



1300 I Street, N.W., Suite 400 West
Washington, D.C. 20005

Phone 202 515-2533
Fax 202 336-7858
kathleen.m.grillo@verizon.com

January 30, 2015

The Honorable Thomas E. Wheeler
Chairman
Federal Communications Commission
445 12th Street, S.W.
Washington, D.C. 20554

Re: Technological Advisory Council Report on Mobile Device Theft Prevention, ET Docket No. 14-143

Dear Chairman Wheeler:

I am writing in response to your December 4, 2014 letter to Lowell McAdam, Chairman and Chief Executive Officer of Verizon, regarding the recommendations of the Commission's Technological Advisory Council (TAC) on preventing the theft of mobile devices. The TAC report, developed by a broad set of "stakeholders with widely different areas of focus and expertise," recognized the contributions that the wireless industry has made and offered recommendations geared toward harnessing these and additional efforts, such as improved outreach and education. While wireless companies like Verizon continue to play a role in this effort, the TAC report properly emphasized the need for ongoing "participation of all stakeholders including law enforcement, industry, States and U.S. territories" to address stolen device crime through a variety of approaches.

Verizon has worked diligently with CTIA-The Wireless Association, policymakers and law enforcement to develop a proactive, multi-faceted approach to mitigate device theft. Verizon maintains a list of devices reported to it as stolen and does not allow those devices to be activated for service on its wireless network. In 2012, Verizon agreed to enhance its internal list of stolen devices by participating in the GSMA database of lost and stolen devices. The GSMA database is a compilation of identification numbers of devices that have been reported as lost or stolen to approximately 95 participating carriers in 55 countries. Through its participation in the GSMA database, Verizon is able to share information about 4G LTE devices reported to Verizon as lost or stolen with other companies in the U.S. and around the globe. The GSMA database also enables Verizon to block activation of devices reported to other carriers as lost or stolen. Separately, Verizon makes available to its customers information about anti-theft features on devices and services available from Verizon. Further, Verizon supported and will honor the April 2014 CTIA Smartphone Anti-Theft commitment. This includes a commitment to offer a free anti-theft tool in all new smartphones manufactured after July 2015, allowing customers to remotely erase and render inoperable their smartphone if it is stolen.

Regarding the specific points you raise in your letter, you first asked about including "lock/wipe/restore" functionality in devices. As part of the CTIA Smartphone Anti-Theft

The Honorable Thomas E. Wheeler

January 30, 2015

Page 2

commitment, Verizon has worked closely with its device and operating system suppliers so that all smartphones manufactured after July 2015 and sold by Verizon will have enhanced anti-theft tools. These tools will provide the authorized user the capability to: remotely wipe the authorized user's data; render the smartphone inoperable to an unauthorized user; prevent reactivation without the authorized user's permission; and reverse the inoperability and restore the user data on a recovered smartphone to the extent feasible. Some of the smartphones we sell already incorporate these solutions, and Verizon is committed to making these anti-theft tools fully available to our consumers.

Second, you asked about protecting unique device identifiers from alteration. As noted in the TAC report, the GSMA has done significant work with the device manufacturing community to strengthen the integrity of device identifiers and also notes that "all smartphones sold in reputable U.S. retail environments support this set of measures." While this hardware issue is in the control of the device manufacturers, not the carriers, Verizon supports and encourages those device industry efforts because maintaining the integrity of these identifiers is important to the actions we and others take to reduce the market for stolen phones. In addition, Verizon and CTIA have been supportive of legislation introduced in the U.S. Senate that would criminalize the unauthorized tampering with device identifiers.

Third, you asked about "[i]mproving the timeliness, accuracy and availability of data" about smartphone theft for use by law enforcement." As explained above, Verizon participates in the GSMA's shared database of lost and stolen devices, sharing and obtaining new stolen phone information with other participating carriers on a daily basis and ensuring the accuracy and integrity of the data through internal procedures and audits. The GSMA allows law enforcement agencies to access its database of lost and stolen devices and Verizon will continue to assist law enforcement agencies that seek access to this data set. Further, Verizon fully supports the efforts by CTIA and GSMA to improve communications and outreach to law enforcement agencies to better inform such agencies about the availability of this data and the means by which it can be obtained.

Finally, you asked Verizon to ensure that its retail employees check every device initialized for service against Verizon's database of lost and stolen devices. Rather than relying on a manual check by retail employees, Verizon's systems instead automatically screen every device sought to be activated on the Verizon Wireless network against a list of lost and stolen devices that incorporates the GSMA data the company obtains daily. If a device appears on the list, activation of it is automatically rejected. Verizon's sales and service representatives are always available to answer any customer inquiries regarding the security of their devices.

Please let me know if you have any questions.

Sincerely,

A handwritten signature in black ink, appearing to read "Kathleen Grillo". The signature is written in a cursive, slightly slanted style.