

RUSSELL W. SCHRADER
Senior Vice President
Assistant General Counsel

5

VISA

October 8, 2003

Robert E. Feldman
Executive Secretary
Attention: Comments/OES
Federal Deposit Insurance Corporation
550 17th Street, NW
Washington, DC 20429

Ms. Jennifer J. Johnson
Secretary
Board of Governors of the Federal
Reserve System
20th Street and Constitution Avenue, NW
Washington, DC 20551
Attn: Docket No. OP-1155

Public Information Room
Office of the Comptroller of the Currency
250 E Street, SW
Mail Stop 1-5
Washington, DC 20219
Attention: Docket No. 03-18

Regulation Comments
Chief Counsel's Office
Office of Thrift Supervision
1700 G Street, NW
Washington, DC 20552
Attention: No. 03-35

Re: Proposed Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice

Ladies and Gentleman:

This comment letter is submitted on behalf of Visa U.S.A. Inc. in response to the Notice and Request for Comment issued by the Federal Deposit Insurance Corporation, Federal Reserve Board, Office of the Comptroller of the Currency and Office of Thrift Supervision (collectively, "the Agencies") regarding the "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice" ("Proposed Guidance"). Visa appreciates the opportunity to comment on this very important issue.

The Visa Payment System, of which Visa U.S.A.¹ is a part, is the largest consumer payment system, and the leading consumer e-commerce payment system, in the world, with more volume than all other major payment cards combined. There are more than one billion Visa-branded cards, and they are accepted at more than 28 million physical locations in 144 countries. Visa plays a pivotal role in advancing new payment products and technologies, including technology initiatives for protecting personal information and preventing identity theft and other fraud, for the benefit of its 21,000 member financial institutions and their hundreds of millions of cardholders worldwide.

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

Visa supports the statement in the Proposed Guidance that an aggressive response program is a key part of an institution's information security plan and Visa supports the Agencies' efforts to explore measures aimed at enhancing the security of customer information and reducing the deleterious effects of identity theft. However, key aspects of the Proposed Guidance do not effectively recognize the day-to-day realities of customer information security and suggest an overly rigid approach that is likely to be both inefficient and harmful. In particular, a more balanced and flexible approach is needed to allow financial institutions to develop and implement effective and efficient fraud prevention measures, consistent with their overall security procedures and business operations.

Visa believes that the appropriate response to a security breach affecting customer information depends on the specific factors of that breach, including the information accessed, the extent to which the interloper who accessed the information has had an opportunity to use or further disclose the information for illicit purposes, and the tools available to both the financial institution and its customers to identify and address the illicit use of customer information. In addition, an appropriate response must balance the risks of illicit use of the information affected, against the risks that the response itself may lead to customer cost and inconvenience that are actually greater than the risk of illicit use of the information under the circumstances.

The latter issue has particular significance when determining whether customer notification is appropriate following any particular security breach. Implicit in the concept of customer notification is the idea that a customer receiving that notification can take steps to protect himself or herself against identity theft or other fraud. Customer scrutiny of billing statements for unauthorized transactions, the ability to close fraudulently established accounts, the ability of customers to place fraud alerts on their files at consumer reporting agencies, and the ability of customers to review their consumer reporting agency files are all important steps in preventing identity theft and other fraud. However, in the context of payment card accounts—both credit card and debit card accounts—these steps serve merely as backstops to the far more sophisticated fraud detection systems currently in place for both existing and new accounts, including the Visa cardholder account fraud detection systems and the customer identification requirements mandated by Section 326 of the USA PATRIOT Act ("Section 326"). Moreover, while scrutiny of billing statements should be routine, the closing of accounts, the placing of fraud alerts, and the review of files at consumer reporting agencies involve costs and inconvenience for both the customer and the marketplace as a whole. For example, closed accounts must be replaced, fraud alerts may impede future transactions, and repeated access to consumer reporting agency files is costly. Moreover, a proliferation of fraud alerts that are not related to actual fraud can actually dilute the effectiveness of fraud alert programs, since a series of false positives makes it more difficult to identify real fraud, potentially making identity theft easier rather than harder.

Given these considerations, Visa believes that an appropriate response to a security breach should involve a three-step process. First, an assessment of the fraud risks associated with the particular breach, second, an assessment of the tools available to address those risks, and third, an assessment of whether and the extent to which customer participation is likely to be an important element of controlling those risks; in other words, the utilization of a risk-based model for customer notification. In addition, any consideration of the appropriateness of customer

notification must include consideration of the content of the notice and the advice to be given to the customer. While the Proposed Guidance generally recognizes these three steps, Visa believes that the structure and language of the Proposed Guidance could be improved significantly in order to reduce the likelihood that the Guidance will cause institutions to react to security breaches inappropriately.

In order to put these steps in perspective, for example, it is important to understand the fraud prevention systems that are already in place with respect to Visa payment cards. In this regard, Visa, and its card-issuing members, already implement internal procedures that parallel the Proposed Guidance's provision regarding the monitoring of affected accounts for unusual or suspicious activity. These procedures include sophisticated neural networks that flag unusual spending patterns for fraud, and block the authorization of transactions where fraud is suspected. In addition, financial institutions, particularly card issuers, use increasingly sophisticated customer identification procedures in connection with account openings, as required by Section 326.

Visa has long recognized the importance of strict internal procedures to protect the customer information of Visa's members, thereby protecting the integrity of the Visa system. As a result, Visa is currently implementing a comprehensive and aggressive customer information security program known as the Cardholder Information Security Plan ("CISP"). This security program applies to all entities that store, process, transmit, or hold Visa cardholder data. CISP was developed, and is already being used, to ensure that the customer information of Visa's members is kept protected and confidential. As a part of CISP, Visa requires that all participating entities comply with the "Visa Digital Dozen"—twelve basic requirements for safeguarding accounts. These include: (1) install and maintain a working network firewall to protect data; (2) keep security patches up-to-date; (3) protect stored data; (4) encrypt data sent across public networks; (5) use and regularly update anti-virus software; (6) restrict access to data by "need-to-know;" (7) assign a unique ID to each person with computer access; (8) do not use vendor-supplied defaults for system passwords and security parameters; (9) track all access to data by unique ID; (10) regularly test security systems and processes; (11) implement and maintain an overall information security policy; and (12) restrict physical access to data. These requirements are enforced by a mandate that Visa approved third-party firms conduct independent data security audits.

Notification to Regulatory and Law Enforcement Agencies

The Proposed Guidance states that a financial institution should "notify its primary [f]ederal regulator when it becomes aware of an incident involving unauthorized access to or use of customer information that could result in substantial harm or inconvenience to its customers."² Visa believes, however, that too broad of a notification requirement may be counterproductive. As the Agencies can appreciate from their own experience dealing with confidential information, the situations where there is "some potential for harmful results" far exceeds those situations where there is a significant likelihood that information will, in fact, be misused, let alone where there is some evidence that such information has actually been misused.

² 68 Fed. Reg 47,954, 47,959 (Aug. 12, 2003).

In this regard, Visa believes that among the most important tools shared between financial institutions and their service providers in the fight against customer information theft is free and open disclosure. Financial institutions typically require service providers to fully disclose information relating to any breach in security resulting in an unauthorized access to, or use of, the financial institution's customer information. However, Visa believes that a regulatory response program that unnecessarily mandates notification of customers and other entities, such as law enforcement and regulatory agencies, of security breaches, or that requires other steps such as securing or monitoring accounts when the breach does not rise to an appropriate threat level, will tend to discourage service providers from disclosing security breaches because of potential liability concerns and reputational risk.

As a result, Visa believes that in order to facilitate free and open disclosure between financial institutions and service providers, all unnecessary responses, including notifications to customers, law enforcement agencies, and regulatory agencies, should be avoided. Accordingly, Visa recommends that the notification provision in the Proposed Guidance be narrowed to situations where substantial harm to customers has occurred, or is at least likely to occur, instead of merely possible. In this regard, it is important to recognize that the Visa system provides for zero liability for unauthorized customer transactions, thereby significantly limiting the potential harm to Visa cardholders from fraud, including identity theft. Thus, financial institutions employing such a zero liability policy should be afforded the flexibility of not taking significant actions that they believe will adversely affect their customers, unless they determine that those customers are likely to suffer actual harm.

Corrective Measures

Flagging Accounts

The Proposed Guidance states that financial institutions should immediately begin identifying and monitoring the accounts of customers whose information MAY have been accessed or misused.³ Like the use of the term "could" with respect to notification of regulatory and law enforcement agencies discussed above, Visa believes that the proposed "may" language regarding the flagging of accounts is unclear and overbroad. It is unclear from the Proposed Guidance's use of the term "may" exactly what constitutes a triggering event and how long such "flagging" should last. Accordingly, Visa believes that the use of the word "may" will result in the unnecessary flagging of accounts in situations where it is unlikely that any customer harm will result. Moreover, unlike customer notification, which would be required under the Proposed Guidance after a security breach of sensitive customer information, flagging would be required after a security breach of *any* customer information—significantly increasing the instances where special monitoring is unnecessarily required.

Moreover, Visa believes that the decision to flag accounts and the nature of that "flag" should be left to individual financial institutions' risk-based procedures, particularly where fraud monitoring systems are already in place. As noted above, Visa and its members already routinely monitor account activity for fraud. Visa believes that this risk-based approach would protect accounts when there is a true threat of fraud from a customer information security breach,

³ *Id.*

instead of the repetitive and unnecessary flagging that is suggested by the language of the Proposed Guidance.

Securing Accounts

The Proposed Guidance states that “[w]hen a checking, savings, or other deposit account number, debit, or credit card account number, personal identification number [PIN], password, or other unique identifier has been accessed or misused, the financial institution should secure the account, and all other accounts and bank services that can be accessed using the same account number or name and password combination until such time as the financial institution and the customer agree on a course of action.”⁴ Again, given the Proposed Guidance’s language, the precise meaning of “secure accounts,” is unclear. In some cases, for example, it may be possible to keep an account open and block transactions on the account that present greater risk, such as those where the customer is not present, until the concern over potential unauthorized use of the account is dispelled. As a practical matter, if accounts are only required to be secured when there is a substantial risk of fraud, it may be simpler to close the account. If securing an account means closing the account, or blocking its use in all situations, the adverse effects on customers will be substantial. Moreover, closing of customer accounts should only be done when the risks of fraud are clear and substantial.

The Proposed Guidance suggests that anytime the requisite information is accessed, an account must be secured. Although Visa supports the closing of accounts when there is material evidence of fraud, the Proposed Guidance could be read to require such a response even where a financial institution reasonably concludes that the potential for fraud or information misuse can be addressed effectively by other means, such as the neural networks described above. Visa believes that the better approach with respect to closing accounts lies with a risk-based model that permits the financial institution the flexibility to determine when and how an account should be closed, or even secured, by weighing the severity and likelihood of harm that a security breach is anticipated to cause. On the contrary, requiring that account(s) be closed in non-threatening situations until the customers and the financial institution can agree on a course of action will only result in inefficiency and the unnecessary burdening of the customers with the hardships and costs associated with replacing accounts. As in the case of other corrective measures, the decision to close accounts should be left to the individual financial institution and, where notification to the customer is appropriate, the customer.

Customer Notification and Internal Fraud Procedures

The Proposed Guidance also states that a financial institution should “notify affected customers whenever it becomes aware of unauthorized access to sensitive customer information unless the institution, after an appropriate investigation, reasonably concludes that misuse of the information is unlikely to occur and takes appropriate steps to safeguard the interests of affected customers, including by monitoring affected customers’ accounts for unusual or suspicious activity.”⁵ Generally, Visa supports the concept of customer notification in appropriate circumstances pursuant to risk-based procedures, as described in this letter. Visa also supports

⁴ *Id.*

⁵ 68 Fed. Reg 47,954, 47,960 (Aug. 12, 2003).

the Proposed Guidance to the extent it would allow financial institutions the flexibility of first performing appropriate investigations into security breaches to ascertain potential customer impact before any decision is made to notify affected customers. Nevertheless, there are significant issues with the proposed customer notification language that should be addressed.

Visa believes that, given the uncertainty and potential breadth of the proposed language regarding customer notification, the Proposed Guidance could trigger the customer notification provision in an unpredictable manner resulting in unnecessary notifications. While the proposed language permits a financial institution to forego notification if, after a reasonable investigation, the institution concludes that fraud or information misuse is unlikely to occur, it is not clear given the language of the Proposed Guidance what constitutes a security breach likely to create significant fraud risks. As a result, the Proposed Guidance is likely to cause unnecessary customer notifications, which will lead to needless customer concern and inconvenience, and eventually will blunt the effectiveness of such notices because of their frequent use in non-threatening situations.

Moreover, the Proposed Guidance's statement, that notification is required "whenever [the financial institution] becomes aware of unauthorized access to sensitive customer information,"⁶ further increases the risk of unnecessary notifications. Because of the short time period between discovery of a security breach, and the deadline set by the Proposed Guidance for customer notification, it is likely that customer notifications will be required before an appropriate investigation can take place. As a result, this statement is at odds with the Proposed Guidance's statement that a financial institution may avoid customer notification, if after a reasonable investigation, it determines that no threat of information misuse is likely to occur. Therefore, the statement requiring that customer notification take place "whenever [the financial institution] becomes aware of unauthorized access," should be removed to make it clear that financial institutions may conduct reasonable investigations to determine whether or not customer notification is necessary.

In the event that customer notification does become necessary, the Proposed Guidance may unnecessarily limit the options available to financial institutions for notification delivery. For example, the Proposed Guidance states that if a financial institution is able to pinpoint individual accounts affected by a security breach, individual notifications to affected customers will suffice. However, if the financial institution is unable to determine precisely what customers are affected, the Proposed Guidance states that the financial institution should "notify each customer in groups likely to have been affected."⁷ First, individual customer notification where there is no evidence regarding which customers may have been affected should be avoided at all costs, since it advises the customer that he or she may be the victim of fraud when there is no evidence that this statement is accurate. In addition, although the Proposed Guidance states that financial institutions may make notification deliveries "in any manner that will ensure that the customer is likely to receive it,"⁸ the only notification delivery methods mentioned are phone, conventional mail, and electronic notice. Instead, the rules for mass customer notification should provide flexibility for the financial institution to notify customers either by the traditional

⁶ *Id.*

⁷ 68 Fed. Reg. 47,954, 47,959 (Aug. 12, 2003).

⁸ *Id.*

methods enumerated in the Proposed Guidance, or, when timely notice or economic restraints are an issue, by substitute methods. For example, if a financial institution determines that a security breach warrants mass customer notification, the financial institution should be permitted to utilize alternative notification methods, such as Internet Web site notification, and notification through national media outlets. Moreover, such notification should be required only where a reasonable investigation actually reveals a threat that the customer needs to address with proper safety measures, and those measures should be consistent with the evidence.

In addition, in determining when customer notification is necessary, the Proposed Guidance appears to exceed the scope of the existing guidelines establishing standards for safeguarding customer information. The Proposed Guidance explains that notice would be required whenever there has been unauthorized access to sensitive customer information unless an appropriate investigation by the financial institution reasonably concludes that misuse of the information is unlikely to occur. Sensitive customer information is defined as certain account related information such as an account number or a PIN number in conjunction with certain identifying information including address.⁹ Instead, sensitive customer information should only include nonpublic personal information as defined in the rules implementing the privacy provisions of Title V of the Gramm-Leach-Bliley Act. For example, a four digit number, that may be a PIN number, coupled with an address, without further information, does not constitute nonpublic personal information, nor should it pose a significant threat of identity theft.

Furthermore, given the complex nature of customer notification under the Proposed Guidance, the Agencies attempt to clarify what constitutes a triggering event by providing several examples to illustrate when customer notification is necessary and when it is not. However, consistent with a risk-based approach to customer notification, these illustrations of appropriate triggering events are too broad and should be narrowed in scope. For example, the first illustration concludes that customer notification should take place when “[a]n employee of the institution has obtained unauthorized access to sensitive customer information maintained in either paper or electronic form.”¹⁰ While this example would cover a situation where an employee actually obtains unauthorized access to customer information for illicit purposes, the example also could be read to include other non-threatening or less threatening situations, such as where an employee gains access to the general area where customer information is stored, but not access to the information itself, or where there is no reasonable evidence to suggest that the employee was acting in furtherance of an illicit purpose. While a financial institution should be expected to investigate each situation where an employee gains unauthorized access to customer information under suspicious circumstances, investigations and notifications based simply upon “access,” with no indication of wrongdoing or wrongful intent, would unduly burden financial institutions. Therefore, the example should be clarified to reflect a flexible risk-based model of investigation and customer notification, allowing the financial institution the flexibility to determine the proper scope of investigation and the proper level of threat that justifies customer notification.

Visa strongly supports customer notification, combined with monitoring of affected accounts for unusual activity, whenever unauthorized access to customer information results in a

⁹ 68 Fed. Reg 47,954, 47,960 (Aug. 12, 2003).

¹⁰ *Id.*

October 8, 2003

Page 8

significant recognizable threat that suggests the need for customer action. However, for situations that involve unauthorized access to customer information, but which do not indicate a significant risk that customer information will be the subject of fraud or misuse, notification of customers should not be required. Instead, the institution should be permitted to monitor the affected customer accounts for the period of time and to the extent warranted by the particular circumstances. This approach is consistent with the Proposed Guidance's direction that no customer notification is necessary when sensitive customer information misuse is unlikely to occur, while still retaining a balance between customer information security and unnecessary and potentially harmful customer notification. In this regard, for example, when a financial institution participates in a payment system, like the Visa payment system, that has a program designed to identify and prevent fraud, and where the liability of individual customers for unauthorized transactions is limited, no notice should be required in conjunction with a security breach of customer information unless there is actual evidence that the personal information obtained is being used for purposes of fraud.

In preparing the final rules on this subject, it is also important for the Agencies to recognize that financial institutions are already aggressively implementing their own monitoring systems to deter fraud and identity theft and, thus, are already in a position to determine the level of response appropriate for each individual security breach through existing risk-based procedures. As a result, the imposition of inflexible notification and monitoring rules will only hamper security response programs by removing the flexibility and effectiveness of the risk-based security response programs described above.

In conclusion, Visa appreciates the opportunity to comment on this very important topic. If you have any questions concerning these comments, or if we may otherwise be of assistance in connection with this matter, please do not hesitate to contact me at (415) 932-2178.

Sincerely,

Russell W. Schrader
Senior Vice President and
Assistant General Counsel