042 3160

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Deborah Platt Majoras, Chairman**
Thomas B. Leary
Pamela Jones Harbour
Jon Leibowitz

In the Matter of	)	
BJ's Wholesale Club, Inc., a corporation.	)	**DOCKET NO. C-4148**

COMPLAINT

The Federal Trade Commission, having reason to believe that BJ's Wholesale Club, Inc. ("Respondent") has violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent BJ's Wholesale Club, Inc. is a Delaware corporation with its principal office or place of business at One Mercer Road, Natick, Massachusetts 01760.

2. The acts and practices of Respondent as alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act.

3. Respondent operates approximately 150 warehouse clubs ("stores") in 16 eastern states. Generally, only consumers who have purchased memberships from Respondent may make purchases at its stores. Approximately 8 million consumers currently have valid memberships. At its stores, Respondent sells memberships as well as approximately 7,500 brand-name food and general merchandise items, including office supplies and equipment, consumer electronics, prerecorded media, small appliances, auto accessories and tires, jewelry, health and beauty aids, household needs, computer software, books, greeting cards, apparel, toys, tools, and seasonal items. Members often pay for such purchases with credit cards and debit cards.

4. Respondent uses computer networks to request and obtain authorization from the bank that issued the card ("issuing bank") for credit card and debit card purchases at its stores. To obtain authorization, Respondent collects information from the customer, including customer name, card number and expiration date, and certain other information (collectively, "personal information").

5. For a purchase at a store, Respondent typically collects the information from the magnetic stripe of the credit or debit card and compiles it into an authorization request on the computer network located in the store ("in-store computer network"). Respondent then transmits the information from the in-store computer network to its central datacenter and from there through outside computer networks to the issuing bank. Respondent receives the issuing bank's response through the same computer networks used to make the request.

6. Respondent also uses its in-store computer networks to manage inventory. Using wireless inventory scanners ("scanners"), Respondent collects inventory information at its stores. Respondent operates wireless access points on its in-store computer networks through which scanners connect and transmit inventory information to in-store computer networks.

7. From at least November 1, 2003, until February, 2004, Respondent did not employ reasonable and appropriate measures to secure personal information collected at its stores. Among other things, Respondent (1) did not encrypt the information while in transit or when stored on the in-store computer networks; (2) stored the information in files that could be accessed anonymously -- that is, using a commonly known default user id and password; (3) did not use readily available security measures to limit access to its computer networks through wireless access points on the networks; (4) failed to employ sufficient measures to detect unauthorized access or conduct security investigations; and (5) created unnecessary risks to the information by storing it for up to 30 days when it no longer had a business need to keep the information, and in violation of bank rules. As a result, a hacker could have used the wireless access points on an in-store computer network to connect to the network and, without authorization, access personal information on the network.

8. Beginning in late 2003 and early 2004, banks began discovering fraudulent purchases that were made using counterfeit copies of credit and debit cards the banks had issued to customers. The customers had used their cards at Respondent's stores before the fraudulent purchases were made, and personal information Respondent obtained from their cards was stored on Respondent's computer networks. This same information was contained on counterfeit copies of cards that were used to make several million dollars in fraudulent purchases. In response, banks and their customers cancelled and re-issued thousands of credit and debit cards that had been used at Respondent's stores, and customers holding these cards were unable to use their cards to access credit and their own bank accounts.

9. As described in Paragraphs 7 and 8 above, Respondent's failure to employ reasonable and appropriate security measures to protect personal information and files caused or is likely to cause substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers. This practice was an unfair act or practice.

10. The acts and practices of Respondent as alleged in this complaint constitute unfair acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a).

THEREFORE, the Federal Trade Commission this twentieth day of September, 2005, has issued this complaint against Respondent.

By the Commission.

Donald S. Clark
Secretary