Verizon Privacy Fixes Show How To Avoid The FTC's Wrath

By **Allison Grande**

Law360, New York (November 26, 2014, 4:00 PM ET) -- The Federal Trade Commission recently dropped its probe into Verizon Communications Inc.'s alleged failure to adequately secure routers it provided to its customers, giving companies a blueprint for how to avoid sweeping consent decrees that could put their privacy practices under the agency's microscope for decades.

The FTC informed Verizon in a **Nov. 12 letter** that it had elected to close its investigation into whether the company had engaged in unfair or deceptive acts or practices in violation of Section 5 of the FTC Act by failing to secure, in a reasonable and appropriate manner, the routers it provided to its high-speed Internet and FiOS customers.

While the agency expressed concerns with Verizon apparently shipping routers to customers with a default encryption security standard that had been rejected by a leading technical association a decade ago, it explained that the strength of the steps that Verizon had taken to address the issue and mitigate the risk to customers' information had encouraged it to close the matter without taking further action.

"The Verizon closing letter is a reminder that effective remediation is a powerful tool in an advocate's tool box when arguing for the FTC to use its prosecutorial discretion not to pursue a law enforcement action in a data security investigation," Morrison & Foerster LLP partner D. Reed Freeman said.

In bringing more than 50 data security actions during the past decade, the FTC has repeatedly pushed private companies to employ "reasonable" measures for shielding the sensitive consumer data with which they are entrusted from known security risks and vulnerabilities.

While the commission's authority to deem certain data security practices as "unreasonable" is currently being challenged in a pair of closely watched cases involvingWyndham Worldwide Corp. and LabMD Inc., the regulator has **continued to aggressively push** its message that data security is an "ongoing process" that requires constant re-evaluation by businesses.

The FTC reiterated the point in its closing letter to Verizon, saying it hopes and expects that companies “adjust practices accordingly” as risks, technologies and circumstances change over time.

"Data security is not static and must evolve based on the current threat environment," said Craig A. Newman, managing partner of Richards Kibbe & Orbe LLP. "The commission's decision made plain that as new cyber-risks emerge, it expects companies to adjust their cybersecurity practices in a way that addresses these new risks."

On their face, the shortcomings that appear to have prompted the FTC's probe are similar to ones that the regulator has identified in prior data security cases that have ended with consent decrees that require the accused party to make certain changes to their data security practices and undergo regular privacy audits for the next 20 years.

According to the commission's closing letter, Verizon regularly shipped routers to customers with the default security set to an encryption standard known as Wired Equivalent Privacy. The WEP standard was deprecated by the Institute of Electrical and Electrics Engineers in 2004 due to weaknesses the organization identified with the standard and was replaced first by the Wi-Fi Protected Access standard and later the Wi-Fi Protected Access 2 standard.

Despite the change in security protocol, Verizon continued shipping some router models with the abandoned standard set as the default, which left the devices vulnerable to hackers, the commission alleged.

But unlike in similar disputes that have been made public, Verizon was able to avoid having to either negotiate a consent decree or fight the claims in court by coming up with a plan to proactively address the regulator's concerns, attorneys say.

“A company's response to a detected cybersecurity vulnerability is critical,” Jones Dayglobal privacy practice co-chair Mauricio Paez said. “Proactive, transparent and comprehensive response and cooperation can lead to positive results, including an end to a governmental investigation and enforcement, provided the company takes sincere steps to address such security risks to protect consumers from potential personal privacy and security breaches.”

In its closing letter, the commission pointed to several steps the company had taken to

address the security concerns, including pulling all WEP-defaulted routers from its distribution centers and setting them to WPA2; implementing an outreach campaign asking customers using WEP or no encryption to update their settings to WPA2; and offering customers that have older routers incompatible with WPA2 an opportunity to upgrade to units that are compatible with the latest standard.

“What made this case different is that Verizon recognized that there was an issue and developed a plan to address and mitigate the risk,” said Vedder Price LLP data privacy and information management practice group chairman Bruce Radke. “So whenever the FTC had a discussion with them, they could say we've formulated a plan that we're in the process of implementing, and that in essence alleviates the need to have a consent decree with a corrective action plan.”

Making sure that the plan addressed any potential harm that could befall consumers also likely helped Verizon in their discussions with the regulator, given that the FTC Act requires that the commission show consumers suffered a “substantial” injury that was not “avoidable,” attorneys noted.

“Unlike in a data breach situation where people's personal data has clearly been exposed and they are vulnerable to financial loss, in this case it was more just the potential for harm as opposed to anyone being able to say a particular Verizon user had been hurt by using this old technology,” VLP Law Group LLP partner Michael Whitener said. “And on top of that, Verizon took some pretty dramatic actions to fix things.”

Given the FTC's response, companies would be wise to take to heart the warning in the closing letter that data security should not be a static exercise and work to ensure that they are taking steps to address changes to protocols in order to avoid the regulator's wrath in the first place, attorneys say.

"It seems like one of the main ideas of the closing letter is that while in the past it might have been a one-and-done situation where a company set up a system and didn't look back, the FTC is now saying that data and privacy security is an ongoing process and it's up to companies to be proactive about staying on top of new technology," Moore & Van Allen PLLC associate Leslie Pedernales said.

But while the closing letter puts pressure on companies to keep abreast of changing

standards, its reaction to the steps that Verizon took to address its failure to update its default settings should give companies some comfort that the regulator is amenable to listening to efforts to correct potential deficiencies.

"The FTC does not appear to be demanding ongoing security reviews to avoid Section 5 liability," Kurt Wimmer, chairman of Covington & Burling LLP's privacy and data security practice, said. "The FTC appears willing to give businesses the benefit of the doubt when they respond to the FTC's concerns with clear steps and strong efforts to mitigate risk to consumers."

Companies should also take comfort from the commission's statement that it took into account Verizon's "overall data security practices related to its routers" when deciding whether to pursue the action, an admission that suggests that the FTC is willing to adopt a holistic approach to enforcement.

"This is a perfect example of why organizations should be prepared for the FTC's examinations of their security practices before any data breach or FTC investigation has actually occurred," said Hsiao Mao, the vice chair of the technology practices group atKaufman Dolowich & Voluck LLP. "Solid security protocols and practices take years to develop and properly document, and it is clear here that the FTC took Verizon's existing efforts before the investigation occurred seriously."

--Editing by John Quinn and Philip Shea.