RUSSELL W. SCHRADER
Senior Vice President
Assistant General Counsel

VISA

July 18, 2005

By Electronic Delivery

Federal Trade Commission
Office of the Secretary
Room H-159
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: BJ's Wholesale Club, Inc., File No. 042 3160

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 BJ's Wholesale Club's ("BJ's") failed to employ reasonable and appropriate security measures to protect sensitive personal information about its consumers. Visa appreciates the opportunity to comment on this 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. For calendar year 2004, Visa U.S.A. card purchases exceeded a trillion dollars, with over 450 million Visa cards in circulation. Visa plays a pivotal role in advancing new payment products and technologies, including technology initiatives for protecting sensitive personal information and preventing identity theft and other fraud, for the benefit of Visa's member financial institutions and their hundreds of millions of cardholders.

Visa Applauds the FTC's Data Security Efforts

Visa applauds the FTC for its 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. Visa has not taken a position on specific pending legislation in this area. In general, we favor federal legislation that would extend reasonable risk-based security and notification requirements to all entities that have sensitive customer information.

[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 U.S.A. INC.
Post Office Box 194607
San Francisco, CA 94119-4607
U.S.A.

Phone 415 932 2178
FAX 415 932 2525

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, thereby protecting the integrity of the Visa system as a whole.

Visa's Data Security Initiatives

Strong security measures and a consumer-focused approach to protect sensitive information are inherent in the Visa system. Visa U.S.A. establishes 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 to Visa's zero liability policy, Visa has developed a number of procedures and policies to help prevent the use of cardholder-related information for fraudulent purposes. For example, Visa U.S.A. employs a multi-faceted approach to combat account fraud and identity theft and has implemented a comprehensive and aggressive customer information security program known as the Cardholder Information Security Plan ("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 not only data security standards, but also provisions for monitoring compliance with CISP and sanctions for failure to comply. Visa has been 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 BJ's.

In addition, Visa 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 cards, Visa again notifies the card issuers, which begins a process of investigation and card re-issuance, where appropriate.

Security Programs Should be Risk-Based

Visa applauds the apparent risk-based approach agreed to in 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, which results from the stealing of one's personal information, like name and Social Security number, in order to create an identity under another person's name, is commonly confused with account fraud. Account fraud is fraud that involves the misuse of existing accounts, but does not necessarily involve the risk of identity theft. The risk of consumer harm for account fraud is significantly different than the risk of harm for identity theft, for example, because of meaningful consumer protections like Visa's zero liability policy. Therefore, the mechanisms to prevent and respond to the different types of fraud should be tailored to match the risk of consumer harm.

Visa also recommends that the FTC 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 BJ's did not encrypt information while in transit or when stored on the in-store computer networks. Visa is concerned that the FTC's complaint, coupled with the consent order, suggests that encryption of all information is necessary to adequately protect information. While 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, 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 risk factors.

Moreover, as the FTC addresses future incidents that may arise, 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 whether 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 would pose 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 U.S.A.'s zero liability policy provides significant protection for Visa cardholders against fraud on their existing accounts due to information security breaches. Because the 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, 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. In order to protect its members from these costs, Visa aggressively protects the customer information of its members.

It is important to understand that 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, and that, because of Visa's zero liability policy, the costs of account fraud are absorbed largely by card-issuing financial institutions and not by consumers.

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