The Impact of Fraud on New Methods of Retail Payment

WILLIAM ROBERDS
The author is a research officer in the macropolicy section of the Atlanta Fed's research department.

IN MARKET ECONOMIES, PAYMENTS SYSTEMS PROVIDE CERTAINTY OF VALUATION IN EXCHANGE. PEOPLE SELLING GOODS OR SERVICES EXPECT MONEY IN RETURN, WHERE *MONEY* MEANS EITHER CURRENCY OR A FINANCIAL CLAIM THAT IS WORTH A FIXED AMOUNT OF CURRENCY. TO PROVIDE THIS CERTAINTY, A SUCCESSFUL PAYMENTS MEDIUM HAS TO OVERCOME VARIOUS RISKS THAT ARE A NATURAL PART OF THE PAYMENTS PROCESS.

An important risk associated with payments systems is the risk of fraud. Fraud can occur because purchases of goods typically involve at least three parties. The first party, a buyer (sometimes referred to as a consumer), wants to purchase some good or service from the second party, a seller (or merchant). In modern economies, such purchases are rarely accomplished by barter, or direct trade of goods between buyers and sellers. Instead, the buyer offers to transfer to the seller a claim on a third party, an issuer.

Such transactions are preferable to barter because it is easier for sellers to value such claims than to value goods offered in barter. If, however, the issuer cannot be physically present to verify the claim when it is transferred from buyer to seller, then there is always some chance that the buyer may offer a fraudulent claim.[1]

Payments fraud takes on many forms, but most cases of fraud consist of one of two types of misrepresentation. The first is an offer to exchange a claim where none exists. For example, a buyer may write a check on insufficient funds. The second type of misrepresentation occurs when a buyer offers to transfer a claim that rightfully belongs to someone else. Examples of this type of fraud include check forgery or use of a stolen credit card.

As these examples indicate, traditional payments media such as currency, checks, and credit cards are not exempt from the risk of fraud. Currency fraud (counterfeiting), check fraud, and credit card fraud are serious problems, costing the U.S. economy billions of dollars each year. But with each of these payments methods, the problem of fraud has been kept at a manageable level so that their overall integrity has been maintained.

This article explores the potential impact of fraud on new forms of retail payment such as electronic cash and stored-value cards. These new payments media can increase economic efficiency by incorporating advances in computer technology into payments systems. Payments systems based on these new media communicate much of the same information as traditional payments systems but at a potentially lower cost. Electronic payments systems have this advantage because it is cheaper to move electrons than it is to move paper. This natural advantage of electronic systems can be a disadvantage, however, when it comes to the risk of fraud. Since computer data are readily stored, copied, and manipulated, complex security procedures are needed to guarantee the integrity of electronic payments data.

Will the risk of fraud hinder the development of the new payments media? This article investigates this issue by first considering which features of payments media are conducive to fraud. The discussion then turns to which of these features are also part of traditional payments systems. Finally, the article considers some new payments media, how certain features of these media differ from more traditional forms of payments, and whether these features are likely to detract from the acceptance of the new media in the marketplace.

The Optimal Incidence of Fraud

Any discussion of payments fraud should begin from the basic economic principle of balancing costs and benefits. That is, the benefits of measures designed to reduce fraud should exceed the costs of such measures.

It is technologically possible to virtually eliminate fraud in electronic payments, as has been demonstrated by the experience of large-value, or wholesale, funds transfer systems. Such systems, which are used by banks and securities markets participants, are practically devoid of fraud. However, large-value systems typically make use of elaborate and costly security measures (for example, using dedicated telephone lines for all transactions) that would be excessively costly, time-consuming, or otherwise inappropriate for retail payments systems.

Thus, the key question for retail payments systems is not whether fraud will occur but instead how much fraud can be tolerated if the payments system is to remain effective. While this amount will most certainly be positive, both economic intuition and practical experience suggest that the optimal amount of fraud is relatively small. Intuitively, fraud is particularly injurious to the provision of payments services because it detracts from the essential quality of the service that is being provided, which is certainty of valuation in exchange. This intuition is backed by the experience with traditional payments media, for which fraud rates are far from negligible but, nonetheless, relatively low.

Incentives for Fraud

The problem of fraud is common to all payments systems and dates back to ancient times. Nonetheless, there are some types of transactions and some features of payments systems that are more likely than others to create incentives for fraud. Some of the key factors influencing the risk of fraud are the following.

Face Value of the Claim. For fraud to be profitable, the reward from committing fraud has to be large enough to offset the threat of punishments imposed by the legal system. There is little incentive to create fraudulent small-denomination claims such as coins. On the other hand, transactions of sufficiently large value are more likely to inspire the use of costly security measures, as noted above.

Verifiability. If the existence and ownership of a claim can be instantly verified, say, through an on-line verification system, this ability obviously reduces the risk of fraud. Effective verification systems are costly to set up and operate, however.

Payments systems based on these new media communicate much of the same information as traditional payments systems but at a potentially lower cost.

Anonymity of the Transaction. If a buyer and seller do not have an ongoing business relationship, the incentive for fraud increases. The incentive for fraud is also enhanced if the ownership of the claim offered in payment cannot be traced.

Point-of-Sale Transactions. If the seller can withhold delivery of the good until the claim can be verified, then the incentive for fraud is reduced. If the good is exchanged at the point of sale, there is always some chance that the claim presented by the buyer is fraudulent.

Allocation of Losses. Perhaps the most critical factor contributing to the incidence of fraud is the allocation of losses.

Suppose that a fraudulent transaction has occurred. Who should bear the costs of the fraud? Note that to the extent that prices must be raised in order to cover losses from fraud, all market participants may end up bearing some of the cost. However, having different rules concerning the allocation of loss from a particular incident of fraud changes the distribution of losses among individual buyers, sellers, and issuers and hence affects the incentives to commit fraud.

One possibility is that these costs are borne directly by an individual buyer. This arrangement gives maximum reassurance to the seller and to the issuer. In some cases, however, the buyer and the legitimate owner of the transferred claim may be two different people. For example, in

1. *A second possibility is that the seller could offer worthless merchandise, which is a potentially serious problem with some forms of electronic commerce. Yet another possibility is that issuers could issue claims on worthless assets. New forms of financial intermediation are not immune to this type of risk, as evidenced by the recent collapse of the European Union Bank, an "Internet bank" based in Antigua (see Rohter 1997). Nonetheless, this article will focus on the first risk as the most likely to affect acceptance of new payments media.*

the case of a check forgery, the forger does not have ownership of the claim (deposit) apparently represented by the forged check. And in point-of-sale transactions, the buyer may be long gone by the time that a fraud is discovered. For these reasons it can be problematic to assign the costs of fraud to buyers.

A second possibility is for the seller to bear the costs of fraud. This arrangement protects the interests of the buyer and the issuer, but it is unlikely to be popular with sellers.

The third possibility is that the issuer of the claim bears the costs. This is clearly the most convenient arrangement for the buyer and seller, but it is also the most likely to promote fraud. Since the issuer is not present at the transaction, the legitimacy of a claim on the issuer can never be verified with absolute certainty.

In spite of this disadvantage, there are many circumstances in which it makes sense for the issuer to bear the risk associated with fraud. If the wealth of the issuer is large, compared with that of the buyer (say, a typical consumer) and the seller (say, a small business), then the issuer may be the party most prepared to face such risks. A large issuer may also be able to lessen exposure to fraud risk by diversifying this risk over many transactions.

The above discussion suggests that the problem of fraud will be greatest in cases involving large informational asymmetries between buyer and seller. Fraud is more likely to occur when transactions involve large amounts, when verification is costly, in anonymous transactions, and in point-of-sale transactions. Fraud will also be more likely in transactions in which at least some of the costs of fraud can be shifted to the third party, the issuer of the claim used for purchase.

Fraud and Traditional Payments Systems

Currency. The simplest traditional payments system is currency. In modern-day currency transactions, the role of issuer is played by a central bank or sovereign government.[2] The claim in this case is a fixed-denomination note or coin that is considered a liability of the issuer. Payment is effected by physical transfer of the note or coin. Among traditional payments systems, currency is unique in that a payment in currency does not need to be cleared and settled through the banking system in order to constitute a valid payment. Another distinguishing feature of currency is that it can circulate indefinitely before it is returned to its issuer.

Fraud can occur in currency transactions if the currency is counterfeit or stolen. The fact that currency is a convenient, widely accepted, and anonymous medium for point-of-sale transactions in turn creates incentives for counterfeiting and theft.

Several factors serve to limit the risk from counterfeiting currency, however, at least within the United States. The first is vigorous law enforcement; according to the U.S. General Accounting Office (GAO) (1996), the majority of counterfeit currency is seized before it can be distributed. The second factor is that since all detected counterfeit currency is subject to seizure by law enforcement authorities, a significant portion of the costs of counterfeit fraud is borne by buyers and sellers. The third factor is that currency is not widely used within the United States for transactions with a high dollar value because other, more suitable payments systems are widely available. Anyone attempting to pass a large amount of counterfeit currency would be forced to use it in a large number of small-value transactions.

The problem of theft also tends to be self-limiting. Since currency is anonymous, a buyer holding a large amount of cash is liable for its theft or loss. Consequently, most people do not hold large amounts of currency.

Statistics on the incidence of counterfeiting are difficult to obtain since counterfeit currency can circulate for some time without being detected. Available statistics suggest that counterfeiting is not an economically significant problem in the United States. In 1994 the total amount of counterfeit currency detected by law enforcement was less than one-tenth of 1 percent of currency outstanding, most of which never reached circulation (GAO 1996, 11).

Checks. Payment by check is by far the most prevalent system for noncurrency retail payments in the United States. In a check transaction, a buyer instructs a bank or similar financial institution to transfer the buyer's deposit claim on a bank. The buyer does so by transferring an order to pay, or check, to the seller. The seller or seller's bank then presents the check to the buyer's bank for payment.[3] In such a transaction, the bank plays the role of issuer, although the check is considered a liability of the buyer and not of the bank on which it is drawn.[4]

Checks are a natural target for fraud as they can be written for large amounts, are relatively easy to alter or forge, and can be difficult or costly to verify at the point of sale. Check fraud has recently become a more serious problem because of several factors. The first is the widespread availability of computer technology, which has made it easier to counterfeit checks (see, for example, Hansell 1994 or Nielsen 1994). The second factor has been the funds availability schedules required by the Expedited Funds Availability Act of 1987 (see Board of Governors 1996b). The act requires that banks make check funds available according to certain, preset schedules. Consequently, banks must sometimes make funds available before they can ascertain whether a deposited check is fraudulent.

Despite these problems, there are certain factors that have served to limit the incidence of check fraud. The first and most important is the allocation of losses. While the law governing the allocation of losses from

check fraud is complex, the end result is that the liability for fraud often resides with the seller and not the bank on which the check is drawn.[5] For example, a merchant who accepts a check in a point-of-sale transaction bears the loss if the check is returned for insufficient funds.[6] Likewise, if a check is stolen, a buyer can stop payment on the check, again leading to potential losses for the seller. As a result of this loss allocation, there is widespread recognition of the potential for fraud in check transactions and sellers are reluctant to accept checks in situations that are conducive to fraud, such as anonymous, point-of-sale transactions.

A second factor limiting the incidence of check fraud has been the increased use of techniques such as positive pay. Under a positive pay arrangement, a buyer (typically a corporation) sends a list of issued checks to the buyer's bank. Only checks on the list are automatically paid by the bank. Any check not on the list requires explicit approval by the buyer before it can be paid. Positive pay has been an effective weapon against losses resulting from check counterfeiting, forgery, and embezzlement, among others. A third factor has been the Federal Reserve's requirement for "large-dollar return notifications." That is, banks must provide prompt notice of nonpayment on checks for $2,500 or more. Prompt notice of nonpayment reduces the likelihood that banks will provide provisional credit for fraudulent checks before the fraud can be discovered.

As is the case with currency, available statistics suggest that check fraud is not a large enough problem to significantly detract from the use of checks as a payments medium. Estimates of the total cost of check fraud in the United States range as high as $10 billion annually (Hansell 1994). An extensive 1995 survey by the Federal Reserve found that banks' share of these losses amounted to $615 million in 1995.[7] While these figures show that check fraud is a serious problem, these numbers are small compared with the total volume of check payments in the United States, which was roughly $73.5 trillion for 1995 (Bank for International Settlements 1996b). The overall rate of check fraud loss is less than 2 basis points, or two-hundredths of 1 percent.[8]

Credit Cards. Credit cards are widely used in retail payment situations, especially when informational asymmetries make payment by check impractical. In a credit card transaction, the buyer pays for a purchase by drawing on a line of credit from the credit card issuer. The issuer pays the seller for the purchase, and the balance on the credit card is then paid down by the buyer. Since the claim presented in payment is considered a liability of the credit card issuer, this type of transaction transfers much of the risk of insufficient funds in the original transaction from the seller to the credit card issuer.

In cases of credit card theft or similar types of fraud, cardholders' liability is restricted by the Truth in Lending Act of 1968 and corresponding Federal Reserve Regulation Z. Generally a cardholder's liability is limited to $50 as long as the cardholder reports a lost or stolen card, and in practice the liability is often less than this maximum. The remaining liability is shared between the seller, or merchant, and the credit-card issuer. While the rules governing the apportionment of this liability vary, the GAO (1997, 114) reports that, on average, the vast majority (70 percent) of the liability is borne by the credit card issuers. To limit incentives for fraud, the issuer's liability is contingent on the merchant taking certain steps intended to curtail fraud (for example, validating a credit card transaction through an on-line verification system).

The key question for retail payments systems is not whether fraud will occur but instead how much fraud can be tolerated if the payments system is to remain effective.

The incidence of fraud in credit card purchases is quite small in absolute terms but is relatively high as compared with checks. While precise figures are unavailable for the credit card industry as a whole, one estimate put total (gross) fraud losses at $2 billion to $3 billion in 1993 (Pearsall 1994), and another placed this figure at $1.3 billion for 1995 (Fryer 1996). Given aggregate credit card use of $879 billion for 1995, the estimates imply a fraud rate of between 10 and 20 basis points (0.1 to 0.2 percent). In the case of bank cards (MasterCard and Visa), a study by the American Bankers Association (1996) estimated total gross fraud loss for 1995 at $790 million versus purchases of $451 billion, implying a loss rate of 18 basis points (0.18 percent).

2. Historically such notes were also issued by commercial banks. These notes are discussed on page 48.
3. For an introduction to details of check clearing and settlement, see GAO (1997).
4. Exceptions are traveler's checks, cashier's checks, and certified checks.
5. Generally the loss allocation is determined by Articles 3 and 4 of the Uniform Commercial Code.
6. Of course, in such cases the merchant is entitled to try to recover the amount of the check through legal action.
7. See Board of Governors (1996b, 5). A smaller survey by the American Bankers Association (1994) put this number at $815 million for 1993. Both numbers represent "gross losses," that is, they do not incorporate any recoveries of lost funds.
8. This is an average rate for all checks, many of which are at low risk for fraud. The risk of fraud is substantially higher for certain types of checks.

Note that the relatively high rate of fraud on credit cards does not reflect any inherent shortcoming of credit cards as a payments medium. Rather, the fraud rate on credit cards reflects the fact that credit cards tend to be used in situations where incentives for fraud are greater, particularly in point-of-sale transactions. The acceptance of credit cards in such situations, together with the fact that the card issuers bear the majority of costs associated with fraud, help make credit cards a secure and convenient payments medium from the standpoint of marketplace participants.

To limit the potential for fraud, credit card issuers have invested heavily in on-line verification technology and other technologies to detect fraudulent use (see Fryer 1996 or Rutledge 1996). While this technology has been effective, it is also costly: Caskey and Sellon (1994) report that credit cards are the most expensive medium for retail transactions.[9]

Debit Cards. Conceptually, a debit card transaction closely resembles a check transaction. In a debit card transaction, a buyer transfers deposit claims from the buyer's bank account to that of the seller, just as in a check transaction. As with checks, this transfer is done as a *debit* transaction, in which funds are "pulled" by the seller (via the card network) from a buyer's bank account.

However, there are several key differences between a debit card transaction and a check transaction. The most important is that in contrast to most check transactions, the transaction itself is subject to an electronic verification process, which varies according to the type of card.[10] This verification process lessens the credit risk associated with the transaction. A second key difference is that a debit transaction is cleared and settled electronically through the card issuer's network rather than through a traditional paper-based check-clearing process. That is, in contrast to checks, the clearing and settlement of transactions does not have to wait for physical delivery or *presentment* of checks but can begin more or less immediately.

Debit card transactions also differ from credit card transactions in that the amount of a purchase is automatically debited from the buyer's bank account within a few days of the time of purchase. By contrast, credit card holders have to either pay for purchases after a grace period or pay interest on the unpaid balance.

In cases of debit card fraud, cardholders' liability is limited by the Electronic Funds Transfer Act of 1978 and the corresponding Federal Reserve Regulation E. Losses are capped at $50 if loss or theft of a debit card is reported within two days and at $500 if the loss is reported within sixty days. Recently the two main debit card issuers, MasterCard and Visa, have announced policies that place more stringent limits on cardholders' liability (see Fickenscher 1997 and Keenan 1997). Under these new policies, cardholders' liability is generally limited to $50. Available estimates suggest that the overall rate of fraud for debit card purchases is quite low, comparable to that for credit card purchases (Lunt 1996 and Keenan 1997).

Why Things Might Be Different with New Payment Technologies

Recently a number of new retail payment technologies have become available (some of which are still undergoing trial). Among the most widely discussed technologies are stored-value cards and a group of technologies that fall under the term *on-line payments.*[11]

A stored-value card is a payment card similar in appearance to a credit or debit card. To use a stored-value card, a buyer must first purchase a card from an issuer. The issuer then stores the value of this purchase on the card itself, in the form of data contained on a magnetic stripe or an electronic chip. A buyer can then purchase goods by presenting the card to a seller, who electronically transfers the value on the card to the seller's card or account. The value on the card must eventually be redeemed by the issuer.

On-line payments technology includes a number of important payments media, including on-line banking, on-line credit card payments, and electronic cash. On-line banking allows consumers direct computer access to banking services, either through "closed" networks such as traditional Automated Teller Machine networks or, more recently, through "open" networks such as the Internet. Using on-line banking, a buyer can initiate payment in much the same way as by writing a check. Clearing and settlement of on-line payment instructions often takes place via the automated clearinghouse system (the electronic interbank payments system for small-value transactions). In on-line credit card payments, a buyer initiates a credit card transaction by sending the buyer's credit card information to a seller over a computer network (almost always the Internet). Finally, payments can be made over the Internet by transfer of electronic cash, a difficult-to-counterfeit series of electronic messages that represent a financial claim on its issuer.[12]

In many ways, these new forms of payment closely resemble traditional forms. For example, stored-value cards have many features in common with travelers' checks, and credit card payments over the Internet are obviously not so different from credit card payments made at the point of sale or over the telephone. There are some features of the new payments media, however, that are not incorporated into traditional modes of payment. Some of these may affect the incidence of fraud and are discussed below.

One noteworthy feature of many of the new payments media (on-line credit card payments, some forms of on-line banking, and electronic cash) is that they allow for payments over the Internet, which is an open system

of computer networks with few restrictions to access.[13] The key advantage of the Internet over closed systems is that it allows buyers and sellers low-cost access to a greater range of transactions. While its open architecture makes the Internet an appealing vehicle for electronic commerce, this same openness offers opportunities for counterfeiting and fraud. The fact that a buyer or seller is on the Internet proves nothing in and of itself; additional verification of the transaction is required. For example, buyers making credit card purchases over the Internet need to convey enough information to show that credit cards offered in payment are not counterfeit or stolen. At the same time, sellers need to demonstrate that they are selling a legitimate product and not just collecting credit card numbers for fraudulent use. And both buyers and sellers need to safeguard against surreptitious monitoring of transactions by third parties. The need to verify on-line transactions has led to the development of technologies such as the Secure Electronic Transactions (SET) protocol (see, for example, Bloom 1997 or "Survey of Electronic Commerce" 1997). These technologies are designed to allow buyers and sellers to identify one another over the Internet and also to prevent unwanted eavesdropping on private transactions.

A similar difficulty exists with stored-value cards. These cards are designed to be used for small-dollar-value transactions, particularly transactions in which traditional methods of verification are too costly or otherwise impractical. Instead, verification is provided by data contained on the card itself (perhaps in combination with on-line information). In this sense, stored-value payments systems may be seen as an electronic analog of currency, where validity of the payments medium is provided by visual inspection. As is the case with currency, this feature of stored-value cards increases the incentives for counterfeiting and fraud. Stored-value systems rely on electronic encryption technologies to protect against counterfeiting and other fraudulent use.[14]

Incentives for fraud are magnified in the case of those stored-value cards that allow for "peer-to-peer" transactions, that is, transactions among cardholders who do not have access to on-line verification or clearing technologies. In this type of system, value can be successively transferred from one stored-value card to another without outside verification. This feature can increase the time interval between counterfeiting or possible fraudulent use of the card and the subsequent detection of fraud when the stored value is ultimately presented for redemption.

The issue of who bears the responsibility for fraud is unresolved for many of the new payments media. For many of these media, however, there are strong justifications for the issuer bearing the responsibility for losses due to fraud. The presence of "network effects" in payments technologies means that new forms of payment are unlikely to be issued by a single financial institution but instead by consortiums of financial institutions, data processing firms, and so on, operating under a single "brand name."[15] A network effect occurs when the entrance of one participant into a payments network increases the benefits or lowers the costs of participating in the network for all other network members. For example, if only one merchant in a small town accepts a particular brand of stored-value card, then consumers might not find it advantageous to use this card, making it difficult for the card issuer to recover costs. If, on the other hand, all the merchants in the same town were to accept this card, then consumers would be more likely to use the card regularly, which would in turn increase its profitability. Since the usefulness and profitability of a branded payments network depends heavily on its widespread acceptance, "branded" networks have a natural incentive to absorb the risk associated with fraud losses.

The general feeling expressed by policymakers is that the long-run benefits to the development of new payments technologies will outweigh any short-term difficulties associated with their introduction.

9. Fraud represents a significant, though relatively minor, component of this cost differential. A more significant component is the cost of delinquencies (failure to pay accounts due). Delinquencies in 1995 amounted to 3.55 percent of outstanding credit card balances, according to the American Bankers Association (1996).

10. Debit cards may be either "on-line" or "off-line." With on-line cards, a transaction is verified by comparing the purchase amount against a buyer's bank balance. With off-line cards, the transaction is verified by comparing the buyer's total purchases over a certain period against a preset limit.

11. These technologies are extensively discussed in Congressional Budget Office (1996), U.S. Department of the Treasury (1996), and GAO (1997).

12. Electronic cash is also known as e-cash, digital cash, electronic scrip, and electronic coins.

13. See McAndrews (1997a) for an introduction to the Internet and its potential uses in electronic commerce.

14. Encryption refers to the use of mathematical algorithms to convert data into a coded form. See Bank for International Settlements (1996a) on the use of encryption in payments systems.

15. A detailed discussion of this scenario is laid out in McAndrews (1997b). More generally, see Weinberg (1997) on network effects in payments systems.

Counteracting this incentive are potential difficulties resulting from anonymity of some of the new payments media, particularly for some stored-value cards. For example, if a stored-value card is issued anonymously there is no way to identify the rightful owner of the card. It would thus be difficult if not impossible for the issuer of the card to stop payment on a lost or stolen card, given the current design of stored-value systems.[16] In such situations, users of stored value cards would have an incentive to handle these cards with the same care as if they were currency.

What Could Go Wrong?

A recent episode in Japan provides some sobering lessons concerning the potential for fraud over new payments systems (see Glain and Shirouzu 1996 and Pollack 1996). This case concerns a stored-value card designed by Sumitomo Corporation and Mitsubishi Corporation, with the cooperation of Nippon Telephone and Telegraph as well as various government agencies. The cards were intended for use with pachinko, a type of pinball game. One purpose of the cards was to limit criminal activities often associated with the pachinko parlors, such as gambling, tax evasion, and money laundering.

The value on the cards was held in the form of data stored on magnetic strips.[17] Criminal organizations were able to defeat the encryption by *cloning,* that is, by transferring the data stored on existing cards to used cards. The cloned stored-value cards were then taken to pachinko parlors and redeemed for cash. Since the stored-value issuers had no way to distinguish fraudulent transactions from legitimate transactions, they were forced to absorb the resulting losses. Published reports estimate the losses from this episode were at least $600 million.

The pachinko fraud is instructive in that it illustrates the power of incentives. Although the pachinko stored-value cards were heavily encrypted, various features of their design created strong incentives for fraud. Apart from the obvious defect of being too easy to copy, the cards were almost perfectly anonymous, were designed for point-of-sale transactions, and were available in large denominations (of about $50 and $100). Pollack (1996) reports that reductions in fraud were achieved only after the card issuers both improved the cards' encryption technology and reduced the incentives for fraud by eliminating large-denomination cards and cracking down on pachinko parlor operators who had apparently tolerated extensive use of cloned cards.[18]

Historical Lessons

Various analyses of new payments media (particularly stored-value cards and electronic cash) have invoked comparisons of the new media with the banknotes that circulated during the U.S. Free Banking Era (1837–65).[19] During this period, banks issued claims in the form of bearer notes, which circulated much as government-issued currency does today. Banknotes usually traded at par value locally but were often traded at a discount in transactions that occurred at any distance from the issuing bank.[20] A major cause for this discounting was the fraud risk associated with counterfeit and altered notes.[21] Given that certain of the new electronic payments media share a number of features with privately issued banknotes, would we expect a similar pattern of discounting to arise? The most likely answer to this question is no, for at least two reasons.

First, Free Banking Era banknotes were particularly attractive targets for fraud. Often the notes were available only in large denominations ($5 and up, the equivalent of roughly $80 today), they were widely used for anonymous, point-of-sale transactions, and nonlocal notes could only be verified at considerable cost and after a lengthy delay.[22] This unfortunate combination of features is not shared by any of the new payments media.

Second, Gorton (1996) shows that despite the prevalence of fraud, the most serious risk to holders of Free Banking Era banknotes, and hence the greatest source of discounting, was not fraud risk but credit risk associated with the issuer. In this case, credit risk refers to the risk that a note would not be honored at full value because of either the insolvency or illiquidity of the issuing institution. During the Free Banking Era, banknotes' credit risk was exacerbated by a combination of poor communications and restrictive banking laws. These laws effectively prohibited banks from branching beyond their home state or local area, thereby making it difficult for banks to build effective coalitions in order to guarantee the value of their notes. In New England, where banks were able to form such a regional coalition, discounting of notes on banks within the coalition was practically nonexistent.[23] The experience of the New England banks suggests that if the credit risk associated with a payments instrument can be held in check, then fraud risk is unlikely to lead to discounting of that instrument.

As discussed above, the "network" economics of the new payments media are likely to limit credit risk associated with new forms of payment. Holders of stored-value cards, for example, would prefer to use stored-value cards that are readily acceptable in as many places as possible. Providers of stored-value cards and similar payments systems therefore have incentives to form broad coalitions with a widely recognizable brand name. The members of such coalitions have strong incentives to monitor each others' credit risk in order to maintain credibility of the brand.

Credit risk could also be eliminated by Federal Deposit Insurance Corporation (FDIC) insurance of a payment instrument. As of this writing, however, it appears that FDIC insurance will not be provided for most types of stored-value cards. The FDIC has also requested

comment on the eligibility of certain other forms of electronic payment for deposit insurance; see FDIC (1996).

The Free Banking Era experience suggests that a necessary downside of containing credit risk may be increased fraud risk, however. According to Gorton (1996, 370) the banknotes of established, creditworthy banks were the most likely targets of counterfeiters. Notes of less creditworthy banks were more likely to be discounted and less likely to circulate, and hence they were not worth the trouble.

Public Policy Concerns

An important challenge for policy in the area of new payments technologies has been to promote increases in efficiency associated with technological improvements while safeguarding consumers from undue risks. To date, public policy toward new forms of retail payment has been largely hands-off. The general feeling expressed by policymakers is that the long-run benefits to the development of new payments technologies will outweigh any short-term difficulties associated with their introduction. The view has also been expressed that premature regulation of new payments media may hinder the development of potentially more efficient payments systems.[24]

In the case of stored-value cards, the Federal Reserve has attempted to avoid excessive regulatory burdens on new payments technology by proposing that Regulation E not apply to certain types of stored-value cards (see Board of Governors 1996a, 1997a). Currently, Regulation E requires that consumers be provided written records for electronic funds transfers and limits consumer liability to $50 (see discussion above) when they use an "access device" to withdraw or transfer funds from a "consumer asset account." While withdrawals from such an account in order to load the stored-value card would be covered by Regulation E, the proposed regulations would not be extended fully to all transactions between buyers and sellers involving stored-value cards. For example, the Federal Reserve proposal would exempt from these provisions all cards containing $100 or less, as well as all cards that are off-line and do not track individual transactions.

Another important public policy issue in this area has to do with potential trade-offs between security and privacy. As discussed above, one of the factors affecting the risk of payment is the anonymity of the transaction. If a seller has access to enough information about a potential buyer (for example, the buyer's current bank balance), then the risk of fraud can be minimized. On the other hand, a seller's need for information about the creditworthiness of potential customers can conflict with the customers' need for privacy.

Payments systems that make use of extensive consumer-identifying information can lessen the incidence of fraud . . . but the value of such information in reducing fraud must be balanced against the value of privacy.

This conflict of interest has become more acute in recent years. Improvements in computing and communications technology have enabled the construction of extensive computer databases of information on consumers.[25] Widespread use of electronic payments media could result in the creation of even more extensive databases, providing detailed information on the purchasing habits of users of new payments media. While there would be many legitimate uses of such information, including abatement of fraud risk, its use could also result in some loss of privacy.

In some cases, identifying information on consumers has served to enable, rather than to deter, fraud.

16. *See Task Force on Stored-Value Cards (1997, 715–20) or Board of Governors (1997a, 52) for a discussion of these issues.*
17. *Stored-value cards that make use of data stored on magnetic strips are generally viewed as less secure than cards on which the data is stored on an electronic chip.*
18. *While it was difficult to detect individual fraudulent cards during this episode, the widespread use of such cards was public knowledge. According to Pollack (1996), the scale of the fraud became evident when long lines of people would form outside of certain pachinko parlors, hours before the parlors were open for business.*
19. *See, for example, Greenspan (1996), Dwyer (1996), Rolnick, Smith, and Weber (1997), McAndrews (1997b), or Schreft (1997).*
20. *Merchants used publications known as "banknote reporters" to keep track of the notes' current market value.*
21. *See, for example, Dillistin (1949) or Gorton (1996) on the prevalence of note fraud during the Free Banking Era.*
22. *At the time, restriction of note issue to large denominations was thought necessary to lessen the incidence of note fraud; see White (1995) for a discussion. The reasoning was that holders of small notes would lack sufficient incentive to check on their authenticity. Another motive for restricting issue of small-denomination notes was the fear that their issue would lead to inflation and ultimately to erosion of the gold standard; see Timberlake (1978, chap. 9). See Sargent and Wallace (1982) for a modern interpretation of this view.*
23. *The regional coalition of New England banks was known as the Suffolk System. See, for example, Calomiris and Kahn (1996) or Rolnick, Smith, and Weber (1997) on the operation of the Suffolk System.*
24. *See, for example, Blinder (1995), Kelley (1996), Greenspan (1996), and Kamihachi (1997).*
25. *See Board of Governors (1997b) or Bernstein (1997) for examples of commercially available data on consumers.*

In these "identity theft" cases, criminals have been able to use stolen information on a consumer to successfully impersonate the consumer in credit card transactions, loan applications, and the like.[26]

Both the need for privacy and the need to protect consumers from fraud resulting from identity theft can complicate the cost-benefit trade-off associated with fraud risk. Payments systems that make use of extensive consumer-identifying information can lessen the incidence of fraud, benefiting society. But the value of such information in reducing fraud must be balanced against the value of privacy, and recent cases of identity theft illustrate that such information may not always be used in a socially benevolent fashion.

Conclusion

An important function of any payments medium is to provide certainty of valuation in market exchanges. One of the risks that must be overcome by payments systems is the risk of fraud. Traditional payments media such as currency, checks, and credit cards have effectively contained fraud risk to a level of 20 basis points (0.2 percent) or less. To be successful in the marketplace, newer forms of payment will need to hold fraud risk to similarly low levels.

Incentives for fraud increase when transactions are made in large amounts, when transactions are made anonymously or at the point of sale, when claims cannot be effectively verified at the point of sale, and when issuers of payment claims bear the costs of fraudulent transactions. While these features may be desirable in some situations in that they allow for a greater range of transactions, they can also encourage fraud. The recent Japanese experience with stored-value cards illustrates that vigilance will be necessary in such cases.

Some of the new payments media have been compared with the banknotes used during the U.S. Free Banking Era. The banknotes were subject to substantial fraud risk and were widely discounted. It is unlikely that similar discounting will apply to new payment instruments, however. Modern communications technology and changes in the organization of the banking and payments industries should largely remove incentives for discounting.

Successful payments systems will also have to confront various trade-offs while addressing the problems posed by fraud. These trade-offs include the need to balance the costs of fraud abatement measures with their benefits, the need to balance security of payments systems with consumers' desire for privacy, and the need to encourage development of new, more efficient payments systems while ensuring equitable treatment of participants in these systems.

26. One such identity theft is recounted by Vickers (1996).

REFERENCES

American Bankers Association. 1994. *1994 ABA Check Fraud Survey.* Washington, D.C.

———. 1996. *1996 Bank Card Industry Survey Report.* Washington, D.C.

Bank for International Settlements. 1996a. *Security of Electronic Money.* Basel.

———. 1996b. *Statistics on Payments Systems in the Group of Ten Countries.* Basel.

Bernstein, Nina. 1997. "Online, High-Tech Sleuths Find Private Facts." *New York Times,* September 15, sec. A.

Blinder, Alan S. 1995. Statement before the Subcommittee on Domestic and International Monetary Policy, U.S. House Committee on Banking and Financial Services, October 11.

Bloom, Jennifer Kingson. 1997. "Visa and MasterCard Publish SET Protocol for Internet." *American Banker,* June 5.

Board of Governors of the Federal Reserve System. 1996a. "Electronic Funds Transfers." *Federal Register* 61 (May 2): 19696–705.

———. 1996b. *Report to Congress on Funds Availability Schedules and Check Fraud at Depository Institutions.* Washington, D.C.

———. 1997a. *Report to Congress on the Application of the Electronic Fund Transfer Act to Electronic Stored-Value Products.* Washington, D.C.

———. 1997b. *Report to Congress Concerning the Availability of Consumer Identifying Information and Financial Fraud.* Washington, D.C.

Calomiris, Charles W., and Charles M. Kahn. 1996. "The Efficiency of Self-Regulated Payments Systems: Learning from the Suffolk System." *Journal of Money, Credit, and Banking* 28 (November): 766–97.

Caskey, John P., and Gordon H. Sellon Jr. 1994. "Is the Debit Card Revolution Finally Here?" Federal Reserve Bank of Kansas City *Economic Review* 79 (Fourth Quarter): 79–95.

Congressional Budget Office. 1996. *Emerging Electronic Methods for Making Retail Payments.* Washington, D.C.

Dillistin, William H. 1949. *Banknote Reporters and Counterfeit Detectors, 1826–1866.* New York: American Numismatic Society.

Dwyer, Gerald P., Jr. 1996. "Wildcat Banking, Banking Panics, and Free Banking in the United States." Federal Reserve Bank of Atlanta *Economic Review* 81 (December): 1–20.

Federal Deposit Insurance Corporation. 1996. "Stored-Value Cards and Other Electronic Payments Systems." *Federal Register* 61 (August 2): 40494–97.

Fickenscher, Lisa. 1997. "MasterCard to Cap Consumer Debit Card Liability." *American Banker*, July 31.

Fryer, Bronwyn. 1996. "Visa Cracks Down on Fraud." *Information Week*, August 26.

Glain, Steve, and Norihiko Shirouzu. 1996. "How Japan's Attempt to Slow Nuclear Work in North Korea Failed." *Wall Street Journal*, July 24, sec. A.

Gorton, Gary. 1996. "Reputation Formation in Early Bank Note Markets." *Journal of Political Economy* 104 (April): 346–97.

Greenspan, Alan. 1996. Remarks at the U.S. Treasury Conference on Electronic Money and Banking: The Role of Government, Washington, D.C., September 19.

Hansell, Saul. 1994. "New Breed of Check Forgers Exploits Desktop Publishing." *New York Times*, August 15, sec. A.

Kamihachi, James. 1997. "Supervisory Issues in Electronic Money." Remarks at the *American Banker* Conference on Future Money, June 11. Available on the Internet at http://www.occ.treas.gov/emoney/kami6-11.htm.

Keenan, Charles. 1997. "Visa One-Ups Rival on Consumer Card Liability." *American Banker*, August 14.

Kelley, Edward W., Jr. 1996. Remarks at the CyberPayments '96 Conference, Dallas, Texas, June 18.

Lunt, Penny. 1996. "Is It First and Goal for Debit Cards?" *ABA Banking Journal* 88 (September): 44.

McAndrews, James J. 1997a. "Making Payments on the Internet." Federal Reserve Bank of Philadelphia *Business Review* (January/February): 3–14.

———. 1997b. "Banking and Payments System Stability in an Electronic Money World." Federal Reserve Bank of Philadelphia Working Paper 97-9.

Nielsen, David. 1994. "Check Fraud Rose 136 Percent Over Two Years, ABA Finds." *American Banker*, December 1.

Pearsall, Susan. 1994. "Combating Credit Card Fraud." *New York Times*, December 18, sec. CN.

Pollack, Andrew. 1996. "Counterfeiters of a New Stripe Give Japan One More Worry." *New York Times*, June 20, sec. D.

Rohter, Larry. 1997. "New Bank Fraud Wrinkle in Antigua: Russians on the Internet." *New York Times*, August 20, sec. A.

Rolnick, Arthur J., Bruce Smith, and Warren E. Weber. 1997. "Lessons from a Laissez-Faire Payments System: The Suffolk Banking System (1825–1858)." Federal Reserve Bank of Minneapolis Working Paper 584, September.

Rutledge, Gary. 1996. "Taming the Fraud Monster." *Credit World* (September/October): 10.

Sargent, Thomas J., and Neil Wallace. 1982. "The Real-Bills Doctrine versus the Quantity Theory: A Reconsideration." *Journal of Political Economy* 90 (December): 1212–36.

Schreft, Stacey. 1997. "Looking Forward: The Role for Government in Regulating Electronic Cash." Federal Reserve Bank of Kansas City *Economic Review* 82 (Fourth Quarter): 59–84.

"Survey of Electronic Commerce." 1997. *Economist*, May 10.

Task Force on Stored-Value Cards. 1997. "A Commercial Lawyer's Take on the Electronic Purse: An Analysis of Commercial Law Issues Associated with Stored-Value Cards and Electronic Money." *Business Lawyer* 52 (February): 653–727.

Timberlake, Richard H. 1978. *The Origins of Central Banking in the United States.* Cambridge, Mass.: Harvard University Press.

U.S. Department of the Treasury. 1996. "An Introduction to Electronic Money Issues." Paper prepared for the Treasury Department conference "Toward Electronic Money and Banking: The Role of the Government," Washington, D.C., September 19–20.

U.S. General Accounting Office. 1996. *Counterfeit U.S. Currency Abroad: Issues and U.S. Deterrence Efforts.* Washington, D.C.

———. 1997. *Payments, Clearance, and Settlement: A Guide to the Systems, Risk, and Issues.* Washington, D.C.

Vickers, Marcia. 1996. "Stop Thief! And Give Me Back My Name." *New York Times*, January 28, sec. C.

Weinberg, John A. 1997. "The Organization of Private Payment Networks." Federal Reserve Bank of Richmond *Economic Quarterly* 83 (Spring): 25–43.

White, Eugene N. 1995. "Free Banking, Denominational Restrictions, and Liability Insurance." In *Money and Banking: the American Experience*, 99–118. Fairfax, Va.: George Mason University Press.