



Russell W. Schrader
Vice President and Senior Counsel

March 11, 1998

VIA MESSENGER

United States Sentencing Commission
One Columbus Circle, N.E.
Suite 2-500
Washington, DC 20002-8002
Attn: Public Information

Re: Notice of Proposed Amendments to Sentencing Guidelines,
Policy Statements And Commentary

VISA U.S.A. ("Visa")¹ is submitting this comment letter to the United States Sentencing Commission (the "Sentencing Commission") in response to its proposed amendments to the sentencing guidelines, policy statements and related commentary. The Sentencing Commission published its proposed amendments in the Federal Register (63 Fed. Reg. 602) on January 6, 1998, and these amendments are referred to in this comment letter as the "Proposed Amendments."

Visa is the largest consumer payments system in the United States and the world. Visa is made up of nearly 21,000 financial institution members from around the world that issue Visa brand cards. There are more than 580 million Visa cards held by consumers globally, which are accepted at more than 14 million merchant locations and 350,000 automated teller machines worldwide. Visa -- which provides transaction authorization, clearing and settlement, and risk management services to Visa financial institution members -- supports more than \$1 trillion in Visa-related payment transactions annually throughout the world. Visa's transactions volume in the United States is approximately \$470 billion per year.

Theft and fraud involving Visa credit and debit cards is a matter of critical importance to Visa, its financial institution members and their customers. Visa and its members have over the years expended substantial resources to develop, refine and

¹ Visa U.S.A. is a membership organization comprised of financial institutions licensed to use the Visa service marks in connection with payment systems.

implement a broad range of theft and fraud detection and avoidance programs. These programs are summarized in the attachment to this letter. As a result of these programs -- and close cooperation with law enforcement officials -- the ratio of Visa credit and debit card theft and fraud to card sales has been significantly reduced, even as the volume of card transactions has increased dramatically.

Visa recognizes, however, that these detection and avoidance programs can never completely eliminate credit and debit card fraud and theft. Indeed, notwithstanding these programs, last year Visa credit and debit card theft and fraud losses totaled approximately \$485 million.

As a result, Visa and its members have a strong interest in appropriate sentencing guidelines for criminals who are convicted of theft and fraud involving Visa credit and debit cards. Appropriate sentencing guidelines will result in a reduction in credit and debit card theft and fraud for a variety of reasons. They will help ensure that when criminals are caught, they are prosecuted. Without the prospect of sufficient jail time, prosecutors may be reluctant to pursue certain prosecutions. Moreover, once convicted, appropriate sentencing guidelines will ensure that the criminal is off the streets and unable to perpetrate new credit and debit card theft and fraud for a sufficient period of time. Repeat offenders, often working as part of sophisticated and organized criminal gangs, are common among credit and debit card criminals. Finally, appropriate sentencing guidelines will of course serve as a disincentive for those considering this type of crime.

Loss Computation And Loss Tables

In the Proposed Amendments, the Sentencing Commission requested public comment on the definition of "loss," and the weight that it should be given in the theft, fraud and tax guidelines. Visa supports the Sentencing Commission's proposal to provide similar penalties for thefts and frauds involving similar amounts of loss. From a credit and debit card perspective, we see no distinction between theft and fraud. Cards and card account numbers are illegally obtained by criminals through a variety of methods, including through theft (such as by stealing cards from the victim or from the mail) and through fraud (such as by fraudulently applying for and obtaining a card in the name of the victim). The loss caused by this fraud or theft is the same.

Visa also supports the Sentencing Commission's proposal to incorporate the "more than minimal planning" ("MMP") enhancement in the loss tables for both fraud and theft. Credit and debit card theft or fraud always requires more than minimal planning, as the criminal must obtain the card or card number without the victim's knowledge (to avoid the victim canceling the card), and then must misrepresent himself

(such as by forging the victim's signature at the merchant location) when using the card. Moreover, the more significant credit and debit card losses typically involve multiple cards, sometimes numbering in the hundreds or even thousands, that were illegally obtained or manufactured by sophisticated criminal enterprises.

Visa supports loss table option 2 proposed by the Sentencing Commission, which provides for higher offense levels, as compared to option 1, for theft and fraud of various amounts. For the reasons discussed above, Visa believes that these higher levels will result in a reduction in credit and debit card theft and fraud.

Special Rules for Credit Cards and Access Devices

The current commentary to the sentencing guidelines provides that, in cases involving stolen credit cards, the loss includes any unauthorized charges made with the stolen credit cards, but in no event less than \$100. Section 2B1.1, Commentary 4. Visa urges the Sentencing Commission to reconsider this rule that, where there have been no unauthorized charges on the stolen credit card, the loss for purposes of the sentencing guidelines is only \$100.

This \$100 rule means that criminals who are caught before they are able to use the credit card or cards they have stolen have a low score, even if they have stolen a significant number of credit cards. Prosecutors have been reluctant to expend their limited resources to prosecute these cases, since even if the prosecution is successful, the criminal would receive a lenient sentence. Even if the criminal is prosecuted and convicted, he or she will be back on the streets far too soon, and our experience has been that he or she often repeats the credit card fraud or theft or other criminal activity. This \$100 rule also undermines the deterrent effect of the credit card fraud and theft laws.

Finally, this \$100 rule does not adequately reflect the injury to the innocent victim. The mere fact that a credit card has been stolen can be quite traumatic for the victim, even if the credit card is never actually used by the criminal. At a minimum, the victim's life is disrupted until he or she obtains a replacement card from the card issuer. Criminals have used the stolen credit card as part of their scheme to take over the identity of the victim, and then use the victim's identity to run up substantial losses. Congress has examined the harm that results from these identity frauds to the innocent victims.² The stolen credit card can be the key to this identity fraud, even if the criminal never charges anything to the card.

² See for example, the September 16, 1997 hearing before the Subcommittee on Financial Services and Technology of the Senate Banking, Housing and Urban Affairs Committee.

Visa recommends that the Sentencing Commission revise this commentary to provide that the loss for a stolen credit card is considered to be the card's available credit line. Once the criminal has possession of the victim's credit card, the criminal has within his or her control access to the full amount of available credit on the card. As recognized by several courts,³ this approach would more accurately reflect the value of the card stolen by the criminal, as well as the potential loss to the victim. This approach also would be consistent with the treatment under the sentencing guidelines of a stolen check that is in the possession of the criminal, but has not yet been cashed. The sentencing guidelines provide that in these circumstances the appropriate amount of loss is the loss that would have occurred had the check been cashed. Section 2B1.1, Commentary 2 (Example 1).

As an alternative approach for stolen but unused credit cards, a graduated scale based on the number of victims could be used. For example, possession of five or more unused stolen credit cards could result in an automatic two level increase for sentencing purposes, with a larger number of unused stolen credit cards resulting in additional increases (for example, 20 or more unused stolen credit cards could result in a four level increase, 50 or more unused stolen credit cards could result in a six level increase and 100 or more unused stolen credit cards could result in an eight level increase). This approach, like the credit line approach recommended above, would impose greater penalties on the more systemic, organized criminal enterprises.

Visa strongly supports the proposed addition of the reference to "access devices" in this Commentary 4. We presume that this reference is designed to include debit cards and ATM cards, and recommend that the commentary be further clarified by referencing the definition of the term "access device" in Federal Reserve Board Regulation E (12 C.F.R. § 205), which the Federal Reserve Board has promulgated under the federal Electronic Fund Transfer Act (15 U.S.C. § 1693 *et seq.*).⁴

Debit cards are the fastest growing new consumer payment device in the history of Visa. In the United States, as of June 30, 1997, approximately 50 million Visa debit cards had been issued and transaction volume exceeded \$80 billion (on an annual basis). When a person uses a debit card to pay for goods or services, funds are deducted from his or her checking account at the bank issuing the card (in contrast, with a credit

³ See U.S. v. Sowels, 998 F.2d (5th Cir. 1993); U.S. v. Egemony, 62 F.3d 425 (1st Cir. 1995); U.S. v. Ismoila, 100 F.3d 380 (5th Cir. 1996).

⁴ Regulation E defines the term "access device" as a "card, code, or other means of access to a consumer's account, or any combination thereof, that may be used by the consumer to initiate electronic funds transfers." 12 C.F.R. § 205.2(a)(1). This definition includes all types of debit cards and ATM cards.

card, a line of credit extended by the card issuer is accessed). Since debit cards are in effect payment substitutes for credit cards and are subject to the same risks of theft and fraud, Visa believes these access devices should be treated similarly as credit cards under the sentencing guidelines.

For the reasons discussed above in the context of credit cards, Visa urges the Sentencing Commission to reconsider its proposed rule that, where there has been no unauthorized use of the stolen debit card, the loss for purposes of the sentencing guidelines is only \$100. For the same reasons why the loss for unused stolen credit cards should be calculated by reference to the available credit line, the loss for an unused stolen debit card should be considered to be the available balance in the victim's account that can be accessed with the stolen debit card. Like the check drawn on the victim's account, the loss in the case of an unused stolen debit card should not be the actual debit to the victim's account, but rather the debits that could have occurred had the criminal used the debit card. Alternatively, the same type of graduated scale based on the number of stolen cards discussed above in the context of credit cards also could be utilized in the case of stolen but unused debit cards.

Finally, Visa also supports the proposed revision to this Commentary 4 that clarifies that this commentary applies to purloined credit card or access device account numbers, even if the criminal never has possession of the victim's actual card or access device. The criminal does not need the card, only the card number, to steal from the cardholder. A criminal with only the card number can engage in a wide variety of transactions where the card need not be present, such as transactions over the telephone. Moreover, certain criminals are able to manufacture their own cards with the victim's number, and then use the manufactured card to engage in the full range of card transactions.

Copyright Infringement

As mentioned above, certain criminals, typically members of sophisticated crime gangs, will manufacture fake credit or debit cards, using stolen card numbers. These fake cards may violate, among other criminal laws, protected trademarks and potentially other intellectual property of Visa and the card issuer. Accordingly, Visa is interested in the proposed revisions to Section 2B5.3(b) addressing penalty levels for crimes involving criminal infringement of copyrights or trademarks.

Visa supports the proposed options that utilize a \$2000 starting point (options 2 and 4). The \$2000 starting point, rather than the \$5000 starting point of the other options, will enable Section 2B5.3(b) to be considered where appropriate in more instances of credit and debit card fraud. Also, for the reasons discussed above, Visa

recommends that this proposed amendment or the related commentary clarify that the retail value of the infringing fake credit or debit card equals the available credit line that can be accessed by the card (for credit cards) or the available balance in the victim's checking account that can be accessed by the card (for debit cards).

Telemarketing Fraud

The Sentencing Commission also requested comment on a number of issues relating to the treatment of telemarketing fraud under the sentencing guidelines. Visa's interest in telemarketing fraud results from the unfortunate fact that many telemarketing fraud criminals obtain from the victim his or her credit or debit card number, typically under fraudulent pretenses, and then use that number to fraudulently obtain the victim's funds.

Given our experiences with telemarketing fraud, Visa believes that the sentencing guidelines should treat telemarketing fraud more severely than other types of fraud involving comparable loss amounts. As recognized by Congress in enacting the Telemarketing and Consumer Fraud and Abuse Prevention Act of 1994 (15 U.S.C. § 6101 et seq.), which Visa strongly supported, there are unique aspects of telemarketing fraud which support this special treatment under the sentencing guidelines. First, telemarketing fraud criminals frequently target the elderly and others they believe to be particularly susceptible to victimization. This is done for example by using telephone lists of elderly Americans, or by referencing products intended to attract the elderly, such as pharmaceuticals. Second, because these fraudulent schemes operate on an interstate basis and the criminals frequently change locations, it is often difficult for law enforcement to track and apprehend them until after a substantial amount of fraud has occurred. The nature of this fraud typically involves a large number of victims, each victimized for relatively small amounts. Indeed, a successful fraudulent telemarketing operation can victimize thousands in a few weeks. Finally, because of the low cost of establishing and operating a telemarketing scam -- frequently just a telephone and scripts -- it is easy for the criminals to restart and many of these criminals do restart their criminal operations after being shut down. Given these characteristics of telemarketing fraud, Visa believes that the Sentencing Commission should revise the sentencing guidelines to increase the levels for telemarketing fraud in order to further deter telemarketing fraud and more severely punish telemarketing fraud criminals.

U.S. Sentencing Commission
March 11, 1998
Page 7

* * * * *

Visa very much appreciates this opportunity to comment on the Proposed Amendments. If Visa can be of assistance to the Sentencing Commission in connection with the Proposed Amendments, or there are any questions regarding this letter, please do not hesitate to contact me, at (650) 432-3111.

Sincerely yours,

A handwritten signature in cursive script, appearing to read "Russell Schrader".

Russell Schrader
Vice President and Senior Counsel

Fraud Control Programs of Visa and Visa Member Financial Institutions

Visa and the Visa member financial institutions have developed a varied arsenal of fraud control programs. These fraud control programs are described below:

Address Verification Service (AVS)

A fraudulent use prevention system that allows mail-order/telephone-order merchants to automatically verify that a billing address provided by a cardholder is the same as the cardholder's billing address currently on file with the Issuer. This service helps merchants minimize the risk of accepting fraudulent mail and telephone order transactions.

Card Activation

An alternative bank card delivery method in which Issuers wait to confirm that a card has been received by the valid cardholder before activating the account. Cards are blocked at the time of mailing; for a card to be activated, the cardholder must call the Issuer to confirm receipt and provide positive proof of identity.

Card Security Features

Alphanumeric, pictorial, and other design and functional elements on bank cards. The exact physical dimensions and placement of these features are specified by the *Visa U.S.A. Operating Regulations* and are difficult to copy exactly. Card security features are checked by merchants at the point of sale to ensure the card is valid.

Card Verification Value (CVV)

A unique three-digit "check number" encoded on the magnetic stripe of all valid cards. The number is calculated by applying an algorithm — a mathematical formula — to the stripe-encoded account information and is verified on-line at the same time a transaction is authorized.

Cardholder Risk Identification Service (CRIS)

A transaction scoring and reporting service that employs neural network technologies to develop risk-scoring models that identify fraudulent transaction patterns. The service, available by subscription through Visa, can be used by Issuers as a stand-alone fraud detection system or as a complement to their internal fraud detection methods.

ATTACHMENT (CONTD)

Exception File

Visa's worldwide data base of account numbers of lost/stolen or other cards Issuers have listed for pickup, referral, or other special handling. The account numbers for all transactions routed to Visa's stand-in processing system are checked against the Exception File.

Issuers' Clearinghouse Service (ICS)

A bank card application verification system shared by Visa with MasterCard. ICS verifies an applicant's address, phone and Social Security numbers, and whether he or she has a history of excessive applications or credit card fraud or abuse. ICS is a mandated service for U.S. card issuers that are Visa members.

NRI Reporting

A computer program developed by Visa for reporting Not Received Items (NRI). All Visa Issuers are required to report NRI mailing information, whether or not fraud has occurred. Visa will then forward this information along with reported NRI fraud transactions to the U.S. Postal Service on a daily basis. This information will allow the Postal Service to conduct investigations in a more timely manner.

Recovered Account Analysis

Assistance to law enforcement for recovered account numbers due to arrests and/or searches. Individual Issuers are identified, contacted and requested to provide information directly back to the investigating law enforcement agency.

Risk Identification Service (RIS)

The Risk Identification Service identifies concentrations of fraud activity at merchant locations. RIS monitors activity such as reported fraud transactions, suspicious fraud activity, and merchant deposits. By carefully monitoring such activity and imposing timely corrective measures, Visa members can reduce their exposure to fraud and subsequent financial losses.

VisaLine

A subscription service providing an interactive computer network dedicated to the communication of time-sensitive risk management and business information between Visa and its members and their third-party processors.