UT LAW CLE THE UNIVERSITY OF TEXAS SCHOOL OF LAW

PRESENTED AT

2016 Essential Cybersecurity Law

Ausgust 19, 2016
Austin, Texas

Top 10 Myths About Cybersecurity

Part I

Gavin George

Phong Tran

Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Franchisors Must Find The Right Data Security Balance


Gavin George


Marc Legrand

Law360, New York (August 21, 2015, 10:23 AM ET) -- In recent years, a number of franchisors have fallen victim to data breaches, including Jimmy John's,[1] Dairy Queen,[2] The UPS Store,[3] Wyndham and SuperValu.[4] Between lost goodwill, the cost of investigating and responding to the breach, private lawsuits, and government enforcement actions, it's no surprise that such data breaches are expensive. In 2014, the Ponemon Institute estimated that U.S. organizations paid an average of $5.9 million dollars per data breach.[5]

Franchisors strive to avoid liability for the acts and omissions of individual franchisees, including acts or omissions that contribute to data breaches. That motivation, however, is in tension with the franchisor's desire to exert sufficient control over franchisees to protect its brand from reputational harm. After a data breach, affected plaintiffs or the Federal Trade Commission may attempt to establish the franchisor's liability by proving that the franchisor wielded a substantial level of control over the franchisee's day-to-day operations, especially the particular aspects most related to the breach.

For example, many data breaches affecting franchised establishments have been attacks on point-of-sale vendors' systems, including the recent breach affecting Jimmy John's. Breaches of POS vendors often involve the use of stolen credentials to remotely access the affected system and upload malicious software to harvest customer information including credit card numbers. Franchisors typically prescribe the particular POS vendor its franchisees must use. As in other situations, such increased franchisor control and increased franchisor liability can go hand-in-hand.[6]

With that in mind, savvy franchisors can adopt certain strategies to ensure reasonable levels of data security by their franchisees, to maintain some level of protection from liability in the case of data breach of a franchisee system, and to retain effective control over the response to a breach.

Franchisor Liability: FTC Enforcement and Private Suits

Over the past decade, the FTC has started pursuing enforcement actions against certain companies that have suffered a data breach. In June 2005, BJ's Wholesale Club Inc. was one of the first companies to settle FTC charges based on its alleged "failure to take appropriate security measures to protect the sensitive information of ... its customers."[7] The FTC often considers the failure to protect consumer data an unfair trade practice in violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a).[8] Specifically, the FTC alleged that BJ's "[failed] to encrypt consumer information when it was transmitted or stored on computers in BJ's stores; [stored] the information in files that could be accessed using commonly known default user IDs and passwords; [and failed] to use readily available security measures to prevent unauthorized wireless connections to its networks."[9] Since that first settlement, the FTC has brought similar accusations against numerous other companies, including franchisors.

Also available as part of the eCourse
2016 Essential Cybersecurity Law eConference

First appeared as part of the conference materials for the
2016 Essential Cybersecurity Law session
"Top 10 Myths About Cybersecurity"