

Analysis of Proposed Consent Order to Aid Public Comment
In the Matter of BJ's Wholesale Club, Inc. File No. 042 3160

The Federal Trade Commission has accepted, subject to final approval, a consent agreement from BJ's Wholesale Club, Inc. ("BJ's").

The consent agreement has been placed on the public record for thirty (30) days for receipt of comments by interested persons. Comments received during this period will become part of the public record. After thirty (30) days, the Commission will again review the agreement and the comments received, and will decide whether it should withdraw from the agreement and take appropriate action or make final the agreement's proposed order.

BJ's operates about 150 warehouse clubs ("stores") in 16 eastern states. BJ's is a membership club with about 8 million current members. Members often use credit and debit cards to pay for their purchases at BJ's. In the course of seeking approval for these credit and debit card purchases, BJ's collected members' personal information, including card number and expiration date and other information, from magnetic stripes on the cards.

The Commission's proposed complaint alleges that BJ's stored members' personal information on computers at its stores and failed to employ reasonable and appropriate security measures to protect the information. The complaint alleges that this failure was an unfair practice because it caused or was likely to cause substantial consumer injury that was not reasonably avoidable and was not outweighed by countervailing benefits to consumers or competition. In particular, the complaint alleges that BJ's engaged in a number of practices which, taken together, did not provide reasonable security for sensitive personal information, including: (1) failing to encrypt information collected in its stores while the information was in transit or stored on BJ's computer networks; (2) storing the information in files that could be accessed anonymously, that is, using a commonly known default user id and password; (3) failing to use readily available security measures to limit access to its networks through wireless access points on the networks; (4) failing to employ measures sufficient to detect unauthorized access to the networks or conduct security investigations; and (5) storing information for up to 30 days when BJ's no longer had a business need to keep the information, in violation of bank security rules.

The complaint further alleges that several million dollars in fraudulent purchases were made using counterfeit copies of credit and debit cards members had used at BJ's stores. The counterfeit cards contained the same personal information BJ's had collected from the magnetic stripes of members' credit and debit cards and then stored on its computer networks. After discovering the fraudulent purchases, banks cancelled and re-issued thousands of credit and debit cards members had used at BJ's stores, and members holding these cards were unable to use them to access credit and their own bank accounts.

The proposed order applies to personal information from or about consumers BJ's collects in connection with its business. It contains provisions designed to prevent BJ's from engaging in the future in practices similar to those alleged in the complaint.

Specifically, Part I of the proposed order requires BJ's to establish and maintain a comprehensive information security program in writing that is reasonably designed to protect the security, confidentiality, and integrity of personal information it collects from or about consumers. The security program must contain administrative, technical, and physical safeguards appropriate to BJ's size and complexity, the nature and scope of its activities, and the sensitivity of the personal information collected. Specifically, the order requires BJ's to:

- Designate an employee or employees to coordinate and be accountable for the information security program.
- Identify material internal and external risks to the security, confidentiality, and integrity of consumer information that could result in unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks.
- Design and implement reasonable safeguards to control the risks identified through risk assessment, and regularly test or monitor the effectiveness of the safeguards' key controls, systems, and procedures.
- Evaluate and adjust its information security program in light of the results of testing and monitoring, any material changes to its operations or business arrangements, or any other circumstances that BJ's knows or has to reason to know may have a material impact on the effectiveness of its information security program.

Part II of the proposed order requires that BJ's obtain within 180 days, and on a biennial basis thereafter, an assessment and report from a qualified, objective, independent third-party professional, certifying, among other things, that: (1) BJ's has in place a security program that provides protections that meet or exceed the protections required by Part I of the proposed order, and (2) BJ's security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of consumers' personal information has been protected.

Parts III through VII of the proposed order are reporting and compliance provisions. Part III requires BJ's to retain documents relating to its compliance with the order. Part IV requires dissemination of the order now and in the future to persons with responsibilities relating to the subject matter of the order. Part V requires BJ's to notify the Commission of changes in BJ's corporate status. Part VI mandates that BJ's submit compliance reports to the FTC. Part VII is a provision "sunsetting" the order after twenty (20) years, with certain exceptions.

The purpose of this analysis is to facilitate public comment on the proposed order. It is not intended to constitute an official interpretation of the proposed order to modify its terms in any way.