Client Update
Court Upholds FTC Cyber Authority; Recent FTC Guidance on Insider Breaches Looms Larger

NEW YORK
Jeremy Feigelson
jfeigelson@debevoise.com

James J. Pastore
jjpastore@debevoise.com

David Sarratt
dsarratt@debevoise.com

Sean Heikkila
sheikkila@debevoise.com

WASHINGTON, D.C.
David A. O'Neil
daoneil@debevoise.com

THE THIRD CIRCUIT UPHOLDS THE FTC'S CYBERSECURITY ENFORCEMENT AUTHORITY

Section 5 of the FTC Act states broadly that "unfair" and "deceptive" business practices are illegal. For about ten years, the FTC has brought a host of enforcement cases in the cybersecurity area. In a nutshell, the Commission asserts in these cases that data security practices are "unfair" if they are substantively inadequate, and "deceptive" if they run contrary to a company's own public statements. But the FTC has not issued formal cybersecurity guidance through a rulemaking process.

Wyndham Hotels got hit with an FTC enforcement action after it experienced multiple data breaches in 2008 and 2009. Wyndham hit back with a legal challenge, asserting that the FTC lacked the authority to sue it for deficient cybersecurity practices.

Ruling on August 24, a three-judge panel of the Third Circuit unanimously sustained the FTC's authority to bring an enforcement action against Wyndham, affirming a ruling below out of the District of New Jersey. The panel held that inadequate cybersecurity measures and privacy policies could constitute "unfair practices" under the FTC Act. The panel stated that Wyndham could be liable for unfair practices violations even where the conduct of the hackers was criminal, so long as the cybersecurity intrusions were foreseeable—and, the panel noted, an unforeseeability argument "would be particularly implausible as to the second and third attacks."

In rejecting Wyndham's argument that the company had insufficient notice of the particular cybersecurity practices favored by the FTC, the Court pointed to

materials like the FTC's complaints in earlier cybersecurity cases and to a cybersecurity guidebook issued by the FTC in 2007.

MORGAN STANLEY'S INSIDER BREACH

In light of the Third Circuit's emphasis on past FTC guidance, the FTC's recent announcement that it would *not* take enforcement action against Morgan Stanley is all the more timely and important.

In January 2015, Morgan Stanley announced that a financial advisor in its wealth management division had stolen client data for some 350,000 accounts, representing nearly 10% of the bank's wealth management clients. Almost none of the compromised accounts were the thief's particular clients. Following the breach, account names, numbers and other customer information relating to approximately 900 accounts appeared on public websites.

The FTC opened an investigation of Morgan Stanley's data security practices prior to the breach. But on August 10, 2015, the FTC's Bureau of Consumer Protection, Division of Privacy and Identity Protection, published a closing letter—that is, it publicly ended its investigation without taking enforcement action.

A closing letter is the FTC enforcement staff's way of saying to industry, "We're taking a pass in this specific case—but the rest of you are now on notice of our reasons, so next time we may not be so lenient."

WHAT MORGAN STANLEY DID RIGHT

In its closing letter, the FTC staff highlighted the key aspects of Morgan Stanley's data security program that contributed to the decision not to pursue enforcement action:

- Morgan Stanley "implemented a policy allowing employees to access only the personal data for which they had a business need." The thief was acting contrary to company policy by reaching for the data of clients he did not personally serve; this was viewed as important by FTC. To state the obvious, an employee who cannot get access to sensitive stuff in the first place cannot steal that stuff.
- Morgan Stanley implemented technological tools to monitor "the size and frequency of data transfers by employees." Such monitoring, done right, can help flag anomalous data flows that are indicative of a breach.

- The company deployed tools to block employee access to high-risk applications and websites. Many financial institutions and other organizations now restrict access to applications and sites that are seen as risky—in particular, webmail, social media and other potential exfiltration points for stolen data.
- Morgan Stanley prohibited employees from using USB drives or other removable media. Although Morgan Stanley's policy ultimately was not properly configured in this instance, the FTC may view the existence of such a policy as required going forward.
- Morgan Stanley responded swiftly once it had notice of the breach. The company reviewed and, where necessary, remediated its network security protections and policies. The company also identified and terminated the employee; promptly alerted law enforcement; worked to remove the compromised data from the Internet; notified affected clients; and offered identity protection services to the clients. Given the FTC's praise for Morgan Stanley on these issues, companies are well advised to review, refresh and test their written incident response plans to see how they compare.

Insider or "Snowden" risk is widely viewed as one of the most daunting challenges in all of data security. After all, it is impossible to run a business without giving your employees liberal access to data and system resources. The closing letter is a reminder to companies in all industries that, however daunting the challenge may be, the FTC sees robust efforts to tackle Snowden risk as a legal requirement.

The closing letter specifically warns that "risks, technologies, and circumstances change over time," and that "companies must adjust security practices accordingly." For today, though, companies are well advised to carefully assess their own Snowden-risk mitigation strategies in light of the Morgan Stanley closing letter. A good approach is to ask with particularity not just "are we doing X?", but "how well are we doing X and are there gaps we need to close?". This approach should help position a company to receive the FTC's next closing letter, rather than its next lawsuit.

* * *

Please do not hesitate to contact us with any questions.