Privacy Law Advisory

KELLEY DRYE
COLLIER SHANNON

ChoicePoint: Latest FTC Data Security Case Produces the Largest Civil Penalty in FTC History

At the end of January 2006, the Federal Trade Commission ("FTC" or "Commission") obtained a $15 million settlement with a leading data broker, ChoicePoint, Inc. ("ChoicePoint"), for its alleged mishandling of sensitive consumer information. The settlement is based on the FTC's charges that ChoicePoint violated the Fair Credit Reporting Act ("FCRA") by furnishing consumer reports to unauthorized third-parties, and violated the FTC Act's prohibition on unfair or deceptive acts or practices with respect to its data security practices and representations.

The action against ChoicePoint is one of a series of data security cases brought by the FTC in the last few years and signals the Commission's continued scrutiny of businesses' receipt, use, and disclosure of consumers' personal information, and whether such practices are reasonably protecting consumers' personal information. Unlike the previous FTC data security cases, which did not require monetary payments, in ChoicePoint, the Commission secured a $10 million civil penalty pursuant to the FCRA, and a $5 million consumer redress award.

PRIOR TO CHOICEPOINT

Lately, consumer data security has taken on increasing importance to the FTC. Starting with an action against Eli Lilly & Co., the FTC brought five actions against companies for deceptive security claims between May 2002 and March 2005. All of these actions involved companies making explicit or implicit claims regarding their security or privacy policies which the FTC alleged the companies failed to fulfill. All of the five cases were brought under the FTC's deceptive acts or practices authority. The consent orders required the companies to implement comprehensive information security programs to conform with the standards of the Gramm-Leach-Bliley Act ("GLBA").

Last summer, the FTC changed course and decided to broaden its pursuit beyond allegedly deceptive descriptions of privacy policies. In June 2005, the FTC Chairman testified to Congress that companies' failures to employ proper safeguards could be regarded as unfair acts or practices under the FTC Act. The same day, the FTC announced that it had settled a case against BJ's Wholesale Club, Inc. ("BJ's"), a retailer, for not providing adequate security for its customer data, which allegedly allowed a data breach. Surprisingly, that case did not involve allegations of deceptive representations about BJ's privacy or security practices, as was routine in the Commission's previous data security cases; instead the FTC charged that BJ's failure to maintain appropriate safeguards was unfair, in violation of Section 5 of the FTC Act.

The BJ's settlement resulted in the retailer agreeing to implement comprehensive information security programs and to submit to audits every other year for 20 years by an independent thirdparty security professional. Despite the use of the unfairness authority in BJ's, the settlement

did not result in monetary penalty.

THE FTC CASE AGAINST CHOICEPOINT

Background on the FTC's Investigation and Complaint

ChoicePoint[1] is a data broker that furnishes consumers' personal information, including their names, Social Security numbers, birth dates, and credit histories to subscribers. ChoicePoint's subscribers include insurance companies, landlords, banks, private investigators, and debt collectors. The company announced in early 2005 that it may have disclosed the personal information of 163,000 consumers to ChoicePoint subscribers who lacked a permissible purpose for obtaining the information. According to the FTC's complaint, some of the subscribers submitted applications that were obviously questionable because they used false credentials, used fax machines at public locations to send multiple applications and/or used commercial mail drops as business addresses. Although there was no "breach" in the sense that no data was stolen, the FTC alleged that at least 800 cases of identity theft occurred as a result of this lapse in security policy.

As a result of these unauthorized disclosures, the FTC charged that ChoicePoint violated the "unfairness" prong of the FTC Act, as in its case against BJ's. In large part, the FTC focused on the company's failure to screen potentially unreliable subscribers before it shared sensitive consumer information with them, thus making such consumer information vulnerable to identity theft. The company's role in permitting relatively easy access to consumer data is factually similar to the BJ's case. The key difference with this case involves the additional FCRA violations: because some ChoicePoint subsidiaries furnished credit reports, the FTC brought two charges under the FCRA, which opens the door to significant civil monetary penalties.

Among other things, the FCRA regulates any entity that supplies persons or entities with consumer reports. The Act prohibits the furnishing of consumer reports to those who lack a permissible purpose for obtaining them. The FCRA also requires a consumer reporting agency to maintain reasonable procedures to ensure that it furnishes consumer reports only for permissible purposes. Each breach of the FCRA can result in a civil monetary penalty of up to $2,500 per violation.

Complaint: Violation of the FCRA and Unfair and Deceptive Practices Under the FTC Act

The FTC brought four charges against ChoicePoint, two undereach law.

Charges under the FCRA:

- Failing to maintain reasonable procedures to limit the furnishing of consumer reports except for permissible purposes and failing to make reasonable efforts to verify the identity of each new user of the consumer information; and
- Furnishing consumer reports to subscribers who lacked a permissible purpose for obtaining the reports.

Charges under the FTC Act:

- Failing to use reasonable and appropriate measures to secure the personal information ChoicePoint collected for sale. The FTC alleged that these inadequate security measures constituted an "unfair" act or practice because they either caused or were likely to cause a substantial consumer injury that was not reasonably avoidable

[1] A publicly-traded company based in Alpharetta, Georgia, ChoicePoint collects, stores, analyzes and delivers consumer data to its more than 50,000 subscribers.

by consumers and was not offset by any countervailing benefit to consumers or to competition generally; and

• Falsely representing that ChoicePoint had implemented reasonable and appropriate privacy policies to maintain and protect the confidentiality and security of consumers' personal information. The FTC alleged that ChoicePoint's privacy policy was misleading or deceptive.

There is no denying that the ChoicePoint and BJ's cases mark a significant departure from the Commission's approach to information security prior to June 2005. Previously, the FTC pursued data security cases where businesses allegedly made inaccurate or deceptive representations (usually in their privacy policies) about their information security practices; these earlier cases did not involve allegations based on the FTC Act's "unfairness" prong.

EXPLANATION OF THE CHOICEPOINT SETTLEMENT

Just as in previous data security case settlements, the ChoicePoint settlement requires the company to institute measures to prevent future data breaches and unauthorized access to consumer information but the two counts brought under the FCRA enabled the FTC to demand a substantial monetary settlement as well.

Civil Penalty: ChoicePoint agreed to pay $10 million in civil penalties, the largest civil penalty ever received by the FTC.

• Note that the FCRA actually allows a penalty of $2500 per violation and if all 163,000 violations were proved, ChoicePoint theoretically could have been liable for a civil penalty of more than $400 million.

Consumer Redress: ChoicePoint agreed to pay $5 million in

equitable relief.

Business Practices: ChoicePoint agreed to a variety of new procedures to more effectively protect consumer information including:

• Verifying the identity of businesses that apply to receive consumer reports by a variety of means depending on the applicant;

• Ensuring that subscribers are using the data they receive for a permissible purpose via means such as audits of the subscriber by an independent third party; and

• Terminating the subscription of any subscriber that ChoicePoint learns has obtained a consumer report for any purpose other than a permissible purpose.

Information Security Program ChoicePoint agreed to implement and maintain a comprehensive security program reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers.

Assessment Requirement: ChoicePoint agreed to obtain every two years, for the next 20 years, an audit from a qualified, independent, third-party professional to ensure that its security program meets the standards of the settlement.

Compliance Monitoring and Reporting: ChoicePoint agreed to:

• Allow the FTC to monitor compliance with the order indefinitely;

• Submit compliance reports for the next 20 years; and

• Create and retain detailed records on its

subscribers and any consumer complaints for the next six years.

WHAT THIS MEANS GOING FORWARD

FTC Scrutiny

ChoicePoint represents the Commission's continuing use of its unfairness authority to compel businesses to safeguard consumers' personal data. One Commissioner recently described the settlement to Congress as a "strong signal to industry that it must maintain reasonable procedures for safeguarding sensitive consumer information and protecting it from data thieves."[2]

The addition of the FCRA to the FTC's arsenal when prosecuting actions where consumer reports are involved demonstrates the Commission's willingness to continue to go beyond the simple prosecution of deceptive privacy policies. Moreover, the receipt of a monetary penalty for a data security violation under the FCRA makes it all the more likely that the Commission will seek monetary damages in similar circumstances in the future.

Accordingly, the FTC may apply its unfairness theory of liability to any business within its jurisdiction (i.e., most businesses) that uses, discloses, and maintains sensitive personal data – such as personal health information, Social Security numbers, and consumer credit and debit card account numbers – in a way that the FTC determines is unreasonable and/or exposes consumers to identify theft. Furthermore, businesses subject to the FCRA that directly (or through subsidiaries) furnish consumer reports to entities that do not have a permissible purpose to receive such information also could be liable under the FCRA.

Best Practices

Privacy and data security compliance, more than ever, should be a priority for all businesses. At its most basic level, this means:

- Take inventory of your current business practices concerning the collection, use, storage, and sharing of sensitive personal data (both customer and employee data).
- Determine whether the safeguards in place are sufficient to protect consumer data from unauthorized use, disclosure, and system breaches.

It is vital that reasonable procedures are created and maintained by all companies handling sensitive consumer information, including contractors and affiliates. Likewise, in addition to keeping abreast of legal developments at both the state and federal levels, firms should monitor whether their safeguards are dynamic and reflect changing technology and risk assessments.

The ChoicePoint case demonstrates that all firms should be particularly vigilant in regard to their obligations to safeguard data when entering into agreements to transmit or receive sensitive consumer information to or from another business entity. With the ChoicePoint settlement, the FTC has shown that it intends to stay aggressive in data security enforcement. While updating your firm's privacy and security practices will require time and resources, those factors pale in comparison to the costs and obligations of an FTC consent order.

ABOUT OUR ADVERTISING AND MARKETING PRACTICE

Collier Shannon Scott's Advertising & Marketing practice comprises attorneys with

[2] *Phone Records for Sale: Why Aren't Phone Records Safe from Pretexting? Before the H. Comm. on Energy & Commerce,* 109th Cong. (Feb. 1, 2006) (statement of John Liebowitz, Comm'r, Federal Trade Commission).

proven success in advertising litigation and NAD proceedings; expertise in the area of advertising, promotion marketing, and privacy and data security 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 and data security 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 and data security laws.

ABOUT OUR GOVERNMENT RELATIONS AND PUBLIC POLICY PRACTICE

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:

Members

William C. MacLeod	wmacleod@kelleydrye.com
Lewis Rose	lrose@kelleydrye.com
John E. Villafranco	jvillafranco@kelleydrye.com

Of Counsel

Julie G. O'Neill	joneill@kelleydrye.com

Associates

Ponneh Aliabadi	paliabadi@kelleydrye.com
Christie Grymes	cgrymes@kelleydrye.com
Jeffrey A. Kauffman	jkauffman@kelleydrye.com
Jason Levine	jlevine@kelleydrye.com
Gonzalo Mon	gmon@kelleydrye.com
Elisa A. Nemiroff	enemiroff@kelleydrye.com
Dustin Painter	dpainter@kelleydrye.com
Alysa N. Zeltzer	azeltzer@kelleydrye.com