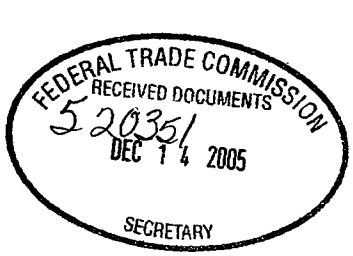
RUSSELL W. SCHRADER
Senior Vice President
Assistant General Counsel



VISA

December 14, 2005

By Hand Delivery

Federal Trade Commission
Office of the Secretary
Room 135-H
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: DSW, Inc., File No. 052 3096

Ladies and Gentlemen:

This comment letter is submitted on behalf of Visa U.S.A. Inc. in response to the proposed consent agreement issued by the Federal Trade Commission ("FTC") concerning the FTC's allegation that DSW Inc. ("DSW") failed to employ reasonable and appropriate security measures to protect sensitive personal information about its customers. Visa appreciates the opportunity to comment on this important issue.

Visa Supports the FTC's Data Security Efforts

Visa applauds the FTC for its extensive efforts relating to the important issue of data security. It is essential that all entities that maintain or have the ability to access sensitive personal information about consumers establish and maintain adequate safeguards to protect that information, and thereby protect consumers from harm.

As the leading consumer electronic commerce payment system in the world, Visa considers it a top priority to remain a leader in developing and implementing 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 security procedures to protect information relating to the cardholders of Visa's members, and thereby to protect the integrity of the Visa system as a whole.

Visa's Data Security Initiatives

Strong security measures and a consumer-focused approach to protecting sensitive information are inherent in the Visa system. For example, Visa has established a zero liability standard for cardholders for unauthorized purchases involving Visa-branded payment cards. As a result, cardholders are not responsible for unauthorized purchases on their Visa cards. In addition, Visa has developed a number of procedures and policies to help prevent the use of cardholder-related information for fraudulent purposes, such as the Cardholder Information

VISA U.S.A. INC.
Post Office Box 194607
San Francisco, CA 94119-4607
U.S.A.
Phone 415 932 2178
Fax 415 932 2525

Security Program ("CISP"). This CISP applies to all entities, including merchants that store, process, transmit or hold Visa cardholder data, and covers enterprises operating through brick-and-mortar stores, mail and telephone order centers or the Internet. CISP was developed to ensure that the customer information of Visa's members is kept protected and confidential. CISP includes provisions for monitoring compliance with CISP and sanctions for failure to comply. Visa was recently able to integrate CISP into the common set of data security requirements used by various credit card organizations without diluting the substantive measures for information security already developed in CISP. Visa supports this new, common set of data security requirements, known as the Payment Card Industry Data Security Standard ("PCI Standard"), and believes that compliance with the CISP program and the PCI Standard will not only help protect cardholder-related information, but also will assist merchants in avoiding enforcement efforts like that brought against DSW.

Visa also uses sophisticated neural networks that flag unusual spending patterns for fraud and block the authorization of transactions where fraud is suspected. When cardholder-related information is compromised, Visa notifies card issuers and puts the affected card numbers on a special monitoring status. If Visa detects any unusual activity in that group of card accounts, Visa again notifies the card issuers, to allow the issuers to begin a process of investigation and, where appropriate, card re-issuance.

Visa continues to work with key players from financial institutions, consumer advocacy groups, the government and the merchant community to provide needed education and to ensure maximum cooperation in data security efforts. For example, Visa hosted a summit on data security, entitled "Cardholder Security in the New Electronic Payments Age," in Washington, DC in October 2005, which brought together key players from various industries, law enforcement, consumer protection organizations and government to address security threats. The summit covered a range of issues, including: reducing the threat of data compromises; protecting customer information; fighting fraud and identity theft; and helping identity theft victims.

Security Programs Should be Risk-Based

Visa applauds the apparent risk-based approach adopted for the proposed consent order. In the context of data security, a one-size-fits-all approach is unworkable. Information security programs should be risk-based and entities should tailor programs to the specific characteristics of their business; in addition, they should regularly assess possible threats to their customer information systems.

When assessing the risk associated with a breach, it also is important to distinguish between the different types of sensitive information and the different types of fraud, and vary accordingly the response to each type of fraud. Identity theft is commonly confused with account fraud. Identity theft results from the stealing of a consumer's personal information, like name and Social Security number, in order to create an identity under that consumer's name and open a new account in that consumer's name. However, the consumer would not face a significant risk that fraudulent transactions will be made on the consumer's existing accounts

because this information is not sufficient to access most accounts. If a breach occurs with respect to sensitive personal information, an affected consumer can take several steps to prevent or mitigate the effects of true identity theft resulting from the breach. For example, the consumer can place an initial fraud alert on his or her credit file in order to alert creditors that an identity thief may attempt to open a fraudulent account in the consumer's name and also trigger the duty of creditors to verify an applicant's identity and confirm that the application is not the result of identity theft. The consumer also may wish to monitor his or her credit report to determine whether an identity thief has opened any fraudulent accounts.

Account fraud, on the other hand, involves the misuse of an existing account, but does not necessarily involve the risk of true identity theft. The risk of consumer harm for account fraud is significantly different than the risk of harm from identity theft, because of the meaningful consumer protections that apply to account fraud, like Visa's neural networks and Visa's zero liability policy. If a consumer's sensitive account information is acquired without authorization, the consumer would not face the risk of true identity theft because this information is not sufficient to open a fraudulent account in the consumer's name.

Therefore, the mechanisms to prevent and respond to the different types of fraud should be tailored to match the risk of consumer harm. This is supported by recent findings by ID Analytics, Inc. in its "National Data Breach Analysis" ("Analysis"). One of the key findings in the Analysis, for example, is that because data breaches vary considerably, it is necessary to classify data breaches in terms of data type. In addition, the Analysis found that account level breaches, where a consumer name and account number are the two most sensitive elements of compromised data, do not directly result in identity theft.

Visa believes it also is important for the FTC to clarify that all failures to encrypt information do not result in a failure to take reasonable and appropriate security measures to protect information. Among other things, the FTC alleges that DSW stored information in unencrypted files that could be accessed easily by using a commonly known user ID and password. Visa is concerned that the FTC's complaint, coupled with the consent order, suggests that encryption of all information is necessary to adequately protect that information. While the encryption of information under particular circumstances offers significant protection, we encourage the FTC to clarify that the consent order is not intended to suggest that all information must be encrypted in all situations. The need to encrypt information, like data security generally, should be risk-based and, thus, when considered in the context of an institution's overall security program, should depend on the nature of the business, the sensitivity of the information, likely threats involving that information, and other similar risk factors.

Moreover, as the FTC addresses future security breach incidents, we encourage the FTC to be mindful that the selection of appropriate corrective efforts can and should vary depending upon the types of information and fraud involved, and the risks associated with such fraud. More specifically, in assessing the type and amount of risk and the appropriate efforts to address that risk, the FTC should consider whether there is, in fact, a significant threat of consumer harm. As part of this assessment, the FTC might consider, for example, whether it is possible to determine that sensitive account information was actually taken or whether there is, in fact, a significant

risk that the loss of a laptop computer or a computer tape containing account information will lead to account fraud. A stolen laptop that is quickly recovered before the thief has time to compromise information, or a lost computer tape returned by a finder, poses little, if any, risk of harm.

Both Consumers and Card Issuers Should be Protected from Harm

Visa believes that it is important that the FTC fully appreciate that card-issuing institutions, as well as consumers, are harmed by security breach incidents and that both consumers and card-issuing institutions should be protected from harm. Specifically, Visa's zero liability policy provides significant protection for Visa cardholders against fraud on their existing accounts due to information security breaches. Because financial institutions that are Visa members do not impose the losses for fraudulent transactions on their cardholders, these institutions and, in some cases, the merchants that honor Visa cards, are the ones that incur the costs resulting from fraudulent transactions.

These costs are largely in the form of direct dollar losses from credit that will not be repaid. In most of these transactions, the fraud losses are borne by the card issuer, although, in some telephone and Internet transactions, some of those costs may be passed back to the acquiring bank or the merchant that participated in a fraudulent transaction. Card issuers also incur costs in opening replacement accounts and in reissuing replacement cards. In order to protect its members from these costs, Visa aggressively protects the customer information of its members.

Nevertheless, it is important to understand that in relative terms, security breaches have resulted in minimal transaction fraud involving Visa-branded accounts, due in large part to Visa's sophisticated neural networks and other anti-fraud programs. These Visa anti-fraud programs protect both card-issuing financial institutions and their cardholders.

Once again, we appreciate the opportunity to comment on this important matter. 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