MINTZ

Corrective Action Earns Verizon End to FTC's FiOS Router Investigation

November 14, 2014 | Blog |

VIEWPOINT TOPICS

- Privacy & Cybersecurity

RELATED PRACTICES

RELATED INDUSTRIES

Corrective action taken by Verizon Communications to fix security issues with its FiOS and DSL routers resulted in the FTC closing its investigation to determine whether Verizon's distribution of the routers was an unfair or deceptive practice.

According to the FTC, Verizon regularly shipped routers to consumers with the default security set to the outdated WEP standard, which has been known for a decade to have weaknesses that leave users of the routers vulnerable to hackers.

After the FTC initiated its investigation, Verizon took steps to mitigate the risks to its customers. It changed the default security setting on the routers going out to customers from the obsolete WEP standard to the current WPA2 standard, it initiated an outreach campaign to its customers to encourage them to update the security settings on their routers, and it offered customers with older routers incompatible with the WPA2 standard the opportunity to upgrade to a newer, WPA2-compatible device.

The FTC emphasized that closing the investigation did not mean that Verizon might not have violated the FTC Act. It cautioned that

> what constitutes reasonable security changes over time as new risks emerge and new tools become available to address them. As most all consumer devices on the market today are compatible with WPA2, it would likely be unreasonable for Internet Service Providers ("ISPs") or router manufacturers to continue to default consumer routers to WEP encryption. We hope and expect that all companies that provide consumers with these products will ensure reasonable and appropriate default security settings.

A copy of the FTC's closing letter is available **here**.

Authors