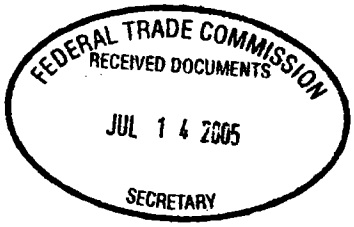

July 14, 2005

Federal Trade Commission
Office of the Secretary, Room H-159
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

Re: Proposed Settlement in the Matter of BJ's Wholesale Club, Inc.
Docket No. 0423160 (Released June 16, 2005)

Dear Sir or Madam:

America's Community Bankers ("ACB")[1] is pleased to comment on the Federal Trade Commission's (the "Commission") proposed consent order in the matter of BJ's Wholesale Club, Inc. (File No. 0423160). The consent order addresses the failure of BJ's Wholesale club to establish appropriate security controls to protect customer credit/debit card account numbers stolen from its computer systems.

ACB Position

ACB appreciates the action by the Commission to challenge companies that fail to adequately protect sensitive consumer information and urges the Commission to remain proactive in this regard. The growing number of major data compromises reported in the news media recently shows no sign of slowing. This means that the Commission will be faced with an increasing caseload where action will be required. We urge the Commission to continue to diligently pursue entities responsible for data breaches.

With respect to the proposed settlement, ACB generally supports the action taken by the Commission; however, we have several suggestions for the Commission in response to the settlement and ongoing public policy concerns. Specifically, ACB urges the Commission to consider the following additional actions:

- BJ's Wholesale Club should be subject to an annual information security audit requirement to ensure sensitive information is protected;

- The Commission should work with the federal banking agencies as they examine the relationships between banks and companies involved in data compromises;

[1]America's Community Bankers represents the nation's community banks. ACB members, whose aggregate assets total more than $1 trillion, pursue progressive, entrepreneurial and service-oriented strategies in providing financial services to benefit their customers and communities.

900 Nineteenth Street, NW ★ Suite 400 ★ Washington, DC 20006
Phone: (202) 857-3100 ★ Fax: (202) 296-8716 ★ www.AmericasCommunityBankers.com

- The Commission should support consideration of legislation that will require entities that handle significant volumes of sensitive consumer information to have effective information security programs in place; and

- The Commission should not hesitate from imposing significant monetary penalties on companies that fail to protect consumer information.

Background

BJ's Wholesale Club is a Massachusetts based company with more than 150 stores operating in the Eastern United States with net sales totaling $6.6 billion in 2003. In early 2004, confidential customer data including credit/debit card numbers and information contained in the magnetic stripe of the each card was obtained and used by criminals to create counterfeit cards that were used to make millions of dollars worth of fraudulent purchases. According to filings with the Security and Exchange Commission, BJ's Wholesale Club faces approximately $13 million in outstanding claims related to this loss of data.

The Commission determined that BJ's Wholesale Club failed to have in place reasonable measures to secure personal information collected at its stores from at least November 2003 until February 2004. Specifically, the Commission noted that BJ's Wholesale Club:

- Stored sensitive customer information in files that could be accessed with known default user identification and passwords;

- Failed to encrypt information on in-store wireless networks;

- Failed to use available security measures to protect wireless networks;

- Failed to establish measures to detect unauthorized access to systems; and

- Stored credit/debit card information in violation of card association rules.

Pursuant to the proposed consent agreement, the Commission has ordered that BJ's establish and implement an "information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers." The consent agreement also requires BJ's to obtain information security audits by an independent third party security professional every other year for the next twenty years. No monetary penalties were imposed as part of the settlement.

Community Banks Hit Hard By Incident

Federal law and card association operating rules require insured institutions to address promptly any consumer losses relating to fraudulent electronic transactions such as those associated with the compromised card information outlined in the consent agreement. As such, no consumer should have borne any direct losses related to fraudulent transactions occurring in their account.

While community banks had no responsibility, or ability to protect customers from the losses associated with BJ's negligent information handling procedures, it is the institutions that bear the burden of notifying consumers, canceling/reissuing cards, and monitoring customer accounts for fraudulent activity. Additionally, it is the community banks with whom the consumer has the relationship that is reflected in customer frustration and the reputation risk associated with compromised card information.

Community banks are especially hard hit by incidents like this as they often do not have the sophisticated--and expensive--systems necessary to dynamically track customer card activity and have few options other than canceling/reissuing affected customer cards. The costs associated with reissuing cards are significant and include expenses for fraudulent transactions, reissuing plastic, risk management, customer support, and compliance/legal expenses. And while some of these costs can be recovered, most are borne exclusively by the institution.

The card association rules provide some opportunities for the banks that are association members to recover costs; however negotiating the complex and cumbersome compliance rules is a challenge for community banks with limited resources. There are countless examples of community banks entitled compensation that came to the determination that the costs associated with obtaining relief through the card association rules (e.g., staff time, legal expenses, etc.) is equaled or exceeded by the amount recoverable.

Information Security Program

The consent agreement requires BJ's Wholesale Club to establish a comprehensive information security program to protect sensitive consumer information. Pursuant to the consent agreement, BJ's Wholesale Club must: (1) designate an employee responsible for information security program; (2) conduct an information security risk assessment; (3) develop and regularly test information security safeguards; and (4) update and adjust information security as needed. The requirements outlined by the Commission are similar to those to which every federally insured depository institution is subject pursuant to the Gramm-Leach-Bliley Act ("GLBA"). Moreover, insured institutions are subject to regular examination by federal regulatory authorities, which includes an assessment of a bank's GLBA information security program.

ACB strongly believes that all entities that handle sensitive financial information should be required to have an adequate information security program designed to protect the integrity and security of such information. We commend Commission Chairman Deborah Majoras for her public expression of support for a new federal law to require businesses not subject to GLBA to establish and maintain an adequate information security program during recent Congressional hearings on information security. ACB encourages the Commission to continue its support for legislative changes that will require all businesses that handle sensitive financial information to maintain an information security program. We also urge the Commission to use its authority related to unfair and deceptive trade practices to continually challenge companies that fail to protect sensitive consumer information.

Audit Requirement Should Be Strengthened

Pursuant to the proposed consent agreement, BJ's Wholesale Club is required to obtain an independent third party assessment of its information security program within 180 days of the agreement, and every other year for the next 20 years. ACB believes the Commission has outlined an effective set of criteria for the information security audit/assessment process, however the biennial requirement should be reconsidered. We urge the Commission to require this assessment every year.

The Commission's complaint indicates that approximately eight million consumers have a valid membership relationship with BJ's Wholesale Club. Businesses that receive and maintain sensitive financial information on this scale should as a regular course of business more regularly review their information security measures. This is especially true in circumstances where an entity has failed to protect consumer information in the past. Twenty-four months between independent audits exposes an enormous amount of consumer data for far too long a period of time. ACB urges the Commission to require BJ's to obtain an annual independent information security audit consistent with the criteria established in the proposed consent agreement.

Card Company Enforcement Should Be More Aggressive/Transparent

Card associations such as VISA and MasterCard have specific requirements and rules for processing electronic transactions through their payments networks. These rules define how merchants should store transaction data, keep it secure, and share information with others involved in processing the payment. The associations' rules allow for the assessment of fines for failure to comply with the operating regulations, however the imposition of fines or other penalties is rarely made public. ACB believes that the associations need to be more aggressive in enforcing their operating rules and increase the level of enforcement actions. Additionally, ACB believes that the card association enforcement actions should be made public to create an effective deterrent for all entities involved in the payments system. Moreover, public disclosure of penalties will help the card associations demonstrate that (1) they are actively enforcing their rules; (2) that penalties are timely and appropriate; and (3) that the treatment of incidents is consistent.

A typical electronic payment transaction processed through the card association's networks involves a merchant, a card processor/software vendor that processes the transaction, an acquiring bank, and the consumer's bank (card issuer). Some type of contractual relationship exists between the merchant, payment processor, and the acquiring bank in order to facilitate access to the card association networks. The Federal Financial Institutions Examination Council ("FFIEC")[2] recently announced[3] that the federal banking agencies would look at the authority of bank regulators to examine card processors relationship with an acquiring bank pursuant to the Bank Service Company Act[4] to assess whether regulatory actions against an acquiring bank are

[2] Interagency group of federal banking regulators that includes: (1) the Federal Reserve; (2) the Federal Deposit Insurance Corporation; (3) the Office of the Comptroller of the Currency; (4) the Office of Thrift Supervision; and (5) the National Credit Union Administration.
[3] "Inquiry Begins on Credit Card Breach," New York Times (June 22, 2005).
[4] U.S.C. 12, Sec. 1861

appropriate. ACB commends the efforts of the FFIEC and urges the Commission to support this initiative through whatever formal or informal means available by sharing its experience and knowledge of problem entities with the federal banking regulators.

Monetary Penalties Should Be Considered

The Commission elected not to impose civil monetary penalties on BJ's Wholesale Club as part of the proposed settlement even though the Commission has the authority to seek redress in cases where consumers experienced economic harm. As outlined in the proposed settlement, BJ's Wholesale Club faces several lawsuits and outstanding claims related to their lack of information security controls.

ACB strongly believes that civil monetary penalties can be a significant incentive for businesses to protect sensitive consumer information. While it is difficult to quantify the precise, or approximated consumer harm in this situation, banks experienced real and quantifiable losses. These losses translate to more expensive products/services for consumers or the decision by management of a community bank that it will no longer offer a product. We urge the Commission to consider the complete economic impact in future settlements to impose fair and appropriate penalties.

Conclusion

ACB appreciates the Commission's efforts to challenge companies that fail to protect sensitive customer information. We look forward to working with the Commission to finalize this important precedent setting settlement. Should you have any questions, please contact the undersigned at 202-857-3121 or via email at cbahin@ACBankers.org, or Rob Drozdowski at 202-857-3148 or via e-mail at rdrozdowski@ACBankers.org.

Sincerely,

Charlotte M. Bahin
Senior Vice President
Regulatory Affairs