WRITTEN STATEMENT

OF

MARK MACCARTHY

ON BEHALF OF

VISA U.S.A. INC.

BEFORE THE

SUBCOMMITTEE ON

TERRORISM, TECHNOLOGY AND HOMELAND SECURITY

OF THE

COMMITTEE ON THE JUDICIARY

UNITED STATES SENATE

November 4, 2003

Mr. Chairman, Ranking Member Feinstein and Members of the Subcommittee, my name is Mark MacCarthy. I am Senior Vice President for Public Policy for Visa U.S.A. Inc. Thank you for the invitation to participate in this hearing. Visa appreciates the opportunity to address the important issues raised by S. 1350, the "Notification of Risk to Personal Data Act" ("S. 1350"). S. 1350 would require federal agencies and persons engaged in interstate commerce, that own or license electronic data containing personal information, to notify affected individuals of any unauthorized acquisition of such information.

The Visa Payment System, of which Visa U.S.A. 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. 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 member financial institutions and their hundreds of millions of cardholders.

Visa commends the Subcommittee for focusing on the important issue of consumer information security. As the leading consumer electronic commerce payment system in the world, Visa considers it a top priority to remain a leader in the development of technology, products, and services that protect consumers from the effects of information security breaches. As a result, 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. 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. Additionally, 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.

In addition, Visa's information security policy for the treatment of personal information includes sophisticated neural networks that flag unusual spending patterns for fraud and block the authorization of transactions where fraud is suspected. As an additional customer protection, the Visa system provides for zero liability for unauthorized customer transactions, thereby significantly limiting the potential harm to Visa cardholders from information security breaches, including identity theft. Visa also maintains the Exception File, 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 through the Visa Payment System have their account numbers checked against the Exception File.

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. Critical to the concept of customer notification is the idea that a customer receiving that notification can take steps to protect him 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. 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 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.

Accordingly, Visa strongly supports customer notification whenever unauthorized access to customer information results in a significant, recognizable threat that requires 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 is not necessary.

In the context of the Visa system, Visa believes that notification of a security breach should only be undertaken when there is clear evidence that the information that has been the subject of a security breach is being used for fraudulent purposes. Further, Visa believes that it is critical that any notification requirements be sufficiently flexible to allow notice to be provided by the account holding institution whose customer is affected by the security breach where the account holding institution believes that it can minimize the disruptive effects of the notice, even if the account holding institution was not the operator of the system experiencing the breach. For example, the account holding institution may wish to offer a new account at the same time that it advises the customer that it may be necessary to close his or her existing account.

Visa is pleased to note that S. 1350 is responsive to both of these issues. S. 1350 permits the use of alternative, reasonable notification procedures where those procedures include a security program, such as the Visa program, that is reasonably designed to block unauthorized transactions before they are charged to the customer's account, and which is subject to examination for compliance by one or more of the functional regulators identified in Section 509 of the Gramm-Leach-Bliley Act, including the federal banking agencies. S. 1350 also provides for flexibility in delivering any required notice in order to minimize the disruptions to existing relationships.

Finally, Visa also is pleased to note that S. 1350 recognizes the importance of establishing consistent procedures for notifying individuals about security breaches and supersedes inconsistent state and local laws.

Visa appreciates the opportunity to appear before you today. We believe our information security response program creates a comfortable and secure environment for consumers engaged in financial transactions. Combating information security breaches and identity theft will continue as a top priority of Visa and its member financial institutions.
I would be happy to answer any questions that you may have.