UNITED STATES OF AMERICA
BEFORE FEDERAL TRADE COMMISSION

In the Matter of Proposed Amendment to the Commission's Telemarketing Sales Rule	FTC File No. R411001

COMMENTS OF COLLIER SHANNON SCOTT, PLLC ON THE COMMISSION'S PROPOSED AMENDMENTS TO THE TELEMARKETING SALES RULE

COLLIER SHANNON SCOTT, PLLC
3050 K Street, NW, Suite 400
Washington, DC 20007
202.342.8400

By: Lewis Rose, Esq.
LRose@colliershannon.com, 202.342.8821

D. Reed Freeman, Jr., Esq.
DFreeman@colliershannon.com, 202.342.8615

Gonzalo E. Mon, Esq.
GMon@colliershannon.com, 202.342.8576

Dated: April 12, 2002

Collier Shannon Scott, PLLC ("Collier Shannon") files these comments pursuant to the Federal Trade Commission's (the "Commission") Notice of Proposed Rulemaking[1] regarding the Telemarketing Sales Rule ("TSR").[2] Collier Shannon is a Washington-based law firm with sixteen lawyers focused on consumer protection issues, five of whom are former Federal Trade Commission staff attorneys, attorney advisors, or senior managers. Our clients include numerous companies that accept debit cards in connection with telemarketing transactions.

I. EXECUTIVE SUMMARY

These comments argue that the Commission's proposal to apply to TSR's express verifiable authorization requirements to debit cards finds no support in policy or law.

There are strong policy reasons supporting the equal treatment of credit, charge, and debit cards under the TSR. Merchants that process credit and debit card transaction over the phone do not have the ability to differentiate between credit cards and debit cards. In other words, merchants are unable to tell whether a sixteen-digit Visa number provided by a consumer is associated with a credit or debit card account. Therefore, in order to comply with the TSR as the Commission proposes to amend it, merchants would have to seek express verifiable authorization from all consumers that use credit or debit cards. This burdensome, expensive result it not what the Commission intends, and is not likely to result in any greater protection for consumers than they already have.

---

[1] *See* 67 Fed. Reg. 4492 (Jan. 30, 2002).

[2] *See* 16 C.F.R. § 310 (2001).

The Commission's proposal to apply the TSR's express verifiable authorization provisions to transactions that do not have the limited liability and dispute resolution "protections provided by, or comparable to those available under, the Fair Credit Billing Act ("FCBA") and the Truth in Lending Act ("TILA")"[3] does not apply to debit cards as a matter of law. Transactions completed with debit cards[4] are afforded liability limitations and dispute resolution protections that are at least comparable — and, in some cases, superior — to those available under the TILA, the FCBA, and their implementing Regulation Z. Accordingly, Collier Shannon respectfully requests that the Commission clarify in the Statement of Basis and Purpose supporting the amended TSR that transactions completed with debit cards are subject to limited liability and dispute resolution protections that are comparable to those available under the FCBA and the TILA, and are therefore not subject to the "express verifiable authorization" requirements of proposed section 310.3(a)(3).

With regard to liability limitation for unauthorized use, the Electronic Funds Transfer Act ("EFTA")[5] and its implementing Regulation E[6] provide a $50 cap on liability for unauthorized use of consumers' debit cards, provided that consumers notify

---

[3] 67 Fed. Reg. at 4507.

[4] The term "debit card" is synonymous with the term "check card." A debit card is linked to a consumer's account. When a consumer uses a debit card, he or she subtracts money from his or her own bank account. Thus, unlike credit cards, debit cards only allow a consumer to spend money that is presently in his or her bank account. *See, e.g.*, FTC, *A Consumer's Guide to E-Payments* <http://www.ftc.gov/bcp/conline/pubs/online/payments.htm>.

[5] *See* 15 U.S.C. § §§ 1693-1693r (2001).

[6] *See* 12 C.F.R. §§ 205.1-205.15.

their financial institution within two days of learning of such unauthorized use. Moreover, Visa International Service Association ("Visa") and MasterCard International Inc. ("MasterCard") have both implemented "zero liability" policies that protect debit card holders from unauthorized use of their cards.

With regard to dispute resolution, the EFTA and Regulation E provide debit card holder consumers with similar, and, in many cases, superior, dispute resolution provisions to those provided to credit and charge card holders under Regulation Z.

The Commission's proposal to expand the types of transactions for which express verifiable authorization will be required is also based upon the Commission's experience in law enforcement actions. For several newly-developed payment methods, the Commission has found that consumers may not understand that by providing certain information (such as their checking account numbers), they will be billed. This concern does not apply to the use of debit cards because consumers understand that when they provide merchants with their debit card account numbers, their checking accounts will be debited. Nothing in the rulemaking record — or, for that matter, the Commission's law enforcement actions — suggests that consumers unwittingly obligate themselves by providing their debit card numbers to merchants. In sum, the Commission's concerns regarding newly-developed alternative payment methods do not apply to debit cards, and thus do not support treating transactions involving debit cards in any way different than it treats transactions involving credit and charge cards.

Based on the foregoing, Collier Shannon respectfully requests that the Commission treat debit card transactions under the TSR in the same manner that it treats

credit card transactions. That is, transactions completed using debit cards should not be subject to the "express authorization" requirements the TSR currently imposes on transactions involving electronic checking account debiting, and which the Commission proposes to apply to other payment methods.

II. ARGUMENT

The TSR currently requires that a telemarketer obtain express verifiable authorization in all sales involving a payment "drawn on a person's checking, savings, share, or similar account."[7] Authorization is deemed "verifiable" if any one of three specified methods are employed to obtain it: (1) express written authorization by the consumer (which includes a consumer's signature on a negotiable instrument such as a paper check); (2) express oral authorization that is tape recorded; or (3) written confirmation of the transaction that is sent to the customer before submission of the draft for payment.[8]

The Commission proposes to extend these requirements to other payment methods such as the use of "debit cards, developing electronic payment systems, and the growing use, by unrelated vendors, of the billing and collection systems of mortgage or utility companies . . . ."[9] The Commission's proposal is motivated by two concerns. First, the Commission is concerned that many emerging payment methods do not offer consumers limited liability and dispute resolution protections that are comparable to those available for credit and charge card users

[7] *Id*. § 310.3(a)(3).

[8] *See id*.

[9] *See* 67 Fed. Reg. at 4506.

under the FCBA and the TILA, and their implementing Regulation Z.[10] Second, the Commission is concerned that consumers who use certain types of payment methods may not be aware that they can be billed for a purchase through such methods. Neither of these concerns apply with regard to the use of debit cards.

A. Express Verifiable Authorization For Debit Cards Will Have The Practical Effect Of Requiring Express Verifiable Authorization For Credit Card Transactions.

Although the Commission does not propose to extend the express verifiable authorization requirements to credit cards, the Commission's proposal would have that effect. Merchants who process credit and debit card transaction over the phone do not have the ability to differentiate between credit cards and debit cards. In comments we prepared in 1999 in connection with the Commission's proposed amendments to the 900-Number Rule, we noted that a company had sent an email to Visa asking how merchants may determine whether a number provided by a consumer is a credit or debit card. A copy of that email is reprinted below.

> *Sent:* *Tuesday, December 15, 1998 21:11*
>
> *To:* *VisaExpo Correspondence*
>
> *Subject:* *Question on Visa Check Cards*
>
> *I am a merchant that accepts Visa on non-face-to-face transactions. For example, my company has numerous web sites which accept Visa. How can I know if a Visa card entered by the consumer over the Internet is a "check card" or a conventional credit card? Does Visa or its merchant banks issue check cards on unique bin's?*

Visa responded as follows:

> *From:* *VisaExpo Correspondence [SMTP: webbalto@visa.com]*

[10] *See id*. at 4507.

Sent: *Tuesday, December 15, 1998 23:15*

Subject: *RE: Question on Visa Check Cards*

Thank you for your message. Currently, Visa makes no distinction between credit cards and check (debit) cards. Thank you for writing.

Accordingly, Visa itself recognizes that merchants are unable to discern whether a number provided by a customer relates to a debit or credit card. Were the Commission to require express verifiable authorization for debit cards, merchants would be forced to seek express verifiable authorization for credit and debit card transactions or risk the possibility of violating the TSR and accruing massive civil penalty liability.

B. The Use Of Debit Cards Is Subject To Liability Limitations And Dispute Resolution Protections That Are At Least Comparable To Those Available Under The FCBA And The TILA.

TILA and its implementing Regulation Z limit a consumer's liability for unauthorized credit or charge card transactions to $50[11] and provide dispute resolution procedures for consumers to resolve billing errors.[12] Although these provisions do not apply to transactions that are completed using debit cards, other federal regulations and private sector initiatives provide users of these cards with protections that are at least comparable to those available under the FCBA, the TILA, and their implementing Regulation Z.

[11] *See* 12 C.F.R. § 226.12(b)(1). In order to take advantage of this liability limitation, a consumer must provide the card issuer with pertinent information about the loss, theft, or unauthorized use of his or her card. *See id*. § 226.12(b)(3).

[12] *See id*. § 226.13.

1. The Public And Private Sectors Offer Liability Limitations That Are Comparable, Or Superior, To Those Offered Under The FCBA And TILA.

a. Public sector provisions are comparable to, and in many cases exceed, those offered under the FCBA and TILA.

A consumer's liability for unauthorized electronic funds transfers is limited by the EFTA[13] and its implementing Regulation E.[14] The EFTA defines an "electronic funds transfer" as "any transfer of funds . . . which is initiated through . . . [a] telephonic instrument . . . so as to order, instruct, or authorize a financial institution to debit or credit an account."[15] Regulation E provides that the term "electronic fund transfer" includes transfers that result "from debit card transactions."[16]

Under Regulation E, a consumer's liability for an unauthorized electronic fund transfer[17] is determined by the timeliness of the notice given by the consumer to the financial institution holding the account. If a consumer notifies a financial institution within two business days after learning of the loss or theft of the card or the code used to access the customer's account, the consumer's liability is limited to the lesser of $50 or the amount of the unauthorized transfers that occurred before the consumer gave notice to

[13] *See* 15 U.S.C. §§ 1693-1693r.

[14] *See* 12 C.F.R. §§ 205.1-205.15.

[15] 15 U.S.C. § 1693a(6).

[16] *Id*. § 205.3(b)(5).

[17] An "unauthorized electronic fund transfer" is "an electronic fund transfer from a consumer's account initiated by a person other than the consumer without actual authority to initiate such transfer and from which the consumer receives no benefit . . . ." 15 U.S.C. § 1693a(11).

the financial institution.[18] This protection is comparable to that offered to consumers who use credit cards, with the only difference being that Regulation E requires consumers to notify their financial institutions of a theft or loss of their debit cards or codes within two business days of becoming aware of such loss.[19]

b. Private sector limitations of liability are superior to those offered under the FCBA and TILA.

Both Visa[20] and MasterCard[21] have recently enacted zero liability policies that offer consumers who use both credit and debit cards limitations of liability extending beyond those provided by Regulation E or Regulation Z. Under these policies, consumers are not held liable for *any* unauthorized charges on their debit cards, and they are not subject to Regulation E's two-business-day reporting requirement.

Last year, Mark MacCarthy, Visa's Senior Vice President for Public Policy, testified before Congress regarding Visa's commitment to reducing online fraud. Mr. MacCarthy noted that Visa has taken steps beyond those required by federal regulations to ensure that consumers are protected against liability arising from unauthorized transactions using their debit and credit cards:

---

[18] *See id*. § 205.6(b)(1). If, however, the consumer fails to notify the financial institution within two business days, the consumer's liability is the lesser of $500 or the sum of: (A) $50 or the amount of unauthorized transfers that occur after the close of two business days, which ever is less; and (b) the amount of unauthorized transfers that occur after the close of two business days and before notice to the institution. *See id*. § 205.6(b)(2).

[19] Under Regulation Z, a credit card holder's liability for unauthorized transactions "shall not exceed the lesser of $50 or the amount of money, property labor, or services obtained by the unauthorized use before notification to the card issuer . . . ." *See id*. § 226.12(b).

[20] Visa's description of its zero liability policy is attached as Appendix A.

[21] MasterCard's description of its zero liability policy is attached as Appendix B.

> In April 2000, a new Visa operating regulation went into effect that eliminated consumer liability in cases of unauthorized use of Visa payment cards. This zero liability policy covers the use of all Visa consumer card products — including debit and credit cards. As a result of this new policy, a consumer will not be held liable for unauthorized use of any Visa payment card.[22]

Visa decided to implement its zero liability policy to ensure that cardholders are comfortable and secure when using their Visa cards.[23]

Similarly, Joshua L. Peirez, MasterCard's Senior Legislative and Regulatory Counsel testified last year before Congress regarding MasterCard's initiatives to protect its credit and debit cardholders against liability for unauthorized transactions. Mr. Peirez noted that under "MasterCard rules, a [debit or credit] cardholder victimized by unauthorized use generally will not be liable for any losses at all."[24] MasterCard implemented its zero liability policy in order give each of its cardholders the "confidence that they will have no liability in the unlikely event that their account number is misused."[25]

---

[22] Mark MacCarthy, Testimony Before the House Energy and Commerce Committee, Subcommittee on Commerce, Trade and Consumer Protection (May 23, 2001) (attached as Appendix C).

[23] *See id*.

[24] Joshua L. Peirez, Testimony Before House Financial Services Committee, Subcommittee on Financial Services and Consumer Credit (Nov. 1, 2001) (attached as Appendix D).

[25] *See id*.

Thus, consumers who use Visa and MasterCard debit cards enjoy exactly the same protections against unauthorized transactions as do consumers who use credit cards.[26] These protections are superior to those offered under either Regulation E or Regulation Z.

In 1997, the Federal Reserve Board testified before Congress against then-pending legislation designed to impose consumer protections on issuers of debit cards, preferring instead to rely on the market to provide incentives for debit card issuers to do so voluntarily.[27] Five years later, the Federal Reserve Board's predictions have materialized. The result of Visa's and MasterCard's zero liability policies is that consumers who use Visa and MasterCard *debit* cards enjoy superior protections against unauthorized transactions to those offered by Regulation Z to Visa and MasterCard *credit* card holders. Imposing additional regulatory burdens on transactions involving debit cards would provide consumers with no protections beyond what they now enjoy, and should be avoided in light of the potential for unintended consequences that unnecessarily burden legitimate commerce.

2. The Use of Debit Cards is Subject to Dispute Resolution Provisions that are Comparable to Those Offered under the FCBA and the TILA.

Although the dispute resolution provisions in Regulation Z do not apply to debit cards, Regulation E offers consumers who use debit cards protections that are comparable — or, in some cases, superior — to those offered by Regulation Z. A side-by-side

[26] We note that Discover Bank does not offer a debit card.

[27] Laurence H. Meyer, Testimony Before the House Committee on Banking and Financial Services, Subcommittee on Financial Institutions of Consumer Credit, (September 24, 1994) (attached as Appendix E).

comparison of the dispute resolution protections offered by Regulation Z and Regulation E follows. A chart comparing these two regulations is attached as Appendix F.

a. Consumer Requirements

Under Regulation Z, a consumer who experiences a billing error must notify a creditor in writing within sixty days after the creditor sent the first statement that contained the error.[28] Under Regulation E, a consumer must also notify a financial institution within sixty days of receiving a statement that contains an error.[29] Regulation E does not itself require that these notices be in writing, although it does permit financial institutions to require consumers to give written confirmation within ten days of an oral notice of a billing error.[30] The requirements imposed on consumers under Regulation E are therefore comparable, if not more lenient for consumers, than the requirements imposed by Regulation Z.

b. Timing of the Investigation

Under Regulation Z, a creditor must conduct a "reasonable investigation" into whether a billing error occurred within ninety days of receiving a consumer's billing error notice.[31]

Under Regulation E, a financial institution must generally conduct an investigation within only *ten* business days of receiving a notice of error.[32] If a financial institution is

[28] *See* 12 C.F.R. § 226.13(b).

[29] *See id*. § 205.11(b).

[30] *See id*. § 205.11(b)(2).

[31] *See id*. § 226.13(c)(2).

not able to complete the investigation within the ten-day time period, it must provisionally "credit[] the consumer's account in the amount of the alleged error (including interest where applicable)," and so notify the consumer.[33] The financial institution will then have an additional thirty-five days in which to conduct its investigation.[34] During this period, the consumer will have full use of the provisional credit.[35] In many instances, therefore, the financial institution must complete its investigation regarding the consumer's billing error notice within forty-five days of its receipt of a consumer's billing error notice. This is at least forty-five days *less* than the time afforded creditors under Regulation Z. Accordingly, the time requirements for an investigation under Regulation E are therefore comparable, if not more favorable to consumers, to the timing requirements under Regulation Z.

c. Treatment of the Disputed Transaction During the Investigation

Under Regulation Z, a creditor may not require a consumer to pay a disputed amount pending the investigation of the consumer's billing error notice.[36] In addition,

---

[32] *See id*. § 205.11(c)(1). If the notice of error involves an electronic fund transfer within thirty days of the first deposit to the account, the bank will have twenty business days to investigate. *See id*. § 205.11(c)(3)(i).

[33] *See id*. § 205.11(c)(2)(i).

[34] *See id*. § 205.11(c)(2). If the notice of error involves an electronic fund transfer that was not initiated within a state, resulted from a point-of-sale transaction, or occurred within thirty days of the first deposit into the account, the bank will have ninety days to investigate. *See id*. § 205.11(c)(3)(ii).

[35] *See id*. § 205.11(c)(2)(ii).

[36] *See id*. § 226.13(d)(1).

the creditor may not make or threaten to make any adverse report to any person about the consumer's credit standing.[37]

Regulation E has no comparable provision because Regulation E does not apply to credit transactions. Because debit card transactions do not result in an amount owed by a consumer to a creditor, there is no debt to collect or to report to a credit reporting agency. Nevertheless, as noted above, if a financial institution is unable to finish its investigation within ten days, it must issue a provisional credit to the consumer.[38] Therefore, just as a credit card holder will have access to the disputed funds because the creditor is prevented from collecting them, a debit card holder will also have access to the disputed funds in his or her account after ten days because a financial institution is required to issue the consumer a provisional credit.

d. Results of the Investigation

Under Regulation Z, a creditor must send a consumer a written report with the results of the investigation within ninety days of receipt of a billing error notice.[39] If the creditor determines that there had been a billing error, it must credit the consumer's account; otherwise the creditor must generally explain why it concluded that there had been no error.[40] The creditor must also notify the consumer in writing of the time when payment is due.[41]

---

[37] *See id*. § 226.13(d)(2).

[38] *See id*. § 205.11(c)(2)(i).

[39] *See id*. § 226.13(e).

[40] *See id*. § 226.13(f).

[41] *See id*. § 226.13(g).

Under Regulation E, a financial institution must send a consumer who has submitted a billing error notice a report with the results of the investigation within three days after completing the investigation, which can be no later than forty-five days after the financial institution's receipt of the consumer's oral or written notice. If the financial institution determines that an error had occurred, it must credit the consumer's account within one day of discovering the error.[42] If the financial institution determines that no error had occurred, it must give the consumer a written explanation of its determination.[43] If the financial institution had issued a provisional credit to the consumer, it must notify the consumer that the provisional credit will be debited and that the financial institution will honor checks payable to third parties for five days after the notification.[44]

Based on the foregoing, he provisions regarding the outcome of the financial institution's investigation and the issuing of any credit offered by Regulation E are comparable to those offered by Regulation Z.

C. Consumers Who Use Debit Cards Understand That Their Accounts Will Be Debited.

In its proposal, the Commission notes that consumers who use certain emerging billing methods "have no reason to anticipate that their accounts can be debited or charged without their signatures, and they may be induced to divulge their billing

[42] *See id*. § 205.11(c)(1). If the financial institution had already issued the consumer a provisional credit, it must notify the consumer that the credit has been made final. *See id*. § 205.11(c)(2)(iii)-(iv).

[43] *See id*. § 205.11(d)(1).

[44] *See id*. § 205.11(d)(2).

information on the basis of this misperception."[45] For example, the Commission has noted that some consumers who were unfamiliar with demand drafts unwittingly provided their bank account numbers to telemarketers without knowing that their accounts would be debited in absence of a signed check.[46]

This concern does not apply to consumers' use of debit cards. Unlike electronic demand drafts, for example, which may be unfamiliar to consumers, debit cards are used in the same manner as credit cards. Debit cards also look like credit cards and are used interchangeably with credit cards. It is just as unlikely that a consumer would give a debit card number to a merchant without knowing that his or her account will be debited as it is that a consumer would give a credit card number to a merchant without knowing that his or her account will be charged. Indeed, there is no evidence in the record of this entire rulemaking proceeding suggesting that consumers do not understand that by giving their debit card numbers, their accounts will be debited.

D. Proposed Changes to the FTC's Proposal

Collier Shannon respectfully requests that the Commission clarify in the Statement of Basis and Purpose supporting the revised TSR that section 310.3(a)(3) does not apply to transactions in which consumers use their debit cards because debit cards are subject to protections that are "comparable" to those afforded to credit card transactions.

---

[45] *Id*.

[46] 60 Fed. Reg. at 43850.

III. CONCLUSION

The Commission has carefully avoided adopting regulations that eliminate emerging payment methods, especially when those methods are not "in and of themselves necessarily harmful."[47] Debit cards, of course, are not harmful in and of themselves. Both the public and private sectors have addressed the limited liability and dispute resolution concerns expressed by the Commission regarding emerging billing methods. Moreover, it is unlikely that a consumer would give a merchant his debit card account number without realizing that his account will be debited. Accordingly, Collier Shannon respectfully requests that the Commission expressly note in the Statement of Basis and Purpose supporting the amended TSR that section 310.3(a)(3) does not apply to transactions in which consumers use debit cards.

We would be happy to meet with the Commission or the Staff to discuss these comments.

Respectfully submitted,

Lewis Rose, Esq.
D. Reed Freeman, Jr., Esq.
Gonzalo E. Mon, Esq.

COLLIER SHANNON SCOTT, PLLC
3050 K Street, NW, Suite 400
Washington, DC 20007

Dated: April 12, 2002

[47] Final Telemarketing Sales Rule, 60 Fed. Reg. 43,842, 43,851 (Aug. 23, 1995) (refusing to require signed authorization for demand drafts, as such a requirement would "be tantamount to eliminating this emerging payment alternative.")

Federal News Service

May 23, 2001, Wednesday

SECTION: PREPARED TESTIMONY

LENGTH: 4363 words

HEADLINE: PREPARED TESTIMONY OF MARK MACCARTHY SENIOR VICE PRESIDENT PUBLIC POLICY VISA U.S.A. INC.

BEFORE THE HOUSE ENERGY AND COMMERCE COMMITTEE SUBCOMMITTEE ON COMMERCE, TRADE AND CONSUMER PROTECTION

SUBJECT - "ON-LINE FRAUD AND CRIME: ARE CONSUMERS SAFE?"

BODY:

Chairman Steams, Ranking Minority Member Towns, and Members of the Subcommittee, my name is Mark MacCarthy, and I am Senior Vice President for Public Policy for Visa U.S.A. Inc. Thank you for the invitation to participate in this hearing on Online Fraud.

The Visa Payment System is a membership organization comprised of 21,000 financial institutions licensed to use the Visa service marks. It is the largest consumer payment system in the world. Over 1 billion Visa-branded cards are accepted at over 20 million locations worldwide. Consumers use their Visa cards to buy over $1.8 trillion in goods and services worldwide. Visa U.S.A., which is part of the Visa Payment System, is comprised of 14,000 U.S. financial institutions. U.S. customers carry about 350 million Visa-branded cards and use them to buy over $800 billion worth of goods and services annually. Electronic commerce is vital to the U.S. economy and to the prospects for our continued economic growth. The size of electronic commerce is difficult to measure and there are gaps of tens of billions of dollars in estimates between different consulting groups. There is no doubt that electronic commerce is a large, growing and permanent new channel for the sale of goods and services to consumers. The Department of Commerce estimates, for example, that online retail sales grew from less than $5.2 billion in the fourth quarter of 1999 to almost $8.7 billion in the same quarter one year later. Sales projections for the electronic commerce market range from $35 billion to $76 billion by the year 2002. By any measure, this counts as explosive growth.

Visa is the leading consumer electronic commerce payment system in the world. Payment cards now account for some 95 percent of online consumer transactions and

Visa accounts for 53 percent of the payment card portion. We expect 10 percent of Visa's overall transaction volume to come from Internet purchases by 2003, up from 2 percent today.

There are some who suggest that online commerce is lagging because people are afraid to shop online. But increasing numbers of people are shopping online, and we expect that comfort levels will grow, as more people become familiar with this new channel of commerce. This is certainly what happened with mail order and catalog and telephone order transactions in the past.

In our view, consumers should continue to feel comfortable using their Visa payment cards to shop online. Fraudulent use of Visa payment cards is at an all-time low. Fraud as a percentage of our total volume has declined over time. In the late 1980s, fraud accounted for about 0.20 percent of total Visa card volume; in the early 1990s, it was about 0.15 percent; today it's a mere 0.07 percent.

Visa has taken steps to promote consumer confidence in this new channel of commerce. These steps include:

- A zero liability policy for unauthorized use of our payment cards.

- Guidance for consumers shopping online.

A range of programs designed to help Internet merchants reduce the risk of unauthorized card use.

A tough new security program that went into effect on May 1, 2001 to protect cardholder data housed in web merchant databases.

An effective system for resolving consumer disputes with online merchants through our chargeback procedures.

Steps to insure online privacy protections for electronic shoppers.

ZERO LIABILITY Under Federal regulations, credit card issuers are required to limit liability for unauthorized use of credit cards to $50. Visa has chosen to go beyond this requirement to ensure that cardholders are fully protected against any monetary losses due to fraudulent use of their payment cards.

In April 2000, a new Visa operating regulation went into effect that eliminates consumer liability in cases of unauthorized use of Visa payment cards. This zero liability policy covers the use of all Visa consumer card products -- including debit and credit cards. As a result of this new policy, a consumer will not be held liable for unauthorized use of any Visa consumer payment card.

This zero liability policy applies to online transactions as well as offline transactions. Customers are protected online in exactly the same way as when they are using their cards at a store, ordering from a catalog by mail, or placing an order over the phone. In case of a problem, Visa provides 100 percent protection against unauthorized card use, theft, or loss. If someone steals a payment card number from one of our cardholders

while the cardholder is shopping, online or offline, our customers are fully protected -- they pay nothing for the thief's fraudulent activity. We took this step in part to make sure that our cardholders know that it is safe to shop online, despite all of the recent attention to Internet security. Although card fraud numbers are very small, Visa's zero liability policy takes away risk of unauthorized use that cardholders face shopping online.

FRAUD CONTROL PROGRAMS

One type of fraud occurs when someone uses a cardholder's account number to engage in an unauthorized transaction online. For example, a person may steal a consumer's credit card number and use it to order merchandise online. The theft might occur in a variety of ways -- for example, by breaking into a merchant's database that contains consumer account numbers, or by intercepting a consumer's credit card billing statement sent to the consumer's home.

It is important to keep in mind that account information can be stolen offline, and then used to engage in an unauthorized transaction online. The fact that unauthorized transactions take place on the Internet does not mean that the Internet itself is a risky place for consumers to shop. If the thief has obtained a card account number, but does not actually have the card, it is only natural for him to use this account information in a channel of commerce, such as the Internet or mail order and telephone order, in which the card does not have to be present in order for the transaction to take place. For this reason, mail order and telephone order and Internet transactions show a higher incidence of unauthorized use. The fraud rate for all Visa transactions is about 0.07 percent. For card-not-present transactions it is 0.15 percent. This, of course, does not mean that it is more risky for consumers to use these channels of commerce. It simply means that those who gain unauthorized access to card information are more likely to try to use that information to engage in fraud in a card-not-present environment.

It is in the interests of Visa, consumers, merchants, and Visa's members to prevent fraud.

Fraud prevention protects merchants from absorbing the costs of fraud and protects consumers from the higher prices that they would have to pay in order to cover fraud losses. Fraud prevention further protects consumers from the trouble of having to exercise their rights in connection with unauthorized transactions. For these and other reasons, preventing fraud involving Visa credit and debit cards is a top priority for Visa and its members. Fraud prevention also is essential to protecting the integrity of the Visa brand and maintaining the confidence of consumers and merchants that use the Visa system. Through significant investments in technology, cooperative efforts between Visa, its members, and law enforcement agencies, and a wide variety of educational initiatives, the incidence of Visa-system fraud in recent years is at an all-time low, even as the volume of Visa card transactions has grown dramatically.

Visa and its member financial institutions have developed a varied arsenal of fraud control programs that help merchants reduce the incidence of unauthorized use of Visa

payment cards. These programs are especially important in addressing fraud in a card-not-present environment like the Internet. These include the Address Verification Service, Cardholder Risk Identification Service, an Exception File, Card Verification Value, and a new pilot program for Payer Authentication.

- The Address Verification Service is a fraud prevention system that allows merchants to verify automatically that a shipping address provided by a cardholder at the time of purchase matches the cardholder's billing address and other information. This service helps merchants minimize the risk that they will accept fraudulent orders from persons using stolen cardholder information.

- Visa's Cardholder Risk Identification Service ("CRIS") is a transaction scoring and reporting service that employs advanced neural network technologies to develop artificial intelligence risk scoring models that help identify fraudulent transaction patterns. Issuers can use CRIS as a stand-alone fraud detection system or together with their own internal fraud detection methods.

- Visa's Exception File is a worldwide database of account numbers of lost/stolen cards or other cards that issuers have designated for confiscation, referral to issuers, or other special handling. All transactions routed to Visa's processing system have their account numbers checked against the Exception File. - The Card Verification Value (CVV) is not printed on the card itself, but can be found on the card's signature strip on the back of the card. These codes help merchants confirm that cardholders are in possession of the actual card. Online merchants and other merchants in situations where the card is not present at the merchant's premises during the transaction can verify that their customers have the actual card in their possession by requesting the customer to provide the CVV from the signature strip.

- Visa's Payer Authentication service is currently a pilot program. This service will enable issuers to confirm a cardholder's identity to the merchant during the virtual (on-line) checkout process. This process will be accomplished using a password that the cardholder registers with his or her issuer. The process will help reduce fraud by enabling merchants to confirm the cardholder's identity at the time of purchase.

GUIDANCE FOR CONSUMERS SHOPPING ONLINE

Visa provides consumers with information on how to protect their cardholder information online. Visa's website, for example, provides an Internet Shopping Guide for consumers, with suggestions for how consumers can shop safely on the Internet. Some of these suggestions are:

Shop with merchants you know and trust and visit Better Business Bureau Online if you have questions about a particular merchant.

Look for signs of security. Symbols like an unbroken lock or key, a URL that begins https://, or the words Secure Sockets Layer (SSL) mean that no one but you and the merchant can view your payment information.

Never send payment information via e-mail. Information that travels over the Internet (like e-mail) is not fully protected from being read by outside parties. Shop with reputable merchant sites that use encryption technologies that will protect your private data from being read by others as you conduct an online transaction. When you pay online, make sure that you are using a secure browser.

- Make a point of reading a merchant's privacy policy to find out what type of information is captured and how it is used.

SECURITY REQUIREMENTS FOR CARDHOLDER DATA

Some consumers express concern that the account information they provide to merchants during online transactions might be subject to unauthorized access after the transaction is complete. The account information might be transmitted to web merchants in a secure fashion, but not maintained securely in the web merchant's database. Reports of intrusion by hackers into web merchant databases have increased this concern. It should be noted, however, that the security of merchant databases of account numbers is not related to whether a transaction is conducted over the Internet, rather it is related to the accessibility of the database from the Internet.

To address this concern about unauthorized access to merchant databases, Visa has developed new security requirements for cardholder data. These requirements apply to any entity holding card data -- including web merchants, gateways and Internet service providers. These requirements prescribe how these companies should store, encrypt and grant access to cardholder data. For example, they require Internet merchants to install firewalls, to keep security systems up- to-date, to encrypt stored data, and to use anti-virus software, among other things. These requirements became effective May 1,2001.

Visa offers assistance to Internet merchants that accept Visa cards in meeting these requirements for safeguarding their customers' payment card data. We provide merchants with training sessions, interactive reviews, compliance and monitoring consultation and information on third-party firms specializing in testing and compliance.

The new program requires the top 100 e-commerce merchants -- who account for 70 percent of Internet commerce in the Visa system -- to have their online security procedures validated by an outside accounting or Internet security firm. Other online retailers will be subject to random security reviews by Visa.

The twelve requirements of the new security program are:.

1. Install and maintain a working network firewall to protect data accessible via the Internet.

2. Keep security patches up-to-date.

3. Encrypt stored data.

4. Encrypt data sent across open networks.

5. Use and regularly update anti-virus software.

6. Restrict access to data by business "need-to-know."

7. Assign a unique ID to each person with computer access to data.

8. Do not use vendor-supplied defaults for system passwords and other security parameters.

9. Track access to data by a unique ID.

10. Regularly test security systems and processes.

11. Maintain a policy that addresses information security for employees and contractors. 12. Restrict physical access to cardholder information.

DISPUTE RESOLUTION

Visa has an effective way of resolving consumer disputes with online merchants through our chargeback system. Chargebacks are contractual ways of resolving transaction disputes involving payment cards between the Visa banks that serve cardholders (the issuers) and the Visa banks that serve merchants (the acquirers). the issuer to the acquirer.

A chargeback is the return of a transaction from Our chargeback system can resolve transaction disputes, even if the merchant and the consumer are geographically dispersed. As a result, Visa's chargeback process provides practical and effective consumer protections for electronic commerce transactions.

Most chargebacks in the Visa system are for housekeeping reasons. In a system that handles 25.5 billion transactions a year, mistakes are bound to occur. These can include double billing, no billing, incorrectly entered amounts, failure to provide requested copies of transactions, mismatches among accounts and so forth. These errors constitute the vast majority of chargebacks.

In addition to these housekeeping chargebacks, there are chargebacks involving consumer complaints. The three most common categories of Internet consumer complaints handled in our chargeback system can be described by the phrases: "I didn't do it," "I didn't get it" and "I don't want it." Visa rules with respect to these complaints are designed to protect cardholders. Cardholders do not have to pay if they did not make the purchase, if they did not get what they ordered or if it was not what they ordered.

The "I didn't do it" dispute relates to situations where the cardholder claims that the transaction was processed without the cardholder's permission. This is the most common category of Internet disputes. It covers fraud, but it also covers situations where the cardholder does not recognize the charge as it appears on the monthly bill. Confusion often can arise when the merchant uses a different billing name or address than the expected trade name. About 50-60 percent of these disputes are resolved by giving the cardholder additional information about the charge.

The "I didn't get it" category of consumer complaint covers untimely receipt or non-receipt for goods. This dispute involves situations where a cardholder claims that he or

she did not receive ordered merchandise at the agreed-upon location or by the agreed delivery date. An issuer can charge back a transaction on the cardholder's behalf if the cardholder sends a letter to the issuer supporting his or her claim. Proof of shipment by the merchant is irrelevant; the Visa member acquiring the transaction can only counter the chargeback on the merchant's behalf by providing proof of delivery, signed by the cardholder or another authorized person.

The "I don't want it" category of Internet disputes includes "quality" disputes, such as when merchandise is received broken, not as ordered (e.g., wrong color or size) or not as described. It is the most difficult type of dispute to deal with because value judgments are involved.

Only a tiny percentage of all Visa transactions are charged back, about 0.07 percent or 7 for every 10,000 transactions. Chargebacks for Internet transactions also are a small portion of all Internet transactions. Even though chargebacks are rare occurrences, they are more common for Internet transactions than for other types of transactions. However, it is difficult for us to say how much more common. Merchants are supposed to report their Internet transactions to the Visa system using an E-commerce code. Not every merchant that operates both in the Internet and the 'real' world -- the so-called 'bricks and clicks' merchants -- report and break down their sales by channel. So the statistics available are not as comprehensive as we would like. That being said, the Visa chargeback rate for Internet transactions is estimated to be about 0.5 percent. Put another way, only about 50 out of every 10,000 electronic commerce transactions are charged back.

There are a number of reasons for this. The Internet is a new channel, much the way mail order and telephone order transactions were new a decade ago. Not all merchants have developed the back office and customer service facilities that consumers have come to expect, and those consumers use the Visa chargeback system to help them resolve their problems with merchants.

In addition, the Internet is a channel of commerce, in which, like mail order and telephone order, the card is not presented to the merchant when the transaction takes place. This naturally creates greater opportunity for unauthorized use of card account information. In this regard it is useful to note that chargebacks for mail order and telephone order transactions are 0.39 percent, or 39 per 10,000 transactions. The fact that there is greater use of chargebacks for payment cards used on the Internet or through mail order or telephone order does not mean that these channels of commerce are inherently more risky for consumers.

Other factors contribute to the higher chargeback rate for Internet transactions. Cardholders are doing business with unfamiliar merchants, or with individuals at auction sites. In some cases, these merchants or individuals are unscrupulous. In other cases, cardholders deny valid charges. In addition, digital goods present some special difficulties. Some digital good subscriptions require the use of a payment card account number for access and this sometimes results in customer confusion on the nature of the

subscription terms and payments. Buying and delivering digital goods like software and music can be difficult on the Internet. For example, the Internet connection may be lost during long downloads. Or a cardholder might repeatedly hit the buy button on a site when the link does not respond quickly.

The Visa chargeback system operates in compliance with federal laws that provide a number of important consumer protections. The Truth in Lending Act, implemented through Regulation Z, gives cardholders various rights regarding billing error resolutions. And it allows the cardholder to assert claims and defenses against the card issuer. The Electronic Funds Transfer Act, implemented under Regulation E, applies to debit cards and also contains error resolution procedures. These legal protections apply to online transactions as well as to face-to- face transactions. These legal protections are just the start of the consumer's protection. There are more protections that are provided voluntarily by competing payment systems. And there can be even more protections provided within systems, bank-by-bank, to meet the needs of cardholders. The payment card business is intensely competitive, with all competitors seeking to gain the business and loyalty of cardholders. Banks are extremely interested in having satisfied customers, as are merchants. Each will do what they can to continue customer relationships. In fact, a joint venture system, like Visa, enhances competition generally because it provides for bank-to-bank competition as well as system competition.

Visa also works with cardholders, merchants, consumer groups and seal programs to avoid consumer disputes in the first place. One important relationship we have established is with the online subsidiary of the Better Business Bureau, BBB Online. BBB Online has developed a comprehensive Code of Online Business Practices and a first-rate Reliability Trustmark Program. The code outlines the responsibilities of online merchants in five key areas: truthful and accurate communications, disclosure of policies, information practices and security, customer satisfaction and protecting children. Their Reliability Trustmark Program is one of the most significant trustmark programs on the web, providing more than 8,800 websites with a seal to signify to potential customers the merchant's commitment to good customer practices. The seal provides consumers navigating the electronic marketplace with a reassuring sign from a well-regarded and well-known organization, the Better Business Bureau.

On November 14, 2000, Visa joined forces with BBB and agreed to promote its Code of Online Business Practices and its Reliability Trustmark Program. This includes a consumer advertising and a consumer education campaign. Many websites that provide excellent customer service and protections are not pan of the BBB Online program. But online consumers can be confident that online sites displaying the BBB Online reliability seal have the highest level of consumer protection.

Visa also maintains a chargeback-monitoring program. This program monitors a merchant's chargeback rate. If this rate exceeds certain levels, Visa asks the merchant's bank to ensure that the merchant takes steps to correct the problem. Usually, the problem is technical and is fixed immediately. In cases where the chargeback rate does not

decline, Visa has a process of assessing fines. A merchant that does not correct a persistent chargeback problem can ultimately be denied the right to accept Visa payment cards for goods and services.

PRIVACY PROTECTIONS

Visa has taken steps to ensure that privacy notices are provided by merchants who accept Visa payment cards to consumers who shop online. Violation of consumer privacy expectations on the Internet is simply bad business, and consumers are right to be upset about the unwanted dissemination of information about their online activities. To respond to privacy concerns, in October 2000, the Visa International Board adopted new consumer protection policies that set global disclosure standards for web merchants. The new policies require web merchants that accept Visa cards to display prominently on their websites the merchant's privacy policy and online security capabilities. These requirements become effective on June 1, 2001.

Merchant banks must update their merchant agreements to include these requirements no later than January 1, 2002. Banks may satisfy this requirement by mailing a disclosure addendum to each of their electronic commerce merchants. Many electronic commerce merchants already disclose this information. However, Visa and its member banks provide guidance to electronic commerce merchants that need assistance in meeting the privacy policy requirement. For instance, we encourage merchants to use the Privacy Policy Statement Generator developed by the Organization for Economic Co-operation and Development.

Visa also has taken other steps to help consumers protect their privacy online. Our website contains an extensive consumer guide to online privacy protection. In addition, we participate in pro-privacy industry organizations such as the Privacy Leadership Initiative, a group of major corporations and associations, dedicated to promoting privacy on the part of U.S. business and educating consumers about ways in which they can protect their privacy.

Finally, Visa has provided extensive legal and regulatory guidance to our member banks to ensure that the mandated online and offline privacy protections of the Financial Modernization Act of 1999 are fully implemented. Financial institutions must be in compliance with the privacy provisions of this law by July 1,2001. These rules generally require financial institutions to disclose their privacy policies at least annually and to provide their customers with the opportunity to opt-out of certain information sharing practices with third parties. These Federal privacy rules apply to information collected on websites in connection with providing a financial product or service. Financial services websites now must comply with notice and opt-out requirements.

Visa appreciates the opportunity to appear before you today. We believe that our payment system represents a reliable and secure means of conducting online transactions in which the rights of consumers are well protected. Visa will continue to adapt to new technologies and practices. Combating fraud and maintaining information security are top

priorities of Visa and its member financial institutions. I will be happy to answer any questions that you may have.

END

LOAD-DATE: May 24, 2001

Federal Document Clearing House Congressional Testimony

November 1, 2001, Thursday

SECTION: CAPITOL HILL HEARING TESTIMONY

LENGTH: 2241 words

COMMITTEE: HOUSE FINANCIAL SERVICES

SUBCOMMITTEE: FINANCIAL INSTITUTIONS AND CONSUMER CREDIT

HEADLINE: IMPACT OF CREDIT POLICIES ON CONSUMERS

BILL-NO: H.R. 61 Retrieve Bill Tracking Report
Retrieve Full Text of Bill

TESTIMONY-BY: JOSHUA L. PEIREZ, SENIOR LEGISLATIVE AND REGULATORY COUNSEL

AFFILIATION: MASTERCARD INTERNATIONAL INCORPORATED

BODY:

WRITTEN STATEMENT OF

JOSHUA L. PEIREZ SENIOR LEGISLATIVE AND REGULATORY COUNSEL MASTERCARD INTERNATIONAL INCORPORATED

HEARING BEFORE THE SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT OF THE COMMITTEE ON FINANCIAL SERVICES

UNITED STATES HOUSE OF REPRESENTATIVES

NOVEMBER 1, 2001

Chairman Bachus, Congresswoman Waters, and members of the Subcommittee, my name is Joshua Peirez. I am the Senior Legislative and Regulatory Counsel for MasterCard International Incorporated ("MasterCard"). MasterCard is a global membership organization comprised of over 22,000 financial institutions that are licensed to use the MasterCard service marks in connection with a variety of payments systems. MasterCard and its members have always provided, and are fully committed to providing,

extensive consumer benefits and the highest quality of consumer services. I thank the Subcommittee for taking the time to consider these issues and for the opportunity to discuss how MasterCard and its members serve and benefit MasterCard cardholders.

Benefits of MasterCard

MasterCard payment cards are enormously beneficial methods of payment for consumers and merchants alike. An individual carrying a MasterCard payment card knows that he or she can walk into an establishment almost anywhere in the world and make a purchase using his or her MasterCard card. In fact, MasterCard cardholders can transact in more than 150 currencies without the need to exchange large amounts of cash. A MasterCard cardholder can virtually travel the world with only a single piece of plastic about 31/2" by 2" large and make payments without the need to carry large amounts of cash or travelers checks. A MasterCard cardholder can also buy everything from groceries to doctors' services on a MasterCard card. Our popular advertising campaign says it best: "there are some things money can't buy for everything else, there's MasterCard." In essence, the MasterCard system is an integral part of the globalization that has fueled our economy over the last thirty years.

MasterCard cardholders can use a MasterCard payment card at millions of merchants. That means fewer trips to the bank, or ATM, and no longer having to worry about carrying the right amount of cash, losing it, or having it stolen. MasterCard cardholders also receive a convenient, detailed accounting of their spending through periodic statements provided by their card issuers. Many times, cardholders obtain what is essentially an interest-free loan for some period of time.

Further, a MasterCard cardholder need not even leave the comfort of his or her own home to shop the globe. The Internet has become a powerful tool for consumers to shop for the lowest prices on a myriad of products. This rapid development of e-commerce is due in large part to a cardholder's ability to pay for a product on- line by using a payment card. It is no overstatement to claim that the Internet would not be such a critical part of our economy today if it were not for the widespread use and acceptance of payment cards. Furthermore, MasterCard is developing, and intends to continue to develop, new and innovative payment options and features related to Internet purchases.

It is also important to note that MasterCard payment cards are valued not just by consumers. Approximately 22 million merchants worldwide have decided to accept MasterCard payment cards to improve business. The guarantee of payment from the MasterCard system is the cornerstone of the MasterCard merchant proposition. A merchant accepting a MasterCard payment card knows that he or she will be paid for goods or services. The merchant typically does not have that protection in accepting a check since the check may bounce. Indeed, the majority of merchants do not even accept checks from outside their local area.

In addition, acceptance of MasterCard cards can be more convenient, cheaper, and safer than other available forms of payment. As an example, merchants need not worry

about cash being stolen (by employees or outsiders) and need not worry about physically depositing funds or checks as MasterCard cards allow merchants to deposit funds into their accounts electronically. Naturally, the acceptance of MasterCard payment cards (along with other payment forms) also allows merchants to give their customers a variety of payment options, which enhances overall customer satisfaction and, importantly, increases sales. It is the increased sales, decreased costs, and enhanced customer satisfaction that has led so many businesses to choose to accept MasterCard cards.

MasterCard has also created a great deal of choice through the vigorous competition with other payments systems and forms of payment as well as among the thousands of MasterCard member financial institutions. Indeed, through the innovation of MasterCard and its members, consumers have thousands of card programs from which to choose. For example, MasterCard cards can be credit cards, debit cards, secured cards, cobranded or affinity cards, or prepaid cards, among many others. This allows consumers to choose great rewards programs, to donate portions of proceeds to favorite charities, and to enjoy attractive interest rates, among many other options.

With all these card programs, the consumers receive the tremendous benefit of universal acceptance, i.e., the knowledge that their cards will be accepted at any of the merchants that accept MasterCard worldwide, regardless of which MasterCard member issued the card, and regardless of the underlying terms of such issuance. Whether the card is a credit card, a prepaid card, a debit card, a platinum card or a secured card, whether the card has a $20,000 or a $200 credit line, whether the card offers frequent flier miles or not, the consumer knows that it will be accepted. This, in and of itself, illustrates the fabulous proposition that is MasterCard, but there is much more that MasterCard has done to increase the security and therefore the consumer benefits of MasterCard cards, as described below. Consumer Protections

MasterCard is also pleased to offer its cardholders outstanding consumer protection benefits. In fact, we believe that our cardholder protections are extremely valuable as they provide consumers with the security and comfort necessary to make the MasterCard system "the best way to pay for everything that matters." For example, MasterCard has voluntarily implemented a "zero liability" policy for the unauthorized use of MasterCard consumer cards issued in the United States. It is important to note that MasterCard's policy with respect to zero liability is superior to what is required by law. Specifically, the Truth In Lending Act imposes a $50 liability limit for the unauthorized use of credit cards. Under the Electronic Fund Transfer Act, a cardholder's liability for unauthorized use of a debit card can be higher. However, MasterCard provides all U.S. MasterCard consumer cardholders, regardless of the particular card type, with even more protection. Under MasterCard rules, a cardholder victimized by unauthorized use generally will not be liable for any losses at all. This has greatly enhanced consumer confidence, including with respect to shopping on-line. Although many Internet merchants have taken care to provide consumers with a secure transaction environment, MasterCard cardholders can shop on-line with the confidence that they will have no liability in the unlikely event that their account number is misused.

Cardholders who use MasterCard cards also gain additional protections against merchants who do not perform as expected. In many instances, if a cardholder uses his or her MasterCard card to pay for a product or service, and the merchant does not provide the product or service as promised, the issuer can "chargeback" the transaction and thereby afford its cardholder a refund.

This is a valuable consumer protection that is obviously not available with other forms of payment such as cash, checks, or travelers checks.

Customer Satisfaction

Consumer feedback also demonstrates the high quality of the services the payments industry provides to consumers. MasterCard is pleased to note that a recent survey by Thomas A. Durkin, of the Federal Reserve Board's Division of Research and Statistics, published in the Federal Reserve Bulletin indicates that consumers are extremely satisfied with their payment cards. For example, 91% of consumers who have a bank-issued payment card are "generally satisfied in [their] dealings with [their] card companies" and 92% believe "card companies provide a useful service to consumers." The survey also found that 90% of bankcard holders agree with the statement that "my credit card companies treat me fairly." Durkin also noted that, to the extent the survey revealed some negative opinions with respect to payment cards, any "negativity may have arisen in part from an individual's perceptions of other consumers' difficulties rather than from the individual's own experiences. . .it seems likely that as card use has become more common, negative opinions about card use may [be] a result of perceptions about 'the other guy.' Views about personal experiences with [] cards, in contrast, are much more positive." (emphasis in original)

How many other major industries can claim a customer satisfaction rate of 90%?
Financial Education

MasterCard firmly believes that financial literacy is critical for individuals of all ages. With this in mind, MasterCard has developed numerous important consumer financial education programs and continues to work with Congress and the Administration on additional efforts to improve consumer financial awareness. The following are just some of MasterCard's consumer education programs:

- "Are You Credit Wise?" With the support of national student leaders, MasterCard developed a campus-based education program providing money management information to college students.

- Creditalk.com. Creditalk.com is an interactive financial education web site created and operated by MasterCard. The site offers a variety of money management information for new and experienced credit consumers such as: obtaining and understanding a credit report; establishing and managing a budget; dealing with a debt crisis; and calculating when outstanding balances will be paid off using an on-line credit calculator. And because web- based initiatives must stay current and fresh, MasterCard is now investing in redesigning and relaunching this site so that it is even more helpful for consumers.

- “Kids, Cash, Plastic, and You.” This is a highly successful consumer education magazine developed with the former U.S. Office of Consumer Affairs. The magazine provides tips to help parents teach children about money management and outlines a “parent coach” approach for achieving this goal.

- League of United Latin American Citizens (LULAC). Through its partnership with LULAC, MasterCard has developed “The Art of Building a Financial Future” that is helping Latino leaders conduct financial management workshops in communities across the United States.

- “Master Your Future.” The “Master Your Future” program materials consist of a video and curriculum guide for high school teachers that can be integrated into their lesson plans. More than 23 million students have had the opportunity to develop positive personal finance habits as necessary life skills through this program.

- “Money Talks.” A collaboration between MasterCard and College Parents of America, the Money Talks brochure provides advice to parents on how to talk to their college-aged students about personal finances.

MasterCard is also active in Washington with respect to efforts to improve our nation’s financial literacy. For example, MasterCard is a strong supporter of H.R. 61, the “Youth Financial Education Act” introduced by Representatives David Dreier and Earl Pomeroy. The Dreier-Pomeroy legislation would authorize the Secretary of Education to provide grants to state educational agencies to develop and integrate youth financial education programs for students in elementary and secondary schools. We are pleased that the House and Senate have each incorporated this bill in the larger education reform measure that currently awaits final action in conference.

MasterCard has also been working with the current Administration to develop approaches to increasing financial literacy. We were pleased to see that Secretary O’Neill had been scheduled to testify in the Senate to highlight the Administration’s efforts in this area. Unfortunately, the hearing had been scheduled for shortly after the terrorist attacks and has not yet been rescheduled. MasterCard looks forward to resuming our progress on this matter at the appropriate time.

Conclusion

MasterCard is proud of its, and its members’, record of offering cardholders and merchants a highly beneficial and convenient payment method with superior protections. MasterCard is also proud of its efforts in the private and public sectors to improve financial literacy for Americans of all ages. Quite simply, we have set high standards, and, as always, we will strive to meet them.

Mr. Chairman, thank you again for the opportunity to discuss MasterCard’s commitment to its cardholders. I would be pleased to address any questions the Subcommittee may have.

LOAD-DATE: November 16, 2001

Federal Document Clearing House Congressional Testimony

September 24, 1997, Wednesday

SECTION: CAPITOL HILL HEARING TESTIMONY

LENGTH: 3143 words

HEADLINE: TESTIMONY September 24, 1997 LAURENCE H. MEYER MEMBER, BORAD OF GOVERNORS FEDERAL RESERVE SYSTEM HOUSE BANKING FINANCIAL INSTITUTIONS AND CONSUMER CREDIT DEBIT CARDS

BODY:

For Release Delivery
10:00 a.m. EDT
September 24, 1997
Statement by
Laurence H. Meyer
Member, Board of Governors of the Federal Reserve System
before the
Subcommittee on Financial Institutions and Consumer Credit
of the
Committee on Banking and Financial Services
U.S. House of Representatives
Washington, DC
September 24, 1997

The Board of Governors appreciates this opportunity to comment on issues concerning debit cards that can be used without security codes (sometimes referred to as "check cards" or "offline" debit cards). Users of these cards have some consumer protections related to liability, issuance, and disclosure under the Electronic Fund Transfer Act (EFTA) and the Board's Regulation E. A bill introduced by Representatives Schumer and Gonzalez, and another by Representative Barrett, would further limit a consumer's potential liability for the unauthorized use of debit cards and place restrictions on their issuance. The Board's testimony discusses the existing statutory and

regulatory scheme concerning debit card liability and issuance and provides comment on the legislative proposals. The testimony also provides comment on issues related to unsolicited "loan checks," which are addressed in proposed legislation introduced by Representatives Hinchey and Gonzalez that would amend the Truth in Lending Act (TILA).

Generally speaking, the oldest type of debit card in the United States is the automated teller machine (ATM) card used by consumers to make deposits, withdrawals, and transfers between deposit accounts. The cards require the use of a magnetic stripe reader (built into the ATM) and the consumer's security code -- a personal identification number (PIN). Because of the method of operation, these cards are sometimes characterized as "online" debit cards. That is, at the time of the transaction, the account number, PIN, and account balance are verified; and instructions for the funds transfer are communicated, through the ATM network, to a database at the card-issuing institution.

At first, institutions issued cards that could be used only at their own ATMs. Over time, the development of regional, nationwide, and internationally linked networks has enabled consumers to access funds using ATMs at institutions other than their own. The subsequent linking of electronic point-of-sale (POS) terminals to these networks has allowed consumers to use their debit cards to pay for purchases at supermarkets, gas stations, and other sites by debiting their deposit accounts. At merchant locations requiring the use of a PIN, the cards operate as "online" debit cards. The use of PIN-protected cards in these online systems has increased substantially in the United States over the past several years, while until recently the use of "offline" debit cards has remained more limited.

Some financial institutions began issuing "offline" debit cards more than a decade ago. Consumers have used these cards in place of credit cards at retail locations. Typically, the consumer signs a charge slip, rather than entering a PIN, and the transactions are processed much like credit card transactions. Indeed, early on, this largely "paper-based" mode of operation generated questions about whether these card transactions were covered by the EFTA and Regulation E. As a consequence, the Board amended Regulation E in 1984 to make clear that debit card transactions are covered by the regulation, whether the transaction takes place at a terminal that captures the transaction data electronically, or is carried out manually and only later converted to electronic form.

Over the past year or so, card issuers have begun marketing offline debit cards aggressively, encouraging consumers to use them in place of writing checks. Besides just making them available, many institutions have automatically replaced their customers' existing ATM cards, previously usable only with PINs, with cards that can be used with a PIN at ATMs and electronic POS terminals, and without a PIN in the "offline" mode. This development has raised concerns about the potentially greater consumer exposure to losses in the absence of PIN protection.

Both the TILA and the EFTA -- which govern credit cards and debit cards, respectively -- contain provisions on unauthorized use and unsolicited issuance. The TILA provisions were enacted in 1970, and the EFTA provisions have been part of the act since it became law in 1978. The TILA limits consumer liability for the unauthorized use of a credit card to $50. Under the EFTA, the rules are more complex. Liability for the unauthorized use of a debit card is determined based on when the consumer notifies the financial institution of a lost or stolen card or an unauthorized transaction.

If notice is provided within two business days of learning of the loss, the consumer's liability is limited to $50. For the consumer who fails to report the loss or theft of a debit card within two business days of learning of the loss or theft, the potential liability increases to $500. This higher limit applies to unauthorized transactions taking place after the two business-day period. For example, if a $600 unauthorized debit-card purchase takes place the same day the card is stolen, the consumer's maximum liability for that transaction is $50 even if the consumer fails to give notice within two business days after learning of the theft. If unauthorized transactions appear on the consumer's account statement and the consumer fails to report them within 60 days after the statement is sent, the consumer's potential liability is unlimited for unauthorized transactions occurring after the 60 days. Liability up to the 60th day is capped at $50 (or at $500, if the consumer knew about a debit card loss or theft and failed to report it within two business days).

The explanation for the more complex rules in the EFTA can be gleaned from the history of the act, which followed a study completed in 1977 by the National Commission on Electronic Fund Transfers. The Commission's report on emerging EFT payment mechanisms, which responded to a Congressional directive, recommended legislative action to foster the orderly development of EFT systems. At that time, the banking industry had raised objections to having a $50 cap on consumer liability for debit cards, the same as for credit cards. Industry representatives urged that a negligence standard should apply if the consumer was negligent in handling the card and PIN. The industry believed that a $50 cap was an insufficient incentive for consumers to protect their cards and security codes. In turn, the Commission's report recommended a negligence standard that would hold the consumer liable for acts such as writing the PIN on the card.

The Congress considered and ultimately decided against imposing a negligence standard. Instead, both the House and Senate agreed on the basic $50 liability limit. But in addition, to encourage consumers to protect debit cards and promptly report unauthorized use, the House favored holding a consumer liable for unauthorized transactions occurring a "reasonable time" after the consumer learned of the loss or theft of the card and failed to notify the card issuer. The Senate bill provided for unlimited liability for the failure to report any unauthorized transactions appearing on a statement within 60 days after the statement was sent. The law as finally enacted blended the two exceptions, changing "reasonable time" to two business days and adding the $500 cap for unauthorized transactions taking place within the 60 days.

As to disclosures, both the TILA and the EFTA require that, to impose liability, the card issuer disclose the limits on consumer liability and give a telephone number or address (both phone number and address, in the case of the EFTA) for reporting loss or theft of the card or unauthorized transactions.

For issuance, the TILA prohibits outright the unsolicited issuance of credit cards. The EFTA permits the unsolicited issuance of debit cards, but only if disclosures are given and the card is not usable until after the consumer has requested validation and the consumer's identity has been verified. Both laws permit issuing a new card to replace or substitute for an existing card. Regulation Z (which implements the TILA) and Regulation E also permit an issuer to add features to a card at the time of substitution. Under these rules, it is thus permissible to send a debit card that can be used without PIN protection to replace an "online" PIN-protected debit card, and these substitute cards can be sent validated or unvalidated. When a substitution is made, if there are adverse changes in the terms and conditions that were originally disclosed to the cardholder (such as higher liability limits or higher fees), the issuer must disclose the revised terms. But adding the capability for offline use to a debit card does not, by itself, require a new disclosure under Regulation E.

Without doubt, the issuance of a card that does not require a PIN increases the consumer's risk. The consumer deserves to be informed about this in a very straightforward way. This risk may involve liability for unauthorized transactions or it may simply be the necessity of having to sort out unauthorized activity problems, even if there is no ultimate financial loss. It also seems appropriate to apply a lower liability limit than that which presently applies: under current law, adding non-PIN- protected capability to a card subjects the consumer to higher liability than applies to credit cards. Apart from what the law requires, both VISA and MasterCard have decided to voluntarily limit consumer liability for unauthorized use of debit cards to $50 or less, and this should deal with consumer concern about unwarranted financial risk, although the potential aggravation of demonstrating unauthorized use may remain. Therefore, it seems to us the question is whether voluntary industry activity is sufficient to deal with these concerns, or whether legislation is necessary.

Now, let me turn to the two proposed bills. H.R. 2319, the Consumer Debit Card Protection Act, introduced by Representative Barrett, limits consumer liability to $50 or less for all unauthorized debit card transactions, including those that require a PIN. The bill also calls for a warning notice for debit cards that can be used without a PIN, and would give consumers the option to reject such cards in favor of PIN-protected cards. Each periodic statement would have to include a detailed notice of the procedures for notifying the card issuer of the loss or theft of the debit card, or of unauthorized transactions.

For cards without PIN protection, the Barrett bill would also require the card issuer to provisionally reimburse consumers for claims of unauthorized use within three business days. Currently, the EFTA provides that claims of unauthorized use must be resolved

within 10 business days; alternatively, the disputed amount must be recredited within 10 business days if an investigation cannot be completed within that time, and the investigation must then be completed within 45 days. For POS and foreign transactions, Regulation E doubles the time periods: 20 business days to resolve a claim of error (or to recredit an account if the investigation takes longer); and 90 days to complete the investigation. The longer periods were adopted in 1984, at the same time that Regulation E was amended to cover paper-based debit card transactions. The longer times were deemed necessary for resolving claims that involved third-party merchants or remote institutions, and card issuers wanted to avoid having to provisionally recredit an account before the investigation was complete. The Board is aware that VISA is changing its rules to provide for recrediting within 5 business days, and this suggests that technological improvements in payment systems may permit these consumer claims to be investigated more quickly. We will reexamine the Board's rule in light of these developments.

H.R. 2234, the Dual-Use Debit Cardholder Protection Act, introduced by Representatives Schumer and Gonzalez, addresses liability, disclosures, and issuance. The bill limits a consumer's liability to $50 for a debit card that is not PIN- protected and does not use some other unique identifier; a signature is deemed not to be a unique identifier. It requires card issuers, as a condition of imposing any liability on consumers, to disclose the importance of promptly reporting loss or theft of the card. Under current law, this disclosure is optional. The Schumer-Gonzalez bill also prohibits issuing a debit card that can function without a PIN unless (1) the card is not activated when sent, (2) certain disclosures accompany the card, and (3) the card is activated only upon the consumer's request and after verification of the consumer's identity. These latter rules currently govern the initial issuance of a card on an unsolicited basis, but not a replacement card.

There is considerable merit to having card issuers provide a new offline debit card in unvalidated form when they replace an online card, and only validating the card upon the consumer's request. Requiring validation could be useful for assuring that consumers are not exposed to any additional risk or inconvenience without their consent. It is our understanding that in many cases card issuers already follow, or are planning to adopt, a security procedure in which they validate a renewal card for use only after the cardholder has expressly confirmed receiving the card and has requested validation. However, this procedure may not generally include the step of confirming the consumer's willingness to accept a debit card that is not PIN-protected.

The question is whether current and evolving industry practices are sufficient, or whether a statutory requirement is needed. Given the positive steps being taken by the industry to deal with consumer concerns on a voluntary basis, we are inclined to see how things work before enacting new laws. However, the industry should be on notice that it is in everyone's best interest to assure that the public understands the new risks inherent in transactions that are not PIN-protected, and that individual consumers can make an informed choice about whether to assume that risk.

The Subcommittee also requested information about the tracking of a consumer's debit and credit card spending. Although both regulations -- E for debit cards, and Z for credit cards -- require card issuers to capture transaction information such as transaction date, amount, and merchant name and location, for reporting to the cardholder on the periodic statement, they are silent on the use of this information by the card issuer. However, I think we all know, from our own experience, that for credit cards, and probably also for debit cards, at least some card issuers do use this and other information about cardholders' purchasing patterns for marketing purposes. Industry witnesses can no doubt provide detailed information on this matter.

The Board also has been asked to comment on the mailing of unsolicited "loan checks" to consumers. These credit products are also referred to as "loans by mail" or "live checks." The consumer need only sign and cash or deposit the check to obtain the loan. The amount of these loan checks may be thousands of dollars.

Federal law does not prohibit creditors from mailing unsolicited loan checks. The TILA does mandate that full disclosure of the credit terms, such as the annual percentage rate and the payment schedule, be included with any mailing so that consumers can make informed decisions about whether to accept the loan. Therefore, the primary concern should not be disclosure, but rather the potential for theft and fraud and the consumer inconvenience of refuting a claim of liability. The unsolicited check could be intercepted in the mail by a thief who forges the consumer's and cashes the check. The consumer's rights in the thief who forges the consumer's rights in the case of a forged endorsement are governed by state law, generally under the Uniform Commercial Code, which provides protection against fraud. Although the consumer would not ultimately be liable for the forged instrument, the consumer is nevertheless exposed to risk that was not anticipated and inconvenience resulting from a loan check that was not requested.

H.R. 2053, the Unsolicited Loan Consumer Protection Act, introduced by Representatives Hinchey and Gonzalez, prohibits the unsolicited mailing of loan checks or other negotiable instruments. The bill also provides that if a check or other negotiable instrument is sent unsolicited, a consumer would not be liable for the debt unless the creditor could prove that the consumer received and negotiated the instrument. And whether or not the intended recipient received it, the creditor could not report any liability resulting from the unsolicited instrument to a consumer reporting agency.

Within the past two years, the Board has received a dozen or so complaints about unsolicited loan checks that primarily relate to theft and fraud problems. This is not a vast number of complaints, and the issuance of unsolicited loan checks is not as prevalent as the issuance of unsolicited credit cards in the late 1960s that led to the TILA prohibition. But creditors are increasingly making use of these checks, and the question is whether they pose a significant enough problem to warrant legislation. In answering the question, it seems appropriate to balance any need for consumer protection to combat fraud and other concerns associated with unsolicited checks against unnecessary restrictions on the offering of financial products. Some consumers may appreciate the convenience of

obtaining “instant credit” without having to make a formal application. In addition, the intended recipient of a loan check generally will not be held liable for the amount of a forged loan check, although that may be small comfort to an individual who must contend with proving the forgery of the check. While the Board is mindful of the appearance that consumers are exposed to risks they have not voluntarily assumed, we do not favor an outright prohibition against sending these checks. Absent some evidence of a significant problem, we are inclined to let the market work without the intervention of new legislation.

This hearing provides a useful forum for the industry, consumer representatives, and others to discuss with lawmakers these important policy matters involving debit cards and loan checks, and we appreciate the opportunity to participate in the discussion.

LOAD-DATE: September 25, 1997

COMPARISON OF DISPUTE RESOLUTION PROCEDURES IN REGULATION Z AND REGULATION E

	Regulation Z	Regulation E
Consumer Requirements	Consumer must notify creditor within 60 days.	Consumer must notify financial institution within 60 days.
Timing of Investigation	Investigation must be completed within 90 days.	Investigation must be completed within 10 days. If it cannot be completed in this time, financial institution must issue a provisional credit any may investigate for an additional 35 days.
Treatment of Disputed Transaction During Investigation	Creditor may not seek to collect funds or issue a negative report.	There is no analogous provision, but financial institution must provisionally credit the consumer's account if it cannot complete the investigation within 10 days.
Results of the Investigation	Creditor must correct the error (if any) within 90 days. If there is no error, the creditor must issue a written explanation.	In many cases, financial institution must correct the error (if any) within 45 days. If there is no error, the financial institution must issue a written explanation.