Louisville
BAR BRIEFS
The Newspaper of the Louisville Bar Association

The New Unfair Trade Practice

Failing to Take Reasonable Precautions to Protect Sensitive Customer Information

by Martha Andes Ziskind

On February 23, 2006, the Federal Trade Commission announced the ninth in a series of settlements with companies whose allegedly inadequate information security practices have resulted in the compromise of confidential personal information. The settlement with CardSystems Solutions, Inc. (CardSystems) is the third case where the FTC has charged that failure to take reasonable precautions to protect customer information constitutes an unfair trade practice in violation of Section 5 of the FTC Act. Practices are "unfair" if they cause or are likely to cause consumers substantial injury that is neither reasonably avoidable by the consumers nor outweighed by countervailing benefits to consumers or competition (15U.S.C.45(n)). The settlement agreements, as well as speeches by FTC Commissioners, may be found on the FTC's website, *www.ftc.gov*.

CardSystems Solutions

CardSystems was in the business of providing merchant debit and credit card authorizations for more than 119,000 small and mid-size merchants. The company used the Internet and a web application program to provide information to client merchants about authorizations performed for them. In September 2004, a computer hacker used a Structured Query Language (SQL) injection attack on the CardSystems web application and website to install programs that collected and transmitted customer debit and credit card magnetic stripe information stored on the company's network. Using the magnetic stripe information, the hackers were able to counterfeit cards and engage in numerous fraudulent transactions. Once the card-issuing banks became aware of the frauds, they cancelled and reissued thousands of credit and debit cards, causing great inconvenience to the consumers whose cards were cancelled.

CardSystems was in the "customer information" business, but the two other companies that have agreed to unfair trade practices settlements are retailers: BJ's Wholesale Club, which operated warehouse stores and gas stations in the Eastern United States, and DSW, Inc., a Columbus, Ohio-based shoe discounter that operated 190 stores in 32 states. None of these companies had special federal privacy obligations as financial institutions or health care providers, nor had they made representations to the public as to their customer information privacy practices.

BJ's Wholesale Club

BJ's used a computer network to obtain bank authorizations for credit and debit card purchases and a WiFi system to connect its on-premise computers with instore inventory systems. The FTC alleged that BJ's engaged in a number of practices, which, taken together, amounted to a failure to take reasonable security precautions for sensitive customer information. For example, BJ's failed to encrypt customer information when it was transmitted or stored on computers in BJ's stores; 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.

DSW

DSW also used a wireless system to transmit magnetic stripe information and customer check and ID information to an in-house computer network and from there to the appropriate financial institution or check processor. Among the practices cited by the FTC as constituting a failure to take reasonable and appropriate security measures to protect sensitive customer information were: storing information in multiple files beyond the time period where there was a business need to keep the information; failing to use readily available measures to limit wireless access to its computer networks; storing information in unencrypted files that could be easily accessed; and failure to employ sufficient means to detect unauthorized access.

All three companies agreed to establish and maintain a comprehensive information security program that includes administrative, technical and physical safeguards for customer information, a requirement imposed statutorily on financial institutions and health care providers. Each also agreed to obtain, every two years for the next 20 years, an independent third party audit of its compliance with the FTC's order.

The FTC has become the principal federal agency concerned with the growing problem of identity theft. As Chairman Deborah Platt Majors stated at a program sponsored by the California Department of Consumer Affairs on the same day as the announcement of the CardSystems settlement, the purpose of the actions against companies that fail to adequately protect customer information "is to create a culture of security for sensitive information so that businesses prevent breaches and identity theft." She emphasized that the FTC does not require perfect information security but that "a company's data security be reasonable in light of the nature of its business and the sensitivity of the information it handles." This is the message that attorneys who counsel businesses and nonprofits that handle sensitive personal information should deliver to their clients.

Martha Andes Ziskind is Of Counsel to Wyatt, Tarrant & Combs. She was formerly chief market counsel for PNC Bank's Kentucky-Indiana Market. ■