



DISCUSSION PAPER

PAYMENT CARDS CENTER

The Evolution of EFT Networks from ATMs to New On-Line Debit Payment Products*

Stan Sienkiewicz

April 2002

***Summary:** On June 15, 2001, the Payment Cards Center of the Federal Reserve Bank of Philadelphia sponsored a workshop on the evolution of the electronic funds transfer (EFT) industry. Paul Tomasofofsky and Bruce Sussman of NYCE, the New Jersey-based electronic payments company, led the workshop. Beginning with a brief history of EFT and the automated teller machine (ATM) industry, Tomasofofsky and Sussman discussed the growth of debit card applications and various Internet payment mechanisms. They then described NYCE's new payment product, SafeDebit,TM which is designed to address security issues in making payments over the Internet. This paper provides highlights from the NYCE presentation and the ensuing discussion, complemented by additional background research on the structure and evolution of debit cards.*

*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.phil.frb.org

History of the EFT/ATM Industry

The origins of the electronic funds transfer (EFT) industry can be traced back to the introduction of the first automated teller machine (ATM) in the mid-1960s. The ATM was able to handle account transfers, accept deposits, and dispense cash using a standard magnetic stripe card and personal identification number (PIN). With the introduction and acceptance of ATMs, U.S. financial institutions entered the era of EFT systems.

The term EFT refers to the application of computer and telecommunication technology in making or processing payments. The term itself does not refer to a specific product. Rather, it is a descriptor that defines payment vehicles that use electronic networks instead of cash or checks to conduct a transaction. EFT networks are divided into two main types: wholesale and consumer. Wholesale EFT networks are typically used by financial institutions for large-dollar electronic transfers. Consumer EFT networks handle a variety of electronic payment services used by consumers and generally move small-dollar amounts

Historically, the core of consumer EFT networks has been the ATM and associated access cards. ATM networks were first established as proprietary systems that were owned by a bank or payments processor and that served a limited geographic area. In some cases, the proprietary systems were shared with other financial institutions to expand the network, but the proprietary bank provided the ATM processing. While sharing of ATM networks created economies of scale, its primary benefit was stimulating consumer demand. Financial institutions' customers discovered that their ATM/debit cards could be used to access their accounts at the financial institutions where they held accounts and at local financial institutions where they did not. Initially, these networks

were local, since the McFadden Act legally prohibited expansion into other states. This changed in 1985 when the U.S. Supreme Court upheld an earlier U.S. Court of Appeals decision that ATMs did not represent bank branches, thereby allowing interstate EFT networks to develop.²

With the restriction on interstate expansion of ATM networks lifted, financial institutions recognized that the costs of ATMs and the networks could be shared. As a result, shared regional ATM networks grew, typically as joint ventures of financial institutions within the same geographic area. The national networks, such as Plus and Cirrus, came later. While a shared ATM network allowed a bank's customers to gain access to their accounts and cash in other geographical areas, more important, it supported the deployment of ATMs at new locations. Since there is a minimum cost associated with the installation of each terminal, the sharing of an ATM with other financial institutions allows more ATMs to be placed in areas that may not have been profitable for a single bank. Therefore, economies of scale are realized through greater transaction volume.

This sharing of ATMs represents a network externality, which occurs when the value of a network increases as new users join the network. As more customers join the network, the network becomes more valuable to each user. This network externality results in "increasing returns," that is, as the network continues to grow, it becomes easier to attract additional users. The larger number of users in the expanded network makes deployment of new ATMs more profitable, which further enhances accessibility for

² *Independent Bankers Association of New York State v. Marine Midland Bank*, 583 F. Supp. 1042 (W.D.N.Y., 1984), rev'd in part, vacated in part, and remanded, 757 F.2d 453 *(2nd Cir., 1985), cert.denied, 476 U.S. 1186 (1986).

existing members. Typical examples of network externalities are telephone networks, fax machines, and railroads.

The number of ATM terminals has risen dramatically, from fewer than 10,000 terminals in 1978 to approximately 324,000 in 2001, processing over 1.1 billion transactions per month. This growth of both ATM terminals and volume demonstrates the public acceptance of ATMs. In fact, the number of access cards has increased from 60 million in 1982 to over 236 million in 2001.

As financial institutions began to recognize the benefits of shared ATM networks, the number of networks grew, reaching a peak of almost 200 in 1986.³ However, as the networks consolidated during the 1990s, either through mergers or outright purchases, the number of shared regional networks dropped to 30 in 2001. Currently, the top five networks handle over 78 percent of the transaction volume that is switched through shared regional networks.⁴

The very same factors that led to the development and expansion of the ATM networks led to the consolidation of the industry. First, since ATM networks have proven to have network externalities, the larger the network, the more consumers conduct transactions and accept usage fees. Driven by the increases in usage, network owners are eager to expand their existing network by purchasing additional networks. Second, since ATM networks made significant investments in technology and equipment, the more transactions processed over an individual network, the lower the costs become on a per unit basis. Networks, therefore, can take advantage of economies of scale. Third, with the change in interstate banking legislation, barriers to cross-state lines were eliminated,

³ James McAndrews, "The Evolution of Shared ATM Networks," Federal Reserve Bank of Philadelphia *Business Review* (May/June 1991), pp. 3-14.

allowing competing networks to acquire additional networks in other states and geographical locations.

Financial institutions initially believed that with the introduction of an ATM network, consumers would not use branches as extensively and issue fewer checks. They expected to realize cost savings by moving transactions from the high-cost branch locations to low-cost ATMs. These cost savings were assumed to be so great that financial institutions would be able to absorb the costs of the ATM infrastructure without charging usage fees. Although consumers did find the ability to withdraw cash and transfer balances without physically entering a bank appealing, the cost savings to the financial institutions were never realized. The number of ATM transactions grew dramatically, and the dollar size of transactions declined as consumers fell in love with ATMs as a source of easily accessible cash. At the same time, they did not decrease the number of checks written and continued to use bank branches and bank tellers for all other transactions. In the 1990s, financial institutions instituted transaction fees for ATM usage, especially for transactions made by customers from other banks.

EFT at the Point of Sale

As consumers became comfortable using debit cards for cash withdrawals and other banking transactions, the next logical step in the expanding ATM networks was to introduce the usage of debit cards for purchase at the point of sale. Purchases made at merchant locations using such debit cards are processed through EFT networks just as ATM transactions are processed. The first merchant PIN pads, enabling the debit

⁴ The statistics, both in this and the preceding paragraph, are from the McAndrews article and the *ATM & Debit News*, EFT Data Book, 2002 Edition.

transaction, were installed at supermarkets during the early 1980s. After the establishment of PIN-based debit cards at supermarkets, customers were able to use their ATM/debit cards not just to pay for their purchases but also to receive cash back. The cash back option became popular with supermarket retailers, since store owners recognized savings as a result of less cash to count at the end of the day, a chore that represented a carrying cost to the establishment. In addition, with ATM surcharging in the 1990s, consumers found it cheaper to receive cash back at the counter versus using an ATM terminal in the supermarket that may have charged a usage fee.

When a customer uses his or her PIN for authentication at an ATM or at a merchant location, he or she is participating in what is called an “on-line” debit transaction. These on-line debit transactions are settled by an immediate debit to the consumer’s bank account. As financial institutions and their EFT networks worked to encourage use of debit cards at the point of sale, they met initial resistance from the merchant community. Some resistance was due to the cost incurred in purchasing and maintaining a unique terminal for POS debits. Another problem was related to the operation of the EFT networks themselves. The early EFT networks did not permit interoperability among EFT systems, requiring the merchant to maintain separate terminals for each competing brand.

Visa and MasterCard also introduced their own debit option, the Visa Check and MasterMoney cards, respectively. However, these cards differed from the regional ATM/debit cards in that transactions performed with these cards were considered “off-line” debit transactions. In an off-line debit transaction, the consumer does not use a PIN, but rather signs a sales receipt to authenticate the transaction. As such, the transaction

flows over the bankcard association's credit card network. In addition, since no issuer electronically authenticates the consumer when performing this transaction, this type of transaction bears a higher risk to the merchant.

As a result, the 1990s saw these off-line and on-line debit cards vying for their share of market transactions. Off-line debit cards began to prosper in the mid-1990s when financial institutions added the Visa and MasterCard logos to their ATM cards. With greater merchant acceptance due to the addition of the Visa and MasterCard logos to the ATM card, off-line transactions began to exceed on-line transactions at merchant locations. In 1994, off-line transactions totaled 279.3 million transactions versus on-line transactions of 429.6 million. By 1999, aided by aggressive advertising by the bankcard associations, off-line transactions grew to 4,064 million versus on-line transactions of 2,900 million.⁵

Data since 1999 indicate that on-line transactions have grown at an average annual rate of 38 percent, to 5,200 million in 2001. By comparison, off-line transactions grew at an average annual rate of 33 percent to 6,800 million.

Part of the reason for more rapid recent growth in on-line transactions is that merchants prefer on-line debit. Financial institutions that issue on-line and off-line debit cards (issuers) charge acquirers (the merchant's bank) an interchange fee to recoup the cost of the network infrastructure, a situation similar to the credit card interchange structure.⁶ Acquirers, in turn, pass these charges on to merchants as part of a "merchant discount." Interchange fees are substantially lower for on-line debit transactions than off-line debit transactions.

⁵ *ATM & Debit News*, EFT Data Book, 2002, Thomson Financial.

⁶ Payment Cards Center Workshop Series, "Credit Cards and Payment Efficiency," <http://www.phil.frb.org/pcc/conferences/workshop3.pdf>

Many merchants “prompt” consumers to use PIN-based on-line debits at the point of sale, and some would prefer to accept only the on-line cards. In 1996, a group of merchants, led by Wal-Mart, filed a suit against Visa and MasterCard.⁷ The suit disputes Visa’s and MasterCard’s honor-all-cards rule, which requires all Visa and MasterCard merchants to accept all cards bearing the Visa or MasterCard logo. The merchants argue that they do not want to accept the off-line debit card issued by Visa and MasterCard because acceptance of these cards leads to increased costs to the merchant. The suits were consolidated in the U.S. District Court of New York, and a trial date had not been set as of this writing.

Internet Transactions and Payment Options

While financial institutions, EFT processors, and the bankcard associations were developing debit card products for purchases at merchant locations, Internet sales volumes began to increase during the late 1990s and the Internet became a new market for developing payment vehicles. According to a recent article in *Credit Card Management*, over 40 percent of adults made online purchases in 2001.⁸

The market for consumer-to-business payments over the Internet has grown substantially over the last few years, but it is still only a small portion of the personal consumption market. NYCE’s Tomasofsky noted that while consumer-to-business Internet sales grew more than 66 percent in 2000, they accounted for only 2 percent of total consumer-to-business transactions. However, this number is expected to grow over time. He cited industry estimates that currently 79 million consumers shop on the

⁷ *Wal-Mart Stores, Inc., The Limited, Inc., and All Similarly Situated Parties v. Visa U.S.A., Inc.* (E.D.N.Y., October 25, 1996).

⁸ “Secure Internet Shopping, Take 2,” *Credit Card Management*, (September 2001), pp. 22-30.

Internet, resulting in sales of \$39 billion. By 2004, over 138 million consumers are expected to use the Internet to purchase goods worth over \$184 billion. Some of this is due to customers switching from shopping at a merchant's physical establishment to using its web site for shopping. Also, brick-and-mortar establishments see the Internet as an additional distribution channel and are promoting their Internet sites.

While various forms of payment — including cash, check, credit and debit cards — are accepted in brick-and-mortar locations, credit cards are currently the payment vehicle of choice for transactions conducted on the Internet. However, accepting credit cards via the Internet poses a problem of authenticating the card to the cardholder, since the merchant cannot verify the customer's identity. Unlike point-of-sale transactions at a merchant location where either a PIN or signature verification is used to authenticate the card to the cardholder, there is no such authentication capability in the card-not-present environment. This exposes on-line retailers to increased risk of fraud. Based on current industry reports, the percentage of fraud on the Internet is estimated to be around 1.5 percent of total purchases. Since it is the merchant who is responsible for the cost if the cardholder claims the charges were fraudulent, merchants sometimes pay for fraud detection services, increasing their cost of doing business on the Internet.

Companies that sell merchandise over the Internet are looking for more secure and cheaper payment mechanisms for the card-not-present environment. Various schemes have been created to help solve this problem while improving ease of use for consumers and lowering risk to merchants. The two major credit card associations, Visa and MasterCard, have recently developed a guaranteed payment program for merchants that use their own proprietary authentication systems. Visa's "Verified by Visa" is an on-line

security feature whereby the issuer authenticates the cardholder in real time at participating merchant sites by prompting the cardholder to enter a password.

MasterCard's "Secure Payment Application" (SPA) is also designed to authenticate cardholders when they pay on the Internet. This system requires consumers to install a wallet application on their personal computers that will generate a unique value to each transaction, which is authenticated by the issuer at the time of the transaction. Unlike Visa's application, the MasterCard SPA does not require a password unless the issuer requires its use.

Another new payment vehicle aimed at providing greater security to both the merchant and consumer for Internet transactions is the smart card. The United States consumer's first encounter with smart cards as a tool for making payments was with the introduction of American Express's Blue Card in 1999. Smart cards are plastic cards, similar in appearance to a typical credit card, but with a microcomputer or memory chip embedded in it. There has been great interest in the use of smart cards, especially since the cards are marketed as safer to use for both in-person and Internet transactions.

Some smart cards are considered as being safer for consumers to use because the chip on the card can have a PIN stored on it and can be used for a transaction only if the consumer uses the correct PIN. For merchants, accepting a transaction originated by a smart card provides greater assurance that the card is being used properly, since it provides two authentication forms, namely, the card number and that the consumer is in possession of the card. However, a hindrance to wider use of smart cards for Internet transactions is that consumers need to purchase and install specific hardware on their personal computers to allow them to use the card for transactions. To date, smart cards

are considered an emerging payment that has yet to become generally accepted by both merchants and consumers. However, if major retailers such as Target gain market acceptance with their smart card product, both consumers and merchants may increase their demand for the product.

Internet and PIN-Based Debit

Although consumers have quickly adapted to the use of debit cards at merchant locations, the next challenge seen by EFT networks is gaining the same level of acceptance for Internet-based purchases where credit cards are still the payment vehicle of choice. Despite their popular use, credit cards have two important limitations in the Internet or card-not-present environments. First, as noted earlier, the lack of authentication capability exposes merchants to greater risk of fraud and higher chargebacks for Internet-based credit card purchases. Second, credit card transactions, relative to those made with on-line debit cards, are assessed higher interchange fees. There is anecdotal evidence as well that many consumers are concerned about the security of using credit cards on the Internet and, as a result, will not shop over this medium.

Among the several solutions under development in the payment card industry is NYCE's SafeDebit™ product. SafeDebit™ is a PIN-secured Internet debit payment product. Tomasofsky and Sussman explained that SafeDebit™ operates much the same way as a normal PIN-based debit transaction, allowing consumers to pay for purchases on the Internet with funds withdrawn directly from their checking accounts. The primary difference is that rather than entering a PIN at a merchant's terminal, consumers use a

CD-ROM “card” and a PIN to make secure Internet purchases from any personal computer, anywhere, at anytime. The transaction is routed from the consumer’s computer, in encrypted form, through multiple processing points until an approval message is routed back to the consumer from his or her financial institution. Because of the routing, the consumer’s account number and other sensitive data never reside on the merchant’s system. A typical transaction takes about 10 seconds to complete.

SafeDebit™ addresses the two major challenges to using payment cards on the Internet: processing cost and security. SafeDebit™ carries a relatively lower interchange fee and employs a level of security using triple DES encryption in an already established transactional flow for authentication and authorization.

Conclusion

SafeDebit™ and other emerging applications demonstrate the continuing innovation taking place in the payment cards industry. As consumers’ needs evolve and technology advances create new opportunities, the EFT industry continues to adapt and grow. From its rather straightforward beginning with ATMs to the application of secure payments on the Internet, the EFT industry has supported the continued development of payment cards. An important role of the Payment Cards Center is to monitor these new developments and provide insight into innovative and creative applications of payment cards designed to improve payment system efficiency and effectiveness.