UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, DC 20580

Bureau of Consumer Protection
Division of Privacy and Identity Protection

November 12, 2014

Ms. Dana Rosenfeld
Kelley Drye
Washington Harbour, Suite 400
3050 K Street, NW
Washington, D.C. 20007

Dear Ms. Rosenfeld:

As you know, staff in the Division of Privacy and Identity Protection has conducted an investigation into possible violations of Section 5 of the Federal Trade Commission Act by your client, Verizon Communications, Inc. ("Verizon"). The investigation considered whether Verizon engaged in unfair or deceptive acts or practices by failing to secure, in a reasonable and appropriate manner, the routers it provided to its High Speed Internet (DSL) and FiOS customers.

Among other things, our investigation examined the fact that Verizon regularly shipped routers to consumers with the default security set to an outdated encryption standard known as Wired Equivalent Privacy ("WEP"). Due to certain weaknesses in WEP, the Institute of Electrical and Electronics Engineers ("IEEE") deprecated this standard in 2004 in favor of a new standard known as Wi-Fi Protected Access ("WPA"), and later, Wi-Fi Protected Access 2 ("WPA2").[1] However, until recently, Verizon continued to ship some router models with the WEP encryption standard. As a result, many Verizon customers still have routers that are set to the outdated WEP standard, leaving them vulnerable to hackers.

Despite this concern, staff has determined to close this investigation. Among the factors we considered were Verizon's overall data security practices related to its routers, along with efforts by Verizon to mitigate the risk to its customers' information. Indeed, Verizon has recently taken several steps to address the concerns regarding the security of its customers' routers. First, the company has pulled all WEP-defaulted routers from its distribution centers and set them to WPA2, ensuring that all routers distributed going forward will be set to WPA2 by default. Second, the company has implemented an outreach campaign targeting customers that are currently using WEP or no encryption and asking these customers to update their security settings to WPA2. Lastly, for those customers that have older routers incompatible with

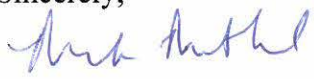
[1] *See* IEEE Std 802.11i -2004, *available at* http://standards.ieee.org/getieee802/download/802.11i-2004.pdf ("This amendment retains the WEP feature for purposes of backwards compatibility with existing IEEE 802.11 devices, but WEP is deprecated in favor of new security features provided in this amendment.").

WPA2, the company is offering an opportunity to upgrade to WPA2-compatible units. We encourage consumers to take advantage of these opportunities to update their router security.

We continue to emphasize that data security is an ongoing process. As risks, technologies, and circumstances change over time, companies must adjust security practices accordingly. In the past, defaulting consumer routers to WEP may not have been unreasonable, given concerns about compatibility with older computing devices. However, 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.

The closing of this investigation is not to be construed as a determination that a violation may not have occurred, just as the pendency of an investigation should not be construed as a determination that a violation has occurred. The Commission reserves the right to take such further action as the public interest may require.

Sincerely,



Maneesha Mithal
Associate Director
Division of Privacy and Identity Protection
Federal Trade Commission