

Complaint

IN THE MATTER OF

BJ'S WHOLESALE CLUB, INC.

CONSENT ORDER, ETC., IN REGARD TO ALLEGED VIOLATIONS OF
SEC. 5 OF THE FEDERAL TRADE COMMISSION ACT

Docket C-4148; File No. 0423160

Complaint, September 20, 2005--Decision, September 20, 2005

This consent order, among other things, requires Respondent BJ's Wholesale Club, Inc. -- a membership club with approximately 8 million current members that operates approximately 150 warehouse stores in 16 Eastern states -- to establish and maintain a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information it collects from or about consumers. The consent order also requires the respondent, for twenty years, to secure biennial assessments and reports to ensure that its security program provides protections that meet or exceed the protections required by the order, and is sufficiently effective to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected.

Participants

For the Commission: *Alain Sheer, Jessica L. Rich, Joel Winston and Louis Silversin.*

For the Respondent: *David Medine and James W. Pendergast, Wilmer Cutler Pickering Hale and Dorr LLP*

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.

Complaint

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”),

Complaint

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.

Complaint

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 20th day of September, 2005, has issued this complaint against respondent.

Decision and Order

DECISION AND ORDER

The Federal Trade Commission having initiated an investigation of certain acts and practices of the Respondent named in the caption hereof, and the Respondent having been furnished thereafter with a copy of a draft Complaint that the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued by the Commission, would charge the Respondent with violation of the Federal Trade Commission Act, 15 U.S.C. § 45 et seq;

The Respondent, its attorney, and counsel for the Commission having thereafter executed an Agreement Containing Consent Order (“Consent Agreement”), an admission by the Respondent of all the jurisdictional facts set forth in the aforesaid draft Complaint, a statement that the signing of said Consent Agreement is for settlement purposes only and does not constitute an admission by Respondent that the law has been violated as alleged in such Complaint, or that the facts as alleged in such Complaint, other than jurisdictional facts, are true, and waivers and other provisions as required by the Commission's Rules; and

The Commission having thereafter considered the matter and having determined that it has reason to believe that the Respondent has violated the said Act, and that a Complaint should issue stating its charges in that respect, and having thereupon accepted the executed Consent Agreement and placed such Consent Agreement on the public record for a period of thirty (30) days, and having duly considered the comments filed thereafter by interested persons pursuant to Section 2.34 of its Rules, now in further conformity with the procedure described in Section 2.34 of its Rules, the Commission hereby issues its Complaint, makes the following jurisdictional findings and enters the following Order:

1. Proposed 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.

Decision and Order

2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the Respondent, and the proceeding is in the public interest.

ORDER**DEFINITIONS**

For purposes of this order, the following definitions shall apply:

1. “Personal information” shall mean individually identifiable information from or about an individual consumer including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name that reveals an individual’s email address; (d) a telephone number; (e) a Social Security number; (f) credit and/or debit card information, including credit and/or debit card number, expiration date, and data stored on the magnetic stripe of a credit or debit card; (g) a persistent identifier, such as a customer number held in a “cookie” or processor serial number, that is combined with other available data that identifies an individual consumer; or (h) any other information from or about an individual consumer that is combined with (a) through (g) above.

2. Unless otherwise specified, “respondent” shall mean BJ’s Wholesale Club, Inc. and its successors and assigns, officers, agents, representatives, and employees.

3. “Commerce” shall mean as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.

I.

IT IS ORDERED that respondent, directly or through any corporation, subsidiary, division, or other device, in connection

Decision and Order

with the advertising, marketing, promotion, offering for sale, or sale of any product or service, in or affecting commerce, shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers, including:

- A. the designation of an employee or employees to coordinate and be accountable for the information security program.
- B. the identification of material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures.
- C. the design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures.

Decision and Order

D. the evaluation and adjustment of respondent's information security program in light of the results of the testing and monitoring required by subparagraph C, any material changes to respondent's operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its information security program.

II.

IT IS FURTHER ORDERED that respondent obtain an assessment and report (an "Assessment") from a qualified, objective, independent third-party professional, using procedures and standards generally accepted in the profession, within one hundred and eighty (180) days after service of the order, and biennially thereafter for twenty (20) years after service of the order that:

- A. sets forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained during the reporting period;
- B. explains how such safeguards are appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers;
- C. explains how the safeguards that have been implemented meet or exceed the protections required by Paragraph I of this order; and
- D. certifies that respondent's security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected and, for biennial reports, has so operated throughout the reporting period.

Each Assessment shall be prepared by a person qualified as a

Decision and Order

Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580. Respondent shall provide the first Assessment, as well as all: plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, whether prepared by or on behalf of respondent, relied upon to prepare such Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by respondent until the order is terminated and provided to the Associate Director of Enforcement within ten (10) days of request.

III.

IT IS FURTHER ORDERED that respondent shall maintain, and upon request make available to the Federal Trade Commission for inspection and copying, a print or electronic copy of each document relating to compliance, including but not limited to:

A. for a period of five (5) years: any documents, whether prepared by or on behalf of respondent, that contradict, qualify, or call into question respondent's compliance with this order; and

B. for a period of three (3) years after the date of preparation of each biennial Assessment required under Paragraph II of this order: all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, whether prepared by or on behalf of respondent, relating to

Decision and Order

respondent's compliance with Paragraphs I and II of this order for the compliance period covered by such biennial Assessment.

IV.

IT IS FURTHER ORDERED that respondent shall deliver a copy of this order to all current and future principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having managerial responsibilities relating to the subject matter of this order. Respondent shall deliver this order to such current personnel within thirty (30) days after service of this order, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities.

V.

IT IS FURTHER ORDERED that respondent shall notify the Commission at least thirty (30) days prior to any change in the corporation that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in either corporate name or address. *Provided, however,* that, with respect to any proposed change in the corporation about which respondent learns less than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. All notices required by this Paragraph shall be sent by certified mail to the Associate Director, Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

Decision and Order

VI.

IT IS FURTHER ORDERED that respondent shall, within one hundred and eighty (180) days after service of this order, and at such other times as the Commission may require, file with the Commission an initial report, in writing, setting forth in detail the manner and form in which it has complied with this order.

VII.

This order will terminate twenty (20) years from the date of its issuance, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

A. any Paragraph in this order that terminates in less than twenty (20) years;

B. this order's application to any respondent that is not named as a defendant in such complaint; and

C. this order if such complaint is filed after the order has terminated pursuant to this Paragraph.

Provided, further, that if such complaint is dismissed or a federal court rules that respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Paragraph as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

Analysis

Analysis of Proposed Consent Order to Aid Public Comment

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

Analysis

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,

Analysis

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.

Analysis

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.

Complaint

IN THE MATTER OF

NOVARTIS AG

CONSENT ORDER, ETC., IN REGARD TO ALLEGED VIOLATIONS OF
SEC. 7 OF THE CLAYTON ACT AND SEC. 5 OF THE FEDERAL TRADE
COMMISSION ACT*Docket C-4150; File No. 0510106**Complaint, September 21, 2005--Decision, September 21, 2005*

This consent order addresses the acquisition by Respondent Novartis AG of Eon Labs, Inc., from Santo Holding AG. The order, among other things, requires the respondent -- through Sandoz, Inc., its generic pharmaceuticals division -- to divest to Amide Pharmaceutical, Inc. the Eon assets necessary to manufacture and market generic desipramine hydrochloride tablets (a tricyclic antidepressant), and the Sandoz assets necessary to manufacture and market orphenadrine citrate ER tablets (a muscle relaxant) and rifampin oral capsules (one of several drugs used in a multi-drug approach to treating tuberculosis) in the United States. The order also requires Novartis, through Sandoz, to enter into a supply agreement with Amide to enable Amide to market these products until Amide obtains Food and Drug Administration ("FDA") approval to manufacture the products itself, and to provide technology transfer assistance to enable Amide to obtain all necessary FDA approvals as quickly as possible.

Participants

For the Commission: *Elizabeth A. Jex, David L. Inglefield, Richard A. Levy, Jeanna L. Composti, Clare E. Jones, Michael R. Moiseyev and Mark Hertzendorf.*

For the Respondent: *Kenneth S. Prince, Shearman & Sterling LLP*

COMPLAINT

Pursuant to the Federal Trade Commission Act and the Clayton Act, and by virtue of the authority vested in it by said Acts, the Federal Trade Commission ("Commission"), having reason to believe that Respondent Novartis AG ("Novartis"), a corporation subject to the jurisdiction of the Commission, has offered to acquire 67% of the outstanding shares of Eon Labs, Inc., a corporation subject to the jurisdiction of the Commission, from