Privacy Law Advisory

JUNE 21, 2005

KELLEY DRYE
COLLIER SHANNON

FTC Settles Landmark Data Security Breach Case with BJ's Wholesale Club – Marks the First Time the FTC Has Brought A Data Security Case Based on Unfairness Rather Than Deception

EXECUTIVE SUMMARY

On the heels of a recent Senate hearing that focused on how Federal Trade Commission ("FTC") representatives viewed pending legislation concerning data security breaches, the FTC has made headlines of its own with a recent settlement agreement for a security breach based on unfairness grounds.

BJ's Wholesale Club, Inc. ("BJ's")[1] was found to have violated the FTC Act by not providing adequate security for its customer data. This case represents the first time that the FTC has alleged a violation of Section 5 of the FTC Act solely for a business's failure to maintain appropriate safeguards of sensitive personal information. By contrast, previous FTC data security cases have focused on a representation about security in a business's privacy policy or other consumer communication, demonstrated that the representation was false, and alleged that the business had therefore engaged in deception in violation of Section 5. These deception allegations were noticeably absent in this case.

THE FTC CASE AGAINST BJ'S

Background

At the end of last week, BJ's agreed to settle FTC charges that its failure to take appropriate security measures to protect the sensitive information of thousands of its customers was an unfair practice that violated Section 5 of the FTC Act. The FTC alleged that the personal customer data was used by an unauthorized person or persons to make millions of dollars of fraudulent purchases. The settlement will require BJ's to implement a comprehensive information security program and obtain audits by an independent third party security professional every other year for twenty years.

[1] A Massachusetts-based company, BJ's operates 150 warehouse stores and 78 gas stations in 16 states in the Eastern United States. Approximately 8 million consumers are currently members with net sales totaling about $6.6 billion in 2003.

Compliant: Unfair Practices

According to the FTC's complaint, BJ's uses a computer network to obtain bank authorization for credit and debit card purchases and to track inventory. For credit and debit card purchases at its stores, BJ's collects information – such as the customer's name, card number, and expiration date – from the magnetic stripe on the back of the cards. The information is sent from the computer network in the store to BJ's central data-center computer network, and then through outside computer networks to the bank that issued the card.

The FTC charged that BJ's engaged in a number of practices that, collectively, did not provide reasonable security for sensitive customer information. Specifically, the FTC alleged that BJ's:

- Failed to encrypt consumer information when it was transmitted or stored on computers in BJ's stores;
- Created unnecessary risks to the information by storing it for up to 30 days in violation of bank security

rules, even when it no longer needed the information;

- Stored the information in files that could be accessed anonymously by using commonly-known default user IDs and passwords;
- Failed to use readily available security measures to prevent unauthorized wireless connections to its networks; and
- Failed to use measures sufficient to detect unauthorized access to the networks or to conduct security investigations.

The FTC's complaint charged that fraudulent purchases were made using counterfeit copies of credit and debit cards used at BJ's stores, and that the counterfeit cards contained the same personal information that BJ's had collected from the magnetic stripes of the cards.

Outcome of Fraudulent Purchases

After the fraud was discovered, banks cancelled and re-issued thousands of credit and debit cards, and consumers had to resolve the affected cards. Banks and credit unions have filed lawsuits against BJ's and pursued bank procedures seeking the return millions of dollars in fraudulent purchases and operating expenses. As of May 2005, the amount of outstanding claims against BJ's was approximately $13 million.

WHAT THIS MEANS GOING FORWARD

FTC Analysis

Amidst growing concern by consumers and legislatures over unending reports of data breaches, this case represents the FTC's willingness to test the bounds of its current enforcement power to go after companies for failing to enact sufficient safeguards to protect customer personal data.

Deborah Platt Majoras, Chairman of the FTC, described the case as "demonstrating our intention to challenge companies that fail to protect adequately consumers' sensitive information." She explained further that "consumers must have the confidence that companies that possess their confidential information will handle it with due care and appropriately provide for its security."

This case is a significant departure from past security data cases because it does not identify any false representation by BJ's. Instead, it focuses exclusively on the adequacy of BJ's security practices, which the FTC alleges to be unfair (as opposed to deceptive) under the FTC Act.

Pursuant to the elements of an unfairness cause of action, the FTC alleged that BJ's security practices resulted in: (1) substantial injury to consumers; (2) which was not reasonably avoidable by consumers; and (3) was not offset by any countervailing benefit to consumers or to competition generally.

It is also important to note that this case was not brought pursuant to the Gramm-Leach-Bliley Act ("GLBA"). As FTC officials have been warning industry for some time, the Commission now appears to be applying the standards of the GLB Safeguards Rule to the safeguarding of sensitive information generally, and not just to sensitive financial information that is expressly regulated under the GLBA and the GLB Safeguards Rule. Accordingly, the FTC may apply this same theory of liability to any business that uses, discloses, and maintains personal data – such as personal health information, Social Security numbers, and consumer credit and debit cards – and the manner in which such businesses are safeguarding this sensitive data.

Steps Businesses Should Take

If they have not already begun, businesses should start taking inventory of their business practices surrounding the collection, use, and storage of sensitive personal data (both customer and employee data) and determine whether the safeguards in place are sufficient to protect such data from unauthorized use, disclosure, and system breaches.

The BJ's case demonstrates that, in addition to keeping abreast of state and federal data security pending legislation and enacted laws, businesses should be mindful that the FTC may become more active in data security enforcement against all businesses that use and maintain personal data.

KELLEY DRYE COLLIER SHANNON

ADVERTISING AND MARKETING LAW PRACTICE GROUP

Kelley Drye Collier Shannon's Advertising & Marketing practice comprises attorneys with proven success in advertising litigation and NAD proceedings; expertise in the area of advertising, promotion marketing, and privacy law; and experience at the FTC, FDA, and the Offices of State Attorneys General. We help leading companies identify risks, respond effectively to inquiries, and prevail in contested proceedings.

We are a leader in advising clients on information privacy issues and have been at the forefront of developments in this growing area of law. Our privacy law group regularly advises clients regarding all aspects of privacy law, including the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, the Health Insurance Portability and Accountability Act, the Children's Online Privacy Protection Act, the EU Data Protection Directive (as well as EU members' state laws and the Safe Harbor negotiated between the US and the EU), the FTC Act, and state privacy laws.

GOVERNMENT RELATIONS AND PUBLIC POLICY PRACTICE GROUP

Our Government Relations practice helps clients interpret and shape governing laws, enabling them to maintain or achieve market leadership. Our experienced privacy attorneys work closely with our Government Relations and Public Policy practice group to stay abreast of new laws and regulations.

FOR MORE INFORMATION

Kelley Drye Collier Shannon is on the forefront of developing privacy industry guidelines and regulations. For more information, or if you would like to receive our daily privacy e-newsletter, please visit www.kelleydrye.com.

If you have any questions about this alert, please feel free to contact one of our team members at (202) 342-8400 or via email:

Partners

Bill MacLeod wmacleod@kelleydrye.com
Lewis Rose lrose@kelleydrye.com
John Villafranco jvillafranco@kelleydrye.com

Special Counsel

Julie G. O'Neill joneill@kelleydrye.com

Associates

Christie Grymes cgrymes@kelleydrye.com
Jeff Kauffman jkauffman@kelleydrye.com
Gonzalo Mon gmon@kelleydrye.com
Elisa Nemiroff enemiroff@kelleydrye.com
Dustin Painter dpainter@kelleydrye.com
Alysa Zeltzer azeltzer@kelleydrye.com