The Laws, Regulations, and Industry Practices That Protect Consumers Who Use Electronic Payment Systems: Policy Considerations

Mark Furletti*

October 2005

Summary: *This is the third in a series of three papers that examines the laws, regulations, and voluntary industry practices that may aid consumers who contest an electronic transaction because of error, fraud, or merchant dispute. The first two papers describe the complex web of protections available to users of four popular electronic payment mechanisms: credit cards, debit cards, prepaid cards, and ACH e-checks. This third paper considers how protections related to fraud, error, and disputes affect market participants. The paper concludes that (i) the current protection mechanisms make it more difficult to encourage the adoption of fraud-reduction schemes, (ii) the current protections represent a significant cost to banks, merchants, processors, and consumers, and (iii) the present federal system of protection, while encouraging innovation and thoughtful regulation, leads to consumer confusion.*

* Payment Cards Center, Federal Reserve Bank of Philadelphia, Ten Independence Mall, Philadelphia, PA 19106. E-mail: mark.furletti@phil.frb.org. Thanks to Christopher Ody for excellent research assistance. The views expressed here are not necessarily those of this Reserve Bank or of the Federal Reserve System.

FEDERAL RESERVE BANK OF PHILADELPHIA

Ten Independence Mall, Philadelphia, PA 19106-1574 • (215) 574-7220 • www.philadelphiafed.org/pcc

I. Introduction

In 2003, consumers used electronic forms of payment to execute almost 45 billion transactions involving $2.5 trillion in goods and services.[1] While the overwhelming majority of these transactions were cleared and settled without incident, some were contested by consumers as being fraudulent or erroneous or became the subject of a dispute with a merchant. This is the third in a series of papers that examines the laws, regulations, and voluntary industry practices that may aid consumers who contest an electronic transaction for one of these reasons. The first two papers, which can be accessed on the Center's website,[2] describe in detail the complicated web of protection available to users of four popular electronic payment mechanisms: credit cards, debit cards, prepaid cards, and ACH e-checks. (For a high-level, tabular summary of the consumer protections available on these mechanisms, see Appendix A.) These products are used to conduct over 90 percent of all electronic consumer payment transactions.[3]

This third paper considers how the protections associated with the four payment products profiled affect market participants. This analysis yields three conclusions: First, the current protection mechanisms make it more difficult to encourage the adoption of fraud-reduction schemes. Second, the current protections represent a significant cost to banks, merchants, processors, and consumers. Finally, the federal portion of the current system, while promoting innovation and well-thought-out regulation, leads to consumer confusion.

II. How Mandatory and Voluntary Consumer Protections Affect Payment System Participants

As described in the two earlier papers, consumers of most electronic payment products are protected from fraud, error, and dispute by relatively strong federal laws, network rules, and

[1] *The Nilson Report*, No. 823, Dec. 2004, p. 6.
[2] These other papers are available at www.philadelphiafed.org/pcc/papers.
[3] NACHA and *The Nilson Report* (No. 823) report that consumers conducted 45 billion electronic transactions in 2003, divided among the various forms of electronic payment as follows: credit cards (21 billion), debit cards (16 billion), prepaid cards (2 billion), ACH e-checks (1 billion), and other ACH (2 billion). (Due to rounding, numbers do not add to 45 billion.)

internal bank policies. As a result, consumers of the most popular electronic payment products face virtually no liability for erroneous transactions and very limited liability for fraudulent transactions. In addition, they have access to a dispute-resolution process that often favors consumer interests. Shielding consumers from most forms of liability and furnishing them with an array of complex federal rights and voluntary protections, however, is costly and difficult. Such protections require that parties with diverse interests, such as card issuers, merchants, merchant banks, and payment networks, settle a variety of thorny issues, including how the costs of these protections should be allocated, how the information systems that will handle consumers' claims should be designed, and how to settle disputes that may arise among industry participants.

The following examines how the protections provided to consumers and the complex infrastructure designed to support these protections influence the behavior of consumers who engage in these types of payment transactions. This analysis focuses on the credit and debit card systems, since these payment vehicles handle the vast majority of consumer electronic payments. Information in this section comes, in part, from interviews the author conducted with merchants, issuers, and processors while researching the first two papers.

A. Making It More Difficult to Adopt Fraud-Reducing Technologies

Arguably, the most valuable consumer protection described in this series of papers pertains to fraudulent transactions. Because of Regulations E and Z, the associations' zero liability policies, and issuers' own practices, consumers of credit and debit cards are shielded from nearly $3 billion in fraud losses each year.[4] Internal rules developed by the associations allocate this expense among merchants, merchant banks, card issuers, and the associations themselves. This section examines these rules, the incentives that underlie the associations' fraud allocation systems, and the effects of these rules and incentives on the behaviors of the various parties to a credit or debit card transaction. My analysis proposes "ideals" for structuring a fraud

[4] See Appendix C for details and sources related to this estimate of fraud loss.

allocation system, examines the current system, and measures the current system against the ideals.

1. The ideal system

If one could design an ideal system of allocating fraud liability among various parties to a fraudulent card transaction, what kinds of behaviors would the system seek to encourage? First, and perhaps most important, the system would encourage the widespread use of payment cards by consumers. In general, consumers are risk adverse and will disproportionately underuse a payment product they believe is risky. For this reason, an ideal fraud allocation system would convince consumers that any checking account balances or lines of credit associated with a payment card are safe and easily replaceable in the event of theft. Without trust in the system's ability to indemnify victims of random acts of fraud or theft, consumers would be hesitant to use it.

Second, the rules of allocating liability in the ideal system would encourage parties to the transaction to exercise due care. System participants, such as consumers, issuers, and merchants, would work to minimize fraudulent activities over which they have some measure of control. Consumers, for example, would take special care to safeguard their cards and monitor their accounts for suspicious activity; issuers would create secure cards and card processing systems that would be difficult to compromise; and merchants would properly use card processing systems and take measures to verify that the cards presented to them actually belong to those doing the presenting. In short, each party would take some simple and relatively cost effective steps that, together, would reduce the system's exposure to most types of fraud.

Finally, in an ideal environment, payment system participants would adopt any fraud-reduction strategy that saved the entire system more money than it cost, even if the benefits of

such a strategy accrued disproportionately to the parties involved.[5] Consider, for example, a hypothetical fraud strategy that could halve the total fraud occurring in the system at a cost equal to 10 percent of total fraud. In an ideal payment system, the strategy would be adopted, even if no single participant experienced enough savings to entirely pay for the strategy's implementation on its own.[6]

2. The current system

I now examine the current fraud allocation system and its incentives. For the purpose of this analysis, four parties are considered: consumers, traditional brick-and-mortar merchants, Internet and catalogue merchants, and card issuers. The payment card networks that make the rules with respect to fraud allocation are also critical entities. But since the major networks in the U.S., i.e., MasterCard, Visa, American Express, and Discover, are controlled by those who issue cards,[7] I will assume that issuer interests and network interests are aligned.[8] Another important entity in a card payment transaction is the merchant's bank. In general, however, any fraud expense incurred by a merchant bank on behalf of a merchant is immediately passed along to the merchant. Appendix B includes a diagram of a typical card transaction, including the parties discussed above.

[5] As used here, the term "cost" includes more than just fraud losses and the expense of anti-fraud technologies and systems. It also includes the time it takes users of a proposed fraud-reduction scheme to meet its requirements and the cost of any legitimate sales lost because of fraud screening.

[6] The type of efficiency described here, in which an improvement to a system will be made as long as its benefits outweigh its costs, is typically referred to as Kaldor-Hicks efficiency. It is different from so-called Pareto efficiency in which a change to the system is made only if it makes some better off and no one worse off.

[7] In August 2005, MasterCard announced that it will overhaul its corporate governance and ownership structure. As part of this overhaul, it plans to become a publicly traded company and shift control of the entity from its existing bank shareholders to investors. It is unclear how this change will affect the relationship between MasterCard and the banks that have traditionally controlled it. See MasterCard press release, "MasterCard Announces Plans for New Governance and Ownership," Aug. 31, 2005, available at www.mastercardinternational.com/cgi-bin/newsroom.cgi?id=1081&category=all.

[8] In the case of American Express and Discover, the issuing bank and network are operated by the same company. As a result, network and issuer interests in their cases are perfectly aligned.

At present, the parties to a credit or debit card transaction incur approximately $3 billion in fraud losses each year.[9] Given the "zero liability" policy of the associations and the strong protections afforded consumers under Regulations Z and E, however, few of the losses associated with fraud are borne by consumers. Specifically, consumers are likely to bear responsibility for fraudulent charges in just two rare cases: when an issuer can prove that a debit card customer purposefully delayed reporting a lost or stolen card and when a debit card customer does not discover fraud because he did not review his statements for more than two months. While there may be consumers who experience losses for these two reasons (and there may be some issuers that do not waive the $50 of federal liability), consumers generally have negligent exposure to card fraud losses. A chart detailing the losses consumers and others experience because of fraud by card product type is presented in Appendix C.

Like consumers, traditional brick-and-mortar merchants also face very little liability for fraudulent transactions. Under the rules of the bank card associations (and those of the PIN debit networks), brick-and-mortar merchants that properly authorize a "card present" transaction have little or no liability if that transaction turns out to be fraudulent. Publicly available excerpts from MasterCard's 2004 Chargeback Guide[10] explain that merchants accepting cards must generally do the following to avoid liability for fraudulent transactions: determine if the card is valid by examining its expiration date, signature, and other security features; obtain authorization for the card's use; provide consumers with a detailed receipt; obtain the cardholder's signature; and compare the signature obtained to the one on the back of the card. While brick-and-mortar merchants interviewed for this paper explained that they did experience fraud losses for card present transactions (because, for example, employees failed to follow proper point-of-sale procedures), the incidence and cost of this fraud are relatively low.

[9] The $3 billion includes the cost associated with goods and services stolen by thieves as a result of fraud. It does not include a myriad of indirect fraud costs, such as the cost of fraud-reducing technologies and bank employees that monitor fraud.

[10] Available at www.mastercardmerchant.com/docs/accept_mastercard/merchant_rules.pdf.

Internet and catalogue merchants, unlike their brick-and-mortar counterparts, bear significant liability for fraudulent transactions. This is the case because, under the rules of the bank card associations, liability for fraud shifts from card issuers to merchants when a transaction is effected without an actual piece of plastic. Presumably, this shift occurs because, without access to the physical card, traditional security features (e.g., magnetic stripe, signature panel, or hologram) cannot be used for authentication. Last year, Internet and catalogue merchants paid nearly $2 billion back to card issuing banks and their customers to cover card-not-present fraud.[11] This represented 1.8 percent (180 basis points) of all online transaction volume.[12] In an effort to reduce their losses, Internet and catalogue merchants have individually invested in a variety of fraud-reducing tools. These tools, which include address verification services, internally built fraud screens, geo-locators, customer history searches, and card verification code checks, can be expensive for merchants to purchase and implement and lead to the rejection of some legitimate consumer orders.[13]

Despite being able to charge back card-not-present fraud losses to Internet and catalogue merchants, card issuers are required under association rules to absorb most of the losses associated with traditional brick-and-mortar merchant fraud. Last year, card issuers paid for approximately $1 billion of the system's fraud losses, mostly as a result of cards being lost, stolen, or counterfeited. As a percentage of the volume that flows through the associations' networks, this represented approximately 0.05 percent (5 basis points)—a record low.[14] Over the past decade card issuers have made great strides in reducing the types of fraud for which they are

[11] Estimate based on a 2005 CyberSource Online Fraud Report (available upon request from CyberSource). It includes both fraud chargebacks to merchants from issuers and credits issued by merchants to consumers because of fraud. While some in the card industry doubt that Internet merchants absorb this much fraud, it is clear that these retailers bear more of the burden of fraud than any other parties discussed here.
[12] 2005 CyberSource Online Fraud Report.
[13] The 2005 CyberSource Online Fraud Report finds the following with respect to Internet merchants: spending on fraud management tools is equivalent to 0.40 percent of total online revenues; direct fraud losses are equivalent to 1.8 percent of total online revenues; and over 5 percent of all Internet sales are rejected because of a suspicion of fraud.
[14] See *The Nilson Report*, March 2005 (#830) and May 2005 (#833).

liable by improving card activation procedures, monitoring card transactions, and adding more sophisticated security features to the card.

3. The ideal system vs. the current system

As described earlier, an ideal system of fraud allocation would accomplish three goals: It would encourage consumer usage of card products, provide parties with incentives to exercise due care, and adopt any fraud-reduction schemes that provide a net benefit to the system as a whole. I argue that the current fraud allocation scheme accomplishes the first of these three goals and falls short with respect to the last two.

By fully insulating most consumers from the liability associated with fraudulent transactions, the current system promotes consumer confidence and, as a result, encourages the widespread use of cards. Evidence of this can be seen in consumers' aggressive adoption of card-based payment products. Credit cards, for example, have become nearly ubiquitous, with three-quarters of U.S. families owning at least one card.[15] Debit cards have also become exceptionally popular. From 1998 to 2003, for example, the percentage of households that owned a debit card increased from 37 percent to 54 percent.[16] In total, credit and debit card purchases now account for almost half of all noncash payments.[17] Overall, the consumer-friendly fraud allocation system adopted by the payment networks approaches the hypothetical ideal in that it has contributed to the widespread adoption of credit and debit cards by consumers.

While the current system achieves nearly ideal levels of consumer adoption, it does so at the expense of another ideal—that of encouraging parties to exercise care. This is the case because the system resolves two competing interests—encouraging consumers to use the payment networks and requiring that they bear the costs of their behaviors—in favor of the consumer. For example, even a consumer who writes his personal identification number (PIN) on the front of his

[15] Thomas A. Durkin, "Credit Cards: Use and Consumer Attitudes, 1970-2000," *Federal Reserve Bulletin*, September 2000, p.625.
[16] Christoslav E. Anguelov et al., "U.S. Consumers and Electronic Banking, 1995-2003," *Federal Reserve Bulletin*, Winter 2004, p.6.
[17] Federal Reserve System, "Federal Reserve Payments Study, 2003," December 2004, p.4.

card with permanent pen is not responsible for subsequent PIN-debit losses as long as he reports the theft of his card or discovers the fraud within relatively generous time frames.[18] These pro-consumer fraud policies make it difficult for card issuers and merchants to encourage consumers to take the relatively simple steps within their control to reduce the system's exposure to fraud. Another example of this is the difficulty Visa is experiencing in enrolling consumers in Verified by Visa (VbV), an Internet payment authentication scheme. While Visa has significantly increased the number of merchants that accept VbV through price incentives, it has not yet enrolled even 1 percent of its U.S. consumer card base.[19] Given consumers' incentives (i.e., zero liability for Internet fraud losses), one would not expect consumers to adopt VbV without a change to the current system.

The incentives built into the current system also fail to encourage brick-and-mortar merchants to exercise reasonable care in order to avoid fraud. In theory, merchants must go through a variety of steps (e.g., examining card security features, verifying signatures) when accepting a credit or debit card in order to avoid any liability for fraud. In practice, however, merchants are challenged to be as exacting as the rules require and often do not attempt to verify signatures or ask for identification when the signature panel is illegible. Fraud losses that result because of a failure to verify a signature are typically covered by issuers because it is difficult for issuers to prove that a merchant did not follow the proper procedures.[20] Because brick-and-mortar merchants are generally not responsible for this fraud, they have little incentive to carefully examine signatures and ask for identification when necessary. In an ideal system, however, merchants would be encouraged to use the simple tools available to them, i.e., the ability to simultaneously observe the card and the signing of the receipt, to avoid losses.

---

[18] See Official Staff Commentary to Regulation E, 12 C.F.R. § 205.6(b)-2 (2005).
[19] John Stewart, "Behind the Buzz in Authentication," *Digital Transactions*, Jan./Feb. 2005, p. 34.
[20] This is the case because a card used to perpetrate fraud is rarely recovered, and, as a result, it is often impossible to verify that the signature on the back of the card differs from the signature on a receipt. In many cases, a thief or counterfeiter will actually sign or re-sign the back of the card with his own hand, rendering verification by the merchant ineffective.

The current fraud allocation system is also less than ideal in that it has not encouraged the adoption of more efficient tools to fight Internet fraud. Ideally, a fraud allocation system would encourage merchants, issuers, and consumers to adopt any fraud management strategy that would represent a net benefit to the system. Because the present fraud allocation rules place all liability for Internet fraud on Internet merchants, however, there is little incentive for consumers or issuers to adopt systemwide tools that prevent Internet-based fraud. As a result, the thousands of merchants that do business on the Internet have had to independently shop for and deploy relatively small-scale solutions to combat fraud. One would assume that a common solution for all Internet merchants would be less expensive and provide a level of fraud protection that is more effective. (To the extent necessary, merchants could then supplement this common solution with additional fraud-fighting strategies.) But because incentives are misaligned, even if card issuers could, for example, build a fraud-fighting machine at a one-time cost of $1 billion that would permanently reduce Internet fraud by 80 percent, they have little reason to do so. Such a system would be of little benefit to issuers and costly. Ideally, however, Internet merchants could compensate issuers for this expense and the common solution would be adopted.

It is clear that the current rules for allocating fraud liability among the various parties to a card transaction have contributed to a very high level of consumer adoption of credit and debit cards. It is also clear that, because of strong economic incentives, issuers have done an excellent job combating the brick-and-mortar-merchant fraud for which issuers themselves are liable. The incentive structure has so far failed, however, to encourage system participants to adopt fraud prevention tools for Internet purchases that are as effective or efficient as those used in the brick-and-mortar environment.

B. Increasing the Costs of Consumer Goods and Services

In addition to influencing the adoption of fraud reduction schemes, the systems of protection described in the two earlier papers in this series significantly increase the cost of electronic payments. As described in the first two papers, depending on card type and issuer, a

payment card transaction may be protected by a variety of federal laws and voluntary policies. All market participants may not appreciate, however, the expense of these protections and how these protections likely increase the cost of the goods and services that are consumed.

In general, the expense associated with providing fraud, error, and dispute protection has two components: a direct cost component and a processing cost component. In the context of a fraudulent transaction, the direct cost component is the value of the good or service that is stolen by the perpetrator of the fraud. As described in the previous section, direct fraud losses from debit and credit card use totals approximately $3 billion per year. In the case of dispute, the direct cost is the value of any goods or services for which the consumer will not be liable (but for which the issuer or merchant will take responsibility). It is difficult to estimate the extent of such direct losses, as issuers may voluntarily accept them or merchants may go on to recover some of these direct losses from the consumer (either by having the consumer return the merchandise or initiating collection proceedings).[21] Information regarding the outcome of merchants' recovery and collections efforts is not available. In the case of error, there typically is no direct loss because the consumer reporting it has paid more for the goods and services then they should have.[22]

The second component is the cost of processing a fraudulent, erroneous, or disputed transaction. When a consumer discovers a fraudulent transaction or wants to initiate a dispute, she notifies her card's issuer. Depending on the circumstances, the issuer may either initiate a "receipt retrieval request" (to get more information about the charge) or reverse, i.e., "charge back," the transaction to the merchant that originated it. In the first instance, the merchant must send a copy of the signed transaction receipt to the issuer. In the second instance, the issuer refuses to pay for

[21] While a consumer who convinces his card's issuer to charge back a disputed transaction is no longer responsible for the charge to the issuer, he may still be responsible for the charge to the merchant. As such, the merchant may pursue the consumer under state sales law for the value of any goods or services from which the consumer benefited. See Official Staff Commentary to Regulation Z, 12 C.F.R. § 226.12(c)-2 (2005).

[22] Errors that merchants and issuers make in favor of consumers are not likely to result in consumer harm and, as a result, are not addressed by consumer protection policies.

the transaction and "charges it back" to the merchant. The merchant, in turn, may refuse to accept the chargeback (a decision usually supported by some kind of evidence). The issuer may once again attempt to charge the transaction back, and, if the merchant again refuses to accept the chargeback, the merchant and issuer submit their claim to arbitration.

Processing retrieval requests and chargebacks that are prompted by consumers' calls is resource intensive and represents a significant cost to the industry. Large issuers, for example, build computer systems and staff entire departments that specialize in handling consumers' calls regarding fraudulent and disputed transactions. The merchant processors on the receiving side of such requests similarly invest in personnel and system resources to handle issuers' inquiries. Beyond systems and staffing costs, issuers and merchants face fees when they use the associations' networks for chargebacks. Issuers who initiate a chargeback, for example, must pay a fee to the association that ranges from $10 to $25, and a similar fee is assessed to the merchant to whom the transaction is returned. If the chargeback is disputed and goes to arbitration, a fee of over $400 is typically assessed to the losing party. To retrieve a receipt, merchants often pay a fee to their merchant processor of up to $8.[23]

Because of a lack of data, it is difficult to estimate the total cost of protecting consumers from fraud, error, and dispute. As mentioned earlier, issuers and merchants incur approximately $3 billion in direct credit and debit card fraud losses each year. Credit card issuers spend approximately $1 billion to $2 billion to process disputed, erroneous, and fraudulent charges.[24] Estimates as to how much debit card issuers and merchants (or merchant processors) spend on processing problem transactions are not available. There are also no estimates for how much merchants lose to chargebacks resulting from error or dispute. Based only on the portion of expenses for which there are estimates (i.e., credit and debit card fraud losses and credit card dispute processing costs), the system spends at least $12 to $18 per active card per year to protect

[23] Mark Betz, "Chargebacks and Consumer Behavior," *Transaction World Magazine*, Oct. 2001, p.9.
[24] See Betz.

consumers.[25] As a percentage of volume that moves through the system, these known costs represent 25 to 30 basis points.

The $4 billion to $5 billion in total known expenses that result from the extension of fraud, error, and dispute protections are not paid for by any single party to credit or debit card transactions. Instead, the costs of these protections are ultimately passed along to consumers in the form of higher interest rates or fees on payment products or higher prices for retailers' goods and services.

One could argue that competition led to the creation of the bulk of these relatively expensive protections, since the extent to which consumers are protected by the bankcard associations often exceeds federal requirements. It is clear, however, that federal law significantly influenced the shape of the current protection system. Consider, for example, the most significant disparity between signature debit cards and PIN debit cards—the ability of a consumer to dispute a charge and request that his or her issuer charge it back to the merchant. The roots of this protection are likely in the bankcard associations' responses to federal law applicable to *credit cards*. Under the Truth in Lending Act, credit card issuers are required to provide a certain level of dispute protection to their customers. Because of this, the bankcard associations built networks that could handle disputes and any related chargebacks. Many years after the networks were built, signature debit cards became popular and the bankcard associations were able to extend dispute protection to debit cards without incurring the high fixed costs associated with modifying their networks. The traditional PIN-debit networks (i.e., those that trace their beginnings to bank ATMs) have not made the significant investments necessary to provide consumers with dispute protection, in part because federal law does not require it and because the high fixed costs of such a project likely outweigh its perceived benefits. Overall, it is clear that the federal government's

[25] Assumes that there are approximately 328 million active credit and debit cards. *The Nilson Report*, No. 828, Feb. 2005, p.7.

efforts to protect consumers affect consumers' expectations and the products beyond those the government sets out to regulate.

The fraud, error, and dispute protections extended to consumers of credit and debit cards generate expenses for the payment system that are high, relatively diffuse, and largely attributable to federal regulation. It is not clear, however, whether the beneficiaries of these protections, i.e., consumers, fully appreciate these expenses and how they increase the costs of goods and services. It is also not clear whether policymakers, who mandated protections on credit cards and not debit cards, appreciate how their policies have shaped the broad payment card market. Without such an appreciation, payment system participants cannot accurately evaluate the utility of various consumer protection policies.

C. Leading to Consumer Confusion

In the U.S., where new payment products are constantly competing for space in consumers' wallets, one can envision at least two ways of implementing federal consumer protections (assuming that such protection is needed). The first is by promulgating rules and regulations that address specific problems associated with a specific payment vehicle after observing how consumers use that vehicle. The second is by promulgating rules and regulations that are generic and applicable to all forms of electronic payments, including emerging payment forms that are being introduced to consumers for the first time. Both of these approaches have advantages and disadvantages that policymakers must consider.

The advantages of the wait-and-see approach are many: First, it allows payment innovators to introduce products that may not otherwise be viable if immediately subjected to costly regulation. In the period preceding regulation, innovators can test how consumers respond to different protection regimes and modify their product and its protections based on these responses. Second, this approach gives policymakers a chance to observe how a new product has been used and marketed before the writing of regulations. This permits policymakers to tailor protections to the actual problems that users of the new payment form are most likely to

experience. In addition, this approach lets policymakers observe the successes and failures associated with different protection regimes, improving the likelihood of policymakers choosing a scheme in line with consumers' needs.

The wait-and-see approach, however, is not without disadvantages. During the wait-and-see period, early adopters of a new payment form may be essentially unprotected, vulnerable to problems such as fraud, error, and dispute. Also during this period, issuers are uncertain as to how their product is going to be regulated. This uncertainty creates incentives for innovators to spend less money developing new payment forms and to spend more time trying to influence how regulators write consumer protection rules. Finally, the wait-and-see approach leads to inconsistent regulation. The rules that apply to each payment product differ based on how most consumers use the product and how the product is marketed—attributes that are probably not apparent to most consumers.

The key advantage of the one-rule-for-all approach is its simplicity for all parties involved in a transaction. Under this approach, issuers understand that any product introduced must carry a minimal level of protection; there is no uncertainty surrounding how the product will be regulated in the future. Consumers understand that, regardless of how a payment product is marketed, how long it has been around, or how other consumers primarily use it, it is protected in the same way as the other products they use. And merchants understand that, when they accept a new form of payment, the range of problems for which consumers will have recourse are generally predictable.

The simplicity of the one-rule-for-all approach comes at a cost. Under this approach, regulators must formulate a rule that sufficiently protects the users of multiple payment products that target different markets and have different uses. Neither consumer expectations nor voluntary industry efforts are considered. Under these constraints, regulators are likely to adopt a protection scheme that overprotects the users of some products and underprotects users of others. This approach also places regulators in the difficult position of crafting rules that apply to payment

forms that have not yet been conceived by the market. Finally, this approach likely discourages innovation, particularly with respect to low-cost products. The cost of federal protections may prevent entrepreneurs from introducing products that consumers demand (and for which consumers are willing to forgo protection), depriving consumers of low-cost payment options.

Which approach to consumer electronic payment regulation have U.S. policymakers favored? Consider the following regulatory developments: Credit cards were first subject to federal consumer protection regulation after 18 years on the market and after nearly 10 percent of U.S. households owned one.[26] Debit cards were explicitly covered by federal consumer protection regulations in 1984, nine years after their introduction[27] and at a time when regulators estimated that there were over 6 million debit cards in use.[28] Electronic benefits transfer (EBT) cards were covered by consumer protection regulations in 1994, two years after federal legislation encouraged states to deploy EBT and at a time when many states had already started operating EBT programs.[29] The regulations applied to EBT were similar to those that applied to debit cards with the exceptions of modifications made in response to the product's unique attributes.[30] At present, regulators are considering providing customized consumer protections for payroll cards.[31] This consideration comes at a time when nearly 2.2 million U.S. workers are paid via payroll card[32] and nine years after regulators considered such regulations for the first time.[33]

---

[26] David S. Evans and Richard Schmalensee, *Paying with Plastic* (MIT Press, 2nd ed., 2005), pp. 53-61.
[27] See Evans, p. 81.
[28] "The Board believes it is important that the coverage issue be resolved at this time because the number of debit cards being used in POS transactions is increasing…By the end of 1983, the number of debit cards was expected to exceed 6 million." 49 Fed. Reg. 2204 (1984).
[29] See 59 Fed. Reg. 10,678 (1994).
[30] See 59 Fed. Reg.
[31] In September 2004, the Board published for comment a proposal to amend Regulation E so that it covers payroll cards. See 69 Fed. Reg. 55,996 (2004).
[32] Ann All, (Apr. 7, 2004) "The Channel Shuffle," ATMmarketplace.com, available at www.atmmarketplace.com/futurearticles.htm?article_id=18820&pavilion=112&step=storywww.ATMmarketplace.com (accessed Sept. 29, 2005).
[33] In May 1996, the Board proposed a rule that would have exempted many stored-value products from Regulation E and subjected other products to limited regulatory requirements. See 61 Fed. Reg. 19,696 (1996).

It seems clear that U.S. policymakers favor the wait-and-see approach. They wait until a product is somewhat popular before regulating, and they regulate in a way that takes account of the payment form's unique characteristics. As compared to the one-rule-for-all approach, the current model likely produces regulations that are more responsive to consumers, less intrusive to industry, and more fostering of innovation. Unfortunately, however, it also causes greater confusion, particularly among consumers who use multiple payment products.

Responses to the wait-and-see policy have been mixed. The few legal scholars who have examined this issue advocate more uniformity among the payment laws that apply to credit cards, debit cards, and other electronic forms of payment.[34] In the context of general government regulation, economists argue that the wait-and-see approach is better because it permits market forces to influence the regulatory outcome. As seen in this series of papers, issuers have responded to the wait-and-see approach by attempting to impose uniformity through the use of voluntary protections. The additional layer of protection issuers provide, however, comes with its own list of exceptions, exclusions, and reporting rules that may add to consumer confusion.

The present system of federal consumer protection values customized and responsive regulation over consistency, predictability, and ease of understanding. While this may be a wise choice, there are likely ways of making the present federal system less opaque for consumers. Overall, policymakers would be wise to consider reforms to our federal consumer protection scheme that make it more transparent without causing it to lose its flexibility.

[34] See, e.g., Mark Budnitz, "Consumer Payment Products and Systems: The Need for Uniformity and the Risk of Political Defeat," *Annual Review of Banking & Financial Law* 24 (2005) pp. 247-293 (arguing for the enactment of "a uniform federal law to impose minimum standards for payment products and systems to ensure essential rights for consumers"); Ronald J. Mann, "Making Sense of Payments Policy in the Information Age," *Georgetown Law Journal* 93 (2005), p. 633 (arguing that "credit and debit cards should have similar limitations on finality").

III. Conclusion

Without a doubt, the protection systems described in the first two papers in this series are of tremendous benefit to all of those involved in the payment system. They encourage the adoption of electronic payment products, function as a type of insurance that spreads the risk of unforeseeable losses, induce consumers to make purchases from merchants whom consumers may not otherwise trust, and encourage payment system innovation. Overall, fraud, error, and dispute protections give consumers confidence in the electronic payment systems on which they often must rely.

These protections and the systems that support them, however, are not without costs. The present system used to allocate responsibility for fraudulent transactions results in (1) consumers and brick-and-mortar merchants not having sufficient incentives to exercise a reasonable level of care during card transactions and (2) Internet merchants inefficiently addressing the problem of Internet fraud on an ad hoc and individual basis. In addition, the direct cost of covering fraud, error, and dispute losses, combined with the cost associated with processing and adjudicating consumers' claims, has a material effect on the prices of the payment products and goods and services consumers use. Finally, the federal government's system for protecting consumers, because of the value it places on customization and flexibility, causes consumers of electronic payment products to be confused about how they are protected. Payment system stakeholders should have an interest in further exploring these issues, since their resolution could increase efficiency, lower costs, enhance competition, and open the consumer payment market to more desirable products.

Appendix A: Protection Summaries

Summary of Credit Card Protections Related to Fraud, Error, and Merchant Dispute

	Federal Law (Regulation Z)	State Law (Various State Statutes)	Association Rules*	General Industry Practice**
PROTECTIONS	**FRAUD:** Caps liability for fraudulent transactions at $50, regardless of consumer's negligence in handling card. Liability limits apply regardless of when the consumer ultimately reports the fraud. Limits liability to $0 for mail, phone, and Internet charges that are fraudulent.	Relevant state statutes mirror federal law as to fraudulent use.	Zero liability policies require issuers to shield consumers from any liability for fraudulent use. Policies, however, are subject to various association- and bank-imposed limitations.	Many issuers will honor the associations' zero liability policies for 90 days or more. A minority will assess the $50 permitted by Regulation Z after 60 or fewer days.
	ERROR: Requires card issuers to investigate and resolve a consumer's claim that a transaction is in error. Consumers must notify issuers of the suspected error within 60 days of receiving the statement on which the alleged error appears.	State statutes generally do not address this specific situation.	"Chargeback" policies permit issuers to assist consumers who discover erroneous transactions for up to 120 days after the date of the transaction.	Issuers will generally leverage the "chargeback" procedures of the associations and assist consumers who discover an error for as long as they are permitted (i.e., 120 days).
	DISPUTE: Permits consumer to assert that a charge for goods that were never delivered was an "error," triggering error resolution procedures described above.	In some states, a creditor in a consumer loan transaction is subject to all of the defenses of the borrower arising from the consumer sale for which the proceeds of the loan were used.	"Chargeback" policies permit issuers to return a transaction if a dispute arises up to 120 days after the date of transaction. While ultimately done at the issuer's discretion, dispute-related chargebacks may not be subject to the same distance or amount limitations as the Regulation Z "claims and defenses" protection.	Most issuers will leverage the associations' chargeback procedures to assist a consumer who is in a dispute with a merchant as long as the consumer provides sufficient proof of her claim. If the issuer cannot charge back the transaction, it may call merchant directly and attempt to settle dispute on behalf of the consumer.
	DISPUTE: Permits consumer to assert merchant-related claims against the card issuer as long as the consumer (i) has not yet paid for charge, (ii) made a good faith attempt to settle dispute, (iii) lives in same state as or within 100 miles of the merchant, and (iii) paid more than $50 for the item.			

*Please note: These protections are provided by card issuers/networks on a voluntary basis and do not have the force of law. Issuers or networks can generally change them unilaterally or decide not to abide by them.

**Information only intended to give the reader an idea of general industry practice. Consumers should consult their individual bank's policies for further information.

Summary of Debit Card Protections Related to Fraud, Error, and Merchant Dispute

	Federal Law (Regulation E)	State Law (Various State Statutes)	Association/Network Rules*	General Industry Practice**
PROTECTIONS	**FRAUD:** Limits liability to $50 if consumer reports loss/theft of card within 2 days of learning of it and $500 if consumer reports after 2 days but within 60 days of being sent statement reflecting fraudulent transaction. Consumer's own negligence is not a factor in assessing liability. Limits liability to $0 for mail, phone, and Internet charges that are fraudulent.	Beyond modest expansions of the time permitted to furnish notice of a lost or stolen card, or a lower maximum liability, states generally have not enhanced the consumer protection measures contained in Regulation E	Signature Debit and Interlink: Zero liability policies require issuers to shield consumers from any liability for fraudulent use. Policies, however, are subject to various association- and bank-imposed limitations. Regional EFT Network PIN Debit: Policies require no additional protection.	Practices vary. The most generous issuers provide $0 liability for 60 days for PIN and signature debit. Others provide $0 liability for as few as 2 days for signature debit only.
	ERROR: Permits consumers 60 days from statement date during which to notify bank about an erroneous transaction.	State statutes generally do not address this specific issue.	Signature Debit and Interlink: "Chargeback" policies permit issuers to return erroneous transactions for up to 120 days. Regional EFT Network PIN Debit: Network rules give issuers 120 to 180 days from settlement date (depending on the network) to return erroneous transactions.	Most issuers will return an erroneous transaction for as long as they are permitted under applicable network rules (120 to 180 days).
	FRAUD & ERROR: Requires banks to investigate claims in a timely manner and provisionally credit if investigation exceeds 10 days.	State statutes generally do not address this specific issue.	Signature Debit and Interlink: Requires banks to provisionally credit within 5 days. Regional EFT Network PIN Debit: Policies do not require faster provisional crediting.	Practices vary. Some issuers promise to provisionally credit immediately. Most credit within 5 days.
	DISPUTE: Does not address merchant disputes or claims.	State statutes generally do not address this specific issue.	Signature Debit and Interlink: "Chargeback" policies permit issuers to return a transaction if a dispute arises up to 120 days after the date of transaction. Chargeback is ultimately done at the issuer's discretion. Regional EFT Network PIN Debit: Policies do not provide dispute protection.	Most issuers will leverage the signature debit and Interlink chargeback policies to assist a consumer who is in a dispute with a merchant as long as the consumer provides sufficient proof of her claim.

***** Please note: These protections are provided by card issuers/networks on a voluntary basis and do not have the force of law. Issuers or networks can generally change them unilaterally or decide not to abide by them.

****** Information only intended to give the reader an idea of general industry practice. Consumers should consult their individual bank's policies for further information.

Summary of ACH E-Check Protections Related to Fraud, Error, and Merchant Dispute

	Federal Law (Regulation E)	State Law (Various State Statutes)	Association/Network Rules* (NACHA Rules)	General Industry Practice**
PROTECTIONS	**FRAUD**: Limits liability to $0 if consumer reports unauthorized use within 60 days of being sent statement containing record of fraudulent transaction.	State statutes generally do not address this specific issue.	Limits liability to $0 for unauthorized use as long as consumer reports within 15 days of being transmitted statement.	Limits liability to $0 for unauthorized use as long as consumer reports within 60 days of transaction settlement date.
	ERROR: Allows consumers 60 days from statement date during which to notify bank about erroneous or fraudulent transactions.	State statutes generally do not address this specific issue.	Allows consumers 15 days from statement date during which to notify bank about erroneous or fraudulent transactions and have those transactions resolved under ACH rules.	Allows consumers 60 days from transaction settlement date during which to notify bank about erroneous or fraudulent transactions and have those transactions resolved under ACH rules.
	ERROR & FRAUD: Requires banks to investigate claims of error and fraud and provide consumer with response within 45 days.	State statutes generally do not address this specific issue.	Does not require bank to investigate, but rather relies on customer's sworn statement.	Most banks do not investigate, but instead rely on customer's sworn statement.
	ERROR & FRAUD: Requires banks to provisionally credit consumer if investigation exceeds 10 days.	State statutes generally do not address this specific issue.	Requires bank to "promptly" credit as soon as it receives customer's sworn statement.	Banks will generally credit consumer's account upon receipt of sworn statement.
	DISPUTE: Does not provide any protection for transactions involving a post-purchase dispute with merchant.	State statutes generally do not address this specific issue.	Does not explicitly provide any protection for transactions involving a post-purchase dispute with merchant.	Effectively extends protection for erroneous and fraudulent transactions to those involving post-purchase disputes with merchant.
	DISPUTE: Does not provide any stop-payment rights.	State statutes generally do not address this specific issue.	Provides stop-payment rights.	Provides stop-payment rights, but limited because of clearing speed.

*Please note: These protections are provided by card issuers/networks on a voluntary basis and do not have the force of law. Issuers or networks can generally change them unilaterally or decide not to abide by them.

**Information intended only to give the reader an idea of general industry practice. Consumers should consult their individual bank's policies for further information.

Summary of Branded Prepaid Card Protections Related to Fraud, Error, and Merchant Dispute

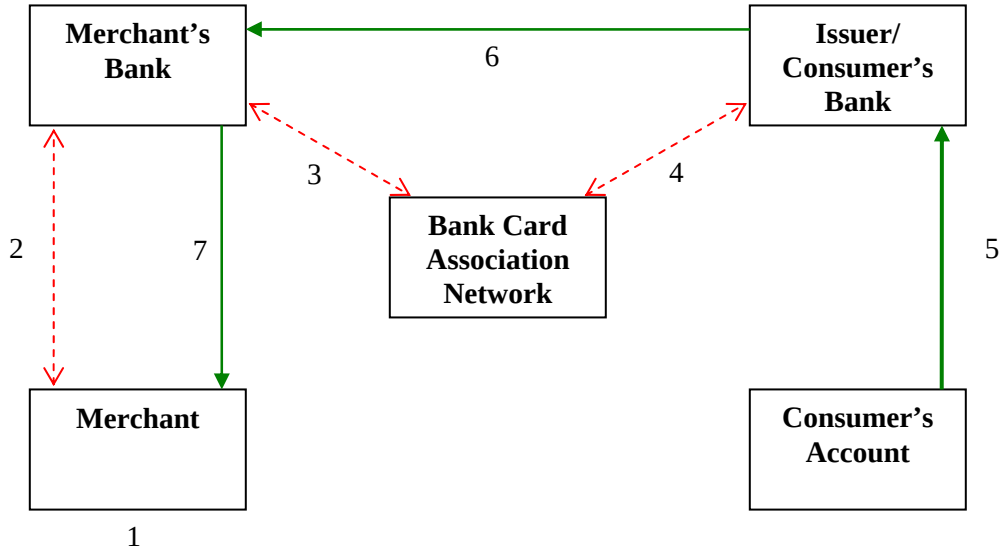
	Federal Law	State Law	Association/Network Rules*	General Industry Practice**
PROTECTIONS	**FRAUD**: Federal statutes generally do not address this specific issue.	State statutes generally do not address this specific issue.	Zero liability policies require issuers to shield consumers from any liability for fraudulent use. Policies, however, are subject to various association- and bank-imposed limitations (e.g., consumers must exercise "reasonable care" in handling card).	Varies by issuer. Some issuers explicitly limit period after loss or theft of card during which they will provide zero liability. These issuers will not provisionally credit for 10 days. Others provide zero liability for 60 days and provisionally credit promptly.
	ERROR: Federal statutes generally do not address this specific issue.	State statutes generally do not address this specific issue.	"Chargeback" policies permit issuers to assist consumers who discover erroneous transactions for up to 120 days after the date of the transaction.	Most issuers explicitly provide strong error-resolution protection for at least 60 days. Many will generally leverage the "chargeback" procedures of the associations and assist consumers who discover an error for as long as they are permitted (i.e., 120 days).
	DISPUTE: Federal statutes generally do not address this specific issue.	State statutes generally do not address this specific issue.	"Chargeback" policies permit issuers to return a transaction if a dispute arises up to 120 days after the date of transaction. Dispute-related chargebacks, however, are ultimately done at the issuer's discretion.	Varies by issuer. Some leverage the associations' chargeback procedures to assist a consumer who is in a dispute with a merchant as long as the consumer provides sufficient proof of her claim. Others require consumers to settle disputes themselves.

*Please note: These protections are provided by card issuers/networks on a voluntary basis and do not have the force of law. Issuers or networks can generally change them unilaterally or decide not to abide by them.

** Information intended only to give the reader an idea of general industry practice. Consumers should consult their individual bank's policies for further information.

Appendix B: Simplified Illustration of the Typical Credit and Signature Debit Card Transaction*

This is a highly simplified illustration of a typical credit and signature debit card transaction. The dotted arrows represent the authorization process (steps 2 through 4), by which the merchant obtains clearance to charge the consumer's account. The solid arrows represent the clearing and settlement process (steps 5 through 7), by which the merchant receives payment from the consumer's card issuer.



Cardholder presents card to merchant for payment.

*For more detailed information about credit card transaction processing, see David Evans and Richard Schmalensee, *Paying With Plastic* (MIT Press, 2nd ed., 2005), pp. 9-12.

Appendix C: Estimates of Payment Vehicle Fraud Losses

	Party			
Product	Consumer	Brick-and-Mortar Merchant	Internet/Catalogue Merchant	Issuer
Credit Card	**NEGLIGIBLE** In most cases, consumer liability for fraud limited to $50 under Regulation Z and to $0 under association rules.	**NEGLIGIBLE** Brick-and-mortar merchants have limited liability for "card-present" transactions under association rules.	**APPROX. $1 BILLION/ 180 BASIS POINTS OF VOLUME**[(1)] Under association rules, because an Internet-based credit card payment cannot be authenticated using the card itself, Internet merchants are liable for transactions that turn out to be fraudulent.	**APPROX. $0.8 BILLION/ 5 BPS OF VOLUME**[(2)] Credit card issuers are generally liable for card-present fraud under association rules.
Signature Debit Card	**NEGLIGIBLE** In most cases, consumer liability for fraud limited to $50 under Regulation E and to $0 under association rules.	**NEGLIGIBLE** Brick-and-mortar merchants have limited liability for "card-present" transactions under association rules.	**APPROX. $1 BILLION/ 180 BPS OF VOLUME**[(1)] Under association rules, because an Internet-based signature debit card payment cannot be authenticated using the card itself, Internet merchants are liable for transactions that turn out to be fraudulent.	**APPROX. $0.2 BILLION/ 5 BPS OF VOLUME** [(3)] Signature debit card issuers are generally liable for card-present fraud under association rules.
PIN Debit Card	**NEGLIGIBLE** In most cases, consumer liability for fraud limited to $50 under Regulation E and $0 under internal bank policies.	**NEGLIGIBLE** Brick-and-mortar merchants have virtually zero liability for PIN debit transactions approved by the network.	**NEGLIGIBLE** In general, Internet-based merchants cannot accept PIN-debit cards.	**APPROX. $0.1 BILLION / <1 BPS OF VOLUME** [(4)] Under Regulation E, PIN debit card issuers are liable for most PIN-debit fraud.

(1) Estimate based on 2005 CyberSource Online Fraud Report. Losses include both chargebacks to merchants because of fraud and credits issued by merchants to consumers without return of goods because of fraud. Assumes that half of the fraud on the Internet is perpetrated using credit cards and the other half is perpetrated using signature debit cards (see "Debit Volume Exceeds Credit, Visa Says," *Bank Systems & Technology*, Aug. 2005, p. 14). Also assumes that total Internet sales volume in 2004 was $117 billion (see comScore press release of Jan. 10, 2005).

(2) Estimate based on data from *The Nilson Report* (No. 830, Mar. 2005) on general purpose credit card losses for 2004.

(3) Estimate based on 2004 Deposit Account Fraud Survey by American Bankers Association and 2004 association signature debit volumes from *Nilson Report* (No. 830, May 2005)

(4) Estimate based on 2004 Deposit Account Fraud Survey by American Bankers Association.