PRESENTED AT

2018

ESSENTIAL CYBERSECURITY LAW

July 25, 2018

Norris Conference Center – CityCentre ■ Houston, Texas

Cybersecurity Regulation and Enforcement

Moderator:

Richard J. Johnson, Jones Day, Dallas, TX

Panelists:

Michael Chu, U.S. Department of Justice, Houston, TX

Jim Elliott, Federal Trade Commission, Dallas, TX

Scott Mascianica, U.S. Securities and Exchange Commission, Fort Worth, TX

Jim Elliott
Assistant Regional Director
Southwest Region
Federal Trade Commission
Dallas, TX

jelliott@ftc.gov
214.979.9373

2018
ESSENTIAL CYBERSECURITY LAW
July 25, 2018 ■ Norris Conference Center – CityCentre ■ Houston, Texas

Jim Elliott[1]
Assistant Regional Director
Federal Trade Commission
Southwest Region

For many companies, collecting sensitive consumer and employee information is an essential part of doing business. It's the company's legal responsibility to take steps to properly secure or dispose of it. Financial data, personal information from kids, and material derived from credit reports may raise additional compliance considerations. In addition, the company may have legal responsibilities to victims of identity theft. Regardless of the size of the company or its line of work, the FTC has compliance resources.

I. Financial Impact

A. Financial Losses Stemming from the Breach

1. The Bureau of Justice Statistics estimates that 16.6 million persons – or 7 percent of all U.S. residents ages 16 and older – were victims of identity theft in 2012. Bureau of Justice Statistics, Victims of Identity Theft, 2012 (Dec. 2013), available at http://www.bjs.gov/content/pub/pdf/vit12.pdf.

2. In *FTC v. Wyndham Worldwide Corp.,* No. 13-1887 (ES) (D.N.J.), FTC alleged that from the three separate intrusions, there was a compromise of more than 619,00 consumer payment card accounts, the exportation of many of those account numbers to a domain registered in Russia, fraudulent charges on many consumers' accounts, and more than $10.6 million in fraud loss.

B. Data Recovery and Response Plan Costs

1. Target – more than $61 million in expenses related to the breach

C. Customer Relations

1. Involving physical injury, economic injury, unwarranted intrusions

2. Trust issue, examples

a. Companies receive complaints from consumers who had been surreptitiously tracked and targeted with prescription drug offers and other health-related materials regarding sensitive medical conditions.

[1] The views expressed in these remarks are my own and do not necessarily reflect the views of the Federal Trade Commission, any individual Commissioner, or the Bureau of Consumer Protection.

b. Unexpected revelation of previously private information, including both sensitive information (e.g., health information, precise geolocation information) and less sensitive information (e.g., purchase history, employment history) to unauthorized third parties.

c. One FTC matter against Google alleged that the company used deceptive tactics and violated its own privacy promises when it launched Google Buzz, even in the absence of such misrepresentations, revealing previously-private consumer data could cause consumer harm. *See* Press Release, FTC, FTC Charges Deceptive Privacy Practices in Google's Rollout of its Buzz Social Network (Mar. 30, 2011), available at http://www.ftc.gov/opa/2011/03/google.shtm (noting that in response to the Buzz launch, Google received thousands of complaints from consumers who were concerned about public disclosure of their email contacts which included, in some cases, ex-spouses, patients, students, employers, or competitors).

d. A survey shows that consumers feel better about brands that give them transparency and control over advertisements. *See* RESEARCH: Consumers Feel Better About Brands That Give Them Transparency and Control Over Ads, Evidon Blog (Nov. 10, 2010), http://blog.evidon.com/tag/better-advertising ("when advertisers empower consumers with information and control over the ads they receive, a majority feels more positive toward those brands, and 36% even become more likely to purchase from those brands").

e. Intuit, Inc. conducted a study showing that making its customers aware of its privacy and data security principles – including restricting the sharing of customer data, increasing the transparency of data practices, and providing access to the consumer data it maintains – significantly increased customer trust in its company. *See* Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers (Mar. 2012), available at http://www.ftc.gov/os/2012/03/120326privacyreport.pdf, Comment of Intuit, Inc. , cmt. #00348, at 6-8 ("The more transparent (meaning open, simple and clear) the company is, the more customer trust increases. . . .").

Title search: Cybersecurity Regulation and Enforcement

First appeared as part of the conference materials for the
2018 Essential Cybersecurity Law session
"Cybersecurity Regulation and Enforcement"