ADVISEN
Insurance Intelligence

THE FTC:

WHAT YOU NEED TO KNOW ABOUT ONE OF THE MOST RELENTLESS FEDERAL CYBER REGULATORS

Sponsored by:

ALLIED WORLD

JUNE 2015

The FTC: What you need to know about one of the most relentless federal cyber regulators

"Although the President's proposed legislation has yet to be authorized by Congress, the FTC already has a reputation as one of the most aggressive cybersecurity regulators, especially in recent years"

Josh Ladeau, Practice Lead - Privacy & Network Security, Allied World

The Federal Trade Commission (FTC) has made an aggressive push to expand its privacy and network security-related regulatory authorities and to force companies with lax security programs to bolster their defenses. This report examines the FTC's initiatives, explains the implications for companies, and discusses risk management and insurance options.

Overview: FTC Initiatives

Data breaches are expensive. A breach can expose an organization to mitigation costs, notification expenses, damage to brand and reputation, and lawsuits by customers, banks, shareholders and others. One additional consideration of increasing importance is the possibility of federal regulatory enforcement actions.

Congress has yet to pass all-encompassing cybersecurity legislation, but earlier this year the Obama administration sent Congress three legislative proposals to respond to growing cybersecurity threats. In short, the president wants to create a single federal breach notification standard to replace the current patchwork of state notification laws. Further, he wants to encourage cybersecurity information sharing between the private sector and the federal government, and to provide law enforcement the necessary authority to investigate and prosecute cyber-crimes. Under the Administration's proposal, the FTC would be given specific authority to implement the laws.

"Although the president's proposed legislation has yet to be authorized by Congress, the FTC already has a reputation as one of the most aggressive cybersecurity regulators, especially in recent years", according to Josh Ladeau, Practice Lead –Privacy and Network Security, Allied World. "The Commission has successfully initiated enforcement actions against name brand companies such as Google and AT&T, as well as scores of smaller, lesser known organizations."

Enforcement activity is increasingly initiated through the FTC's general statutory authority under section 5(a) of the Federal Trade Commission Act. The FTC Act regulates unfair trade practices, and it is the Commission's position that the provision gives the FTC authority to initiate enforcement actions against companies who fail to reasonably safeguard consumer data.

"In recent years, the FTC has broadened its scope, now expanded to include actions against companies for "unreasonably" failing to meet minimum cybersecurity standards regardless of the cybersecurity representations made by the company. "

Other laws under FTC supervision also include privacy provisions and have resulted in enforcement activity. These laws, which are specific to a particular industry or population, include the Gramm-Leach Bliley Act, the Fair Credit Reporting Act (FCRA), and the Children's Online Privacy Protection Act (COPPA), among others.

The chart below tracks FTC cybersecurity enforcement activity since 2000 and clearly illustrates how activity has accelerated substantially both in terms of cases filed and cases settled since 2011.

Exhibit 1: Cases Brought by the FTC over Time[1]

From the time the FTC first started addressing cybersecurity in 2000 to today, its focus has expanded. Early actions concentrated on companies who misrepresented their cybersecurity policies and were primarily resolved through a consent decree requiring appropriate data security safeguards and a period of FTC oversight which could last up to 20 years.

In recent years, the FTC has broadened its scope, now expanded to include actions against companies for "unreasonably" failing to meet minimum cybersecurity standards regardless of the cybersecurity representations made by the company. However, other than precedents established through previous enforcement activity and what has been determined to be "unreasonable" in its prior consent decrees, the FTC's guidance on these standards is minimal.

This lack of guidance, together with the fact that the authority to regulate cybersecurity was never specifically granted to the FTC by Congress, has raised questions over the validity of the FTC's assumed mandate to bring lawsuits against companies or require them to implement data security safeguards.

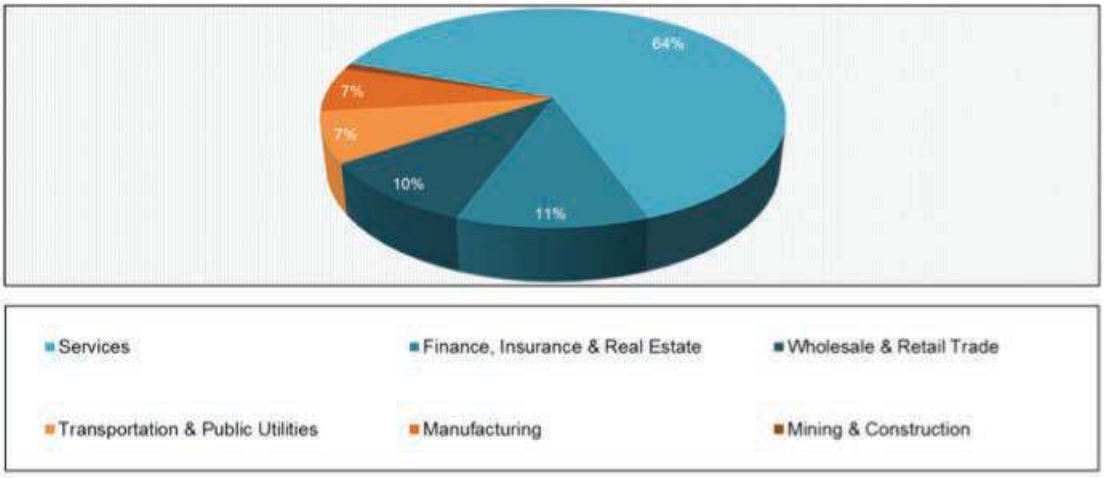
[1] *Exhibits in this paper are reprinted with permission from Advisen. In Exhibit 1, some cases have more than one defendant involved. This exhibit illustrates each defendant as a separate case.*

"In the meantime, the FTC has continued to persistently assert its cybersecurity authority, bringing cyber-related enforcement actions against companies across various industries."

In a widely followed case, the U.S. District Court for the District of New Jersey held last year that the FTC had the authority to bring an enforcement action against Wyndham Hotels and Resorts LLC to remedy its alleged unreasonable data security practices. The case is currently under appeal in the Third Circuit, and could ultimately determine the commission's regulatory authority in this area.

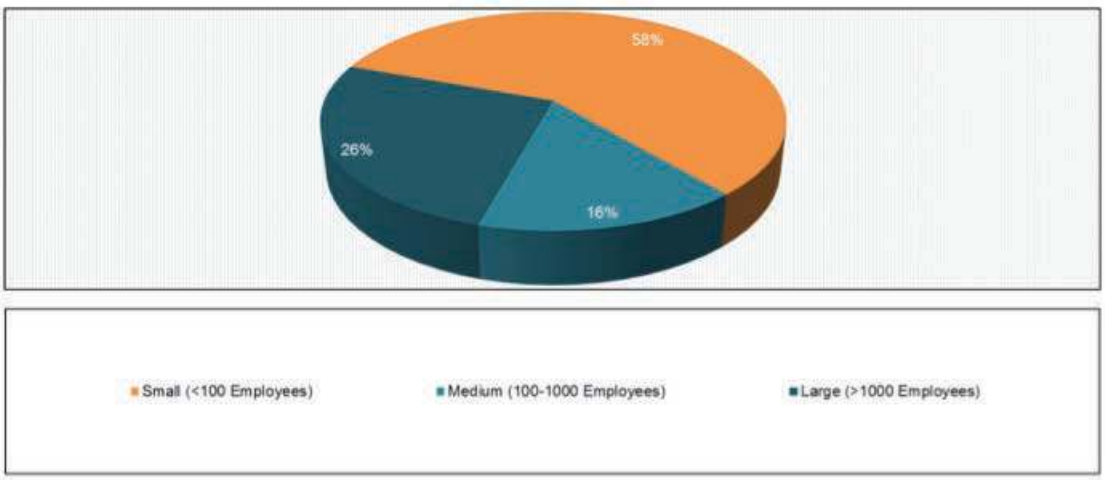
In the meantime, the FTC has continued to persistently assert its cybersecurity authority, bringing cyber-related enforcement actions against companies across various industries. The services industry, which includes healthcare and hospitality, has by far accounted for the largest portion of FTC enforcement activity, according to Advisen. (Exhibit 2)

Exhibit 2: Cases Brought by the FTC: Industry Distribution



The FTC cyber enforcement activity that has generated the most coverage from the media and the legal communities has focused on large companies with recognizable brands, such as Wyndham, Verizon, and AT&T. The bulk of FTC cases, however, involve companies having fewer than 100 employees. (Exhibit 3)

Exhibit 3: Cases Brought by the FTC: Company Size Distribution



"According to Advisen, FTC enforcement actions that result in fines and penalties can have significant financial implications, with the largest fine imposed to date exceeding $20 million."

The FTC has proven an equal opportunity regulator and will aggressively take action against any company who makes false representations or simply fails to adopt reasonable data security programs. Whether through consent decrees that require the implementation of data security measures and long term FTC supervision, or the issuance of fines and penalties, the impact on companies can be severe.

The Wyndham case and its implications

The Wyndham case is the most widely followed FTC cybersecurity case due to its broad implications. The FTC sued Wyndham Worldwide in 2012 after hackers stole credit and debit card numbers of thousands of customers, alleging that Wyndham did not reasonably protect the information from theft. Wyndham challenged the suit claiming that the FTC does not have authority to regulate cybersecurity. In April of 2014, a U.S. District Judge sided with the FTC stating that:

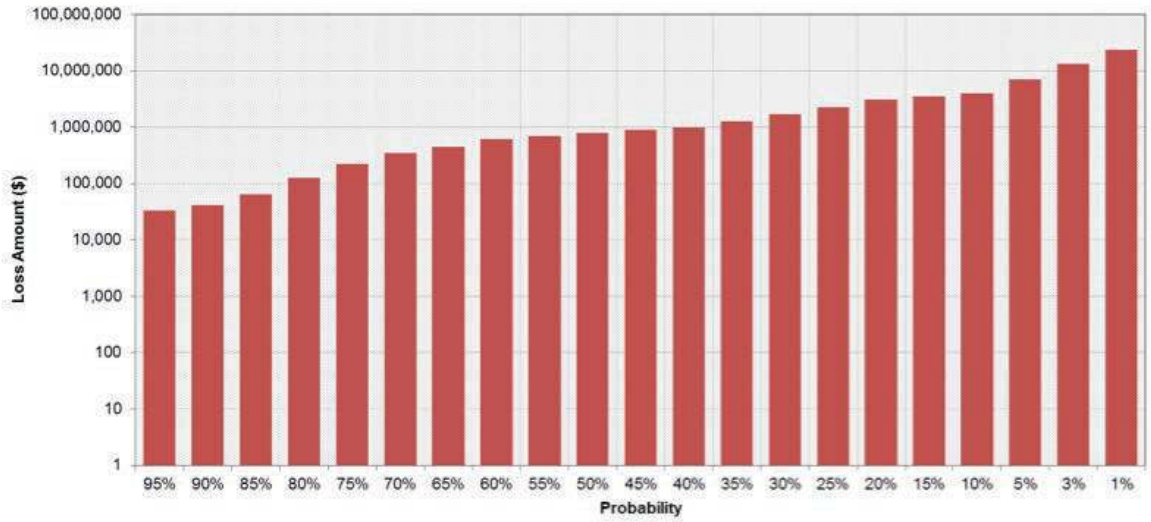
1. Section 5 of the FTC Act provided regulatory authority,
2. The FTC provided adequate notice of what it perceives as reasonable data security standards, and
3. The claim of unfairness or deception was adequate under Section 5 of the FTC Act.

The case is currently under appeal in the U.S. Court of Appeals for the Third Circuit. A reversal of the lower court ruling will have significant implications for FTC cybersecurity enforcement and the potential liabilities of companies when their systems are breached.

According to Advisen, FTC enforcement actions that result in fines and penalties can have significant financial implications, with the largest fine imposed to date exceeding $20 million. The chart below shows the probability of a fine of a certain size being levied. For example, 95 percent of the time, the FTC fine will be $35k or less. Similarly, fines will exceed $10M only 3 percent of the time. (Exhibit 4 on next page)

"Google paid the largest fine ($22.5 million) ever imposed by the FTC for a civil violation to settle a regulatory case questioning the Internet search leader's respect for people's privacy and the integrity of its internal controls. "

Exhibit 4: Loss Probability: FTC Fines & Penalties

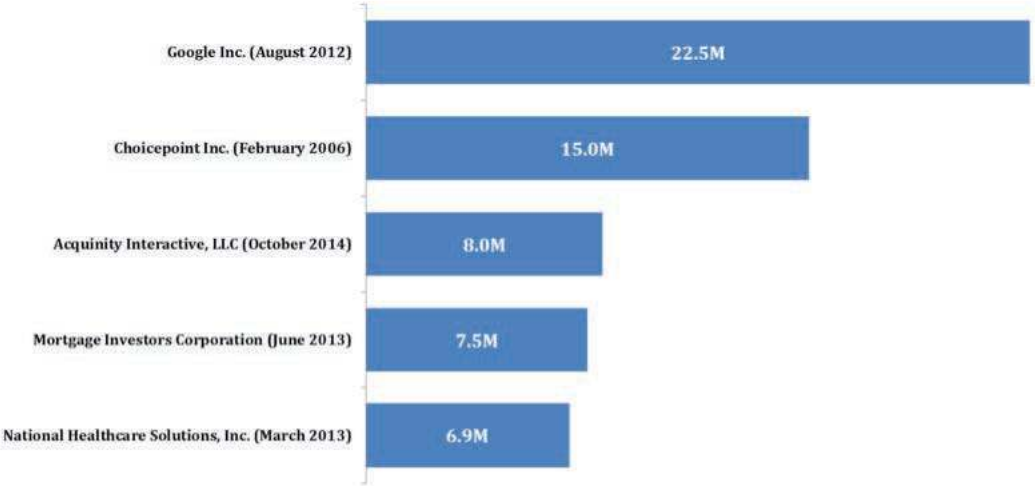


Google paid the largest fine ($22.5 million) ever imposed by the FTC for a civil violation to settle a regulatory case questioning the Internet search leader's respect for people's privacy and the integrity of its internal controls. The fine resolves the FTC's allegations that Google Inc. duped millions of Web surfers who use Apple Inc.'s Safari browser.

Google had assured people that it would not monitor their online activities, as long as they did not change the browser settings to permit tracking. Google broke that promise, according to the FTC, by creating a technological loophole that enabled the company's DoubleClick advertising network to shadow unwitting Safari users. That tracking gave DoubleClick a better handle on what kinds of marketing pitches to show them. The FTC concluded that the contradiction between Google's stealth tracking and its privacy assurances to Safari users violated a vow that the company made in another settlement.

Below is a list of the top five cyber-related FTC Fines & Penalties according to Advisen. (Exhibit 5)

Exhibit 5: Top FTC Fines & Penalties



"Cyber insurance provides more than just indemnity for first and third party losses due to a data breach, it provides access to a variety of services to assist with both pre and post breach activities. "

Cybersecurity-related FTC enforcement activity can have implications beyond the assessment of fines, however. Organizations accused by the FTC of misrepresenting safeguards or failing to meet minimum data security requirements are also exposed to consumer class actions and state level litigation for violations of specific state consumer protection laws.

Insurance and Risk Management Solutions

Although the FTC has not formally established specific guidelines as to what it deems reasonable cybersecurity practices, years of enforcement activity in this area provide baseline parameters. Companies must be proactive in their ability to respond to evolving threats; complacency is not an option, as it eventually will catch the attention of the FTC and have broader implications. Organizations with a well-rehearsed breach response plan and pre-identified breach response team significantly reduce the likelihood of enforcement actions and the threat of fines and private lawsuits.

From fines and penalties coverage, where insurable, through indemnity for first and third party losses due to a data breach, insurance can play a critical risk-transfer role. Cyber policies can also provide access to a variety of risk management and risk mitigation tools and vendors, for both pre-and-post breach activities.