*

_____. 2008. "What's the Industry Cost of PCI Compliance?" Payments News, May 14, *www.paymentsnews.com/ 2008/05/whats-the-indus.html.*

President's Task Force on Identity Theft. 2007. *Combating Identity Theft: A Strategic Plan*, April.

Pulse EFT Association. 2007. "New Comprehensive PULSE Debit Industry Study Reveals Continued Growth in Debit Card Market," press release, February 28.

Schreft, Stacey L. 2007. "Risks of Identity Theft: Can the Market Protect the Payment System?" Federal Reserve Bank of Kansas City, *Economic Review*, Fourth Quarter.

Schwartz, John. 2006. "Researchers See Privacy Pitfalls in No-Swipe Credit Cards," *New York Times*, October 23, *www.nytimes.com/2006/10/23/business/23card.html.*

Star Systems. 2007. *Star POS Debit Cost Study.*

_____. 2006. *Consumer Payments Usage Study.*

Steinfeld, Charles W., Rolf T. Wigand, M. Lynne Markus, and Gabe Minton. 2007. "Promoting E-business Through Vertical IS Standards: Lessons from the US Home Mortgage Industry," in S. Greenstein and V. Stango, eds., *Standards and Public Policy*. Cambridge: Cambridge University Press, chapter 5, pp. 160-207.

U.S. Census Bureau. 2007. "Estimated Annual Retail and Food Services Sales by Kind of Business: 1992 through 2006." Statistics release, March 7, 2008, *www.census.gov/svsd/retlann/pdf/sales.pdf.*

Vamosi, Robert. 2008. "The Hands-Free Way to Steal a Credit Card," CNET, February 21, with update on February 22, *http://news.cnet.com/8301-10789_3-9875961-57.html.*

Ward, Michael. 2006. "EMV Card Payments-An Update," *Information Security, Technical Report* 11, pp. 89-92.

Wheeler, Lynn. 2006. "Naked Payments I-New ISO Standard for Payments Security: the Emperor's New Clothes?" *Financial Cryptography* website, June 10, *financialcryptography.com/mt/archives/000745.html.*

Wiseman, Alan E. 2000. "Network Effects," *The Internet Economy: Access, Taxes, and Market Structure*. Washington, D.C.: Brookings Institution Press, chapter 5, pp. 68-86.

Yip, Pamela. 2008. "Scanning for Identity Theft." *Kansas City Star*, July 6, p. D3, *www.paymentsnews.com/ 2008/05/more-on-the-cos.html.*