CTIA
The Wireless Association™

Expanding the Wireless Frontier

March 31, 2013

Chairman Julius Genachowski
Federal Communications Commission
445 12th Street, SW
Washington, D.C. 20554

Re: CTIA Stolen Smartphones Status Update

Dear Chairman Genachowski:

On April 10, 2012, CTIA – The Wireless Association® ("CTIA"), in coordination with the Federal Communications Commission and the Major City Police Chiefs, announced a voluntary commitment by CTIA and participating wireless companies to take certain actions to help law enforcement deter smartphone theft and protect personal data. Please find attached CTIA's quarterly update detailing progress toward these voluntary commitments, described more fully below.

1. Implement databases to prevent reactivation of stolen smartphones. Wireless providers will work to initiate, implement and deploy database solutions, using unique smartphone identifying numbers, designed to prevent smartphones reported by their customers as stolen from being activated and/or provided service on their own networks. Using unique GSM smartphone identifying numbers, GSM providers will develop and deploy a database designed to prevent GSM smartphones reported as stolen from being activated or provided service. By October 31, 2012, U.S. GSM providers will implement this database so that stolen GSM smartphones will not work on any U.S. GSM network. In addition, U.S. providers will create a common database for LTE smartphones designed to prevent smartphones that are reported stolen by consumers from being activated or provided service on any LTE network in the U.S. and on appropriate international LTE stolen mobile smartphone databases. This database will be completed by November 30, 2013.

2(A). Notify consumers of features to secure/lock smartphones with passwords. By April 30, 2013, smartphone makers will implement a system to notify/inform users via the new smartphones upon activation or soon after of its capability of being locked and secured from unauthorized access by setting a password.

2(B). Educate consumers about features to secure/lock smartphones with passwords. By December 31, 2012, smartphone makers will include information on how to secure/lock new smartphones in-box and/or through online “Quick Start” or user guides.

3. Educate consumers about applications to remotely lock/locate/erase data from smartphones. Wireless providers will inform consumers, using communications including email or text messages, about the existence of – and access to – applications that can lock/locate/erase data from smartphones. Providers will also educate consumers on how to access these applications, including those that are easy-to-find and preloaded onto smartphones. Substantial progress on this will be made by December 31, 2012; it will be completed by April 30, 2013.

4. Educate consumers about smartphone theft, protections and preventative measures. By July 1, 2012, the wireless industry will launch an education campaign for consumers on the safe use of smartphones and highlight solutions one through three by using a range of resources, including a public service announcement and online tools such as websites and social media.

If you have any questions regarding this submission, please contact the undersigned.

Sincerely,

/s/ Brian M. Josef

Brian M. Josef

cc: Charles Mathias

Attachment

AT&T:

AT&T continues to successfully block stolen GSM phones from accessing the network through its own network as well as for other participating GSM providers that are shared through the GSMA-NA central database since October 31, 2012.

To maximize support for customers who have been victimized by stolen phone theft, AT&T enhanced its customers' experience to provide online and 611 automated suspension and device blocking 24x7.

This November, AT&T will block LTE devices submitted through the GSMA-NA after new wireless service providers begin to upload new stolen devices. To meet this date, AT&T has initiated contact with several wireless providers and will provide guidance on best practices using a new Contributing Network Operator User Guide specific to North America.

As other regional interest GSMA groups (Europe, Latin America, Australia, etc.) connect to the database, AT&T will recognize and block shared GSM and LTE wireless devices globally.

CTIA:

CTIA continues to work with smartphone makers and believes they are on track to meet the April 30, 2013 benchmark for notifying users of new phone models via the smartphone upon or soon after activation of their smartphone's capability to be locked with a password.

CTIA launched a Public Service Announcement ("PSA") video, The 5 Stages of Losing a Smartphone, which reminds consumers to use their smartphones' features and apps to remotely lock, track and wipe smartphones if the devices are lost or stolen. As of this filing, the PSA had been viewed nearly 317,000 times on CTIA's YouTube channel alone. CTIA also has seen substantial interest in, and traffic on, its dedicated URL at beforeyouloseit.org. This website provides valuable information on tips to deter smartphone theft as well as a link to the PSA. CTIA has continued to work with the Commission, the law enforcement community, and television broadcast stations throughout the country to encourage placement of the PSA.

In addition to its broad Public Relations efforts surrounding the launch of the Voluntary Commitment, CTIA continues to harness traditional (including print and broadcast), online and social media to provide valuable information about the industry's Stolen Smartphones Initiative to wireless consumers. Specifically, CTIA has prominently featured on the CTIA website's main homepage (www.ctia.org) detailed information on steps that CTIA and participating wireless companies are taking to deter smartphone thefts. CTIA also continues to conduct radio, television and print interviews on the issue.

CTIA maintains its blog posts addressing steps to deter smartphone theft and protect user information (including step-by-step "how-to" videos to assist with setting passwords on various smartphone operating systems). These posts have been broadly distributed via social media including Twitter, Facebook, LinkedIn and YouTube.

CELLCOM:

Cellcom updated its website homepage to feature a link on mobile security to educate customers regarding how to protect their smart phone and personal information. This web page includes information encouraging customers to set up a passcode to lock their devices, use a mobile security app, and back up photos, videos, contact and emails. Cellcom also provides recommendations to assist customers who have a missing phone. Further, customers can link to CTIA's website for more detailed information on how to set a password and view a comprehensive list of anti-theft protection apps.

Cellcom sends an auto-generated 'Welcome' email after each customer activates a smart phone. This email includes a link to Cellcom's mobile security page.

Cellcom uses its Facebook page and Twitter to share the most current information on mobile security and safe, responsible use of online technology and mobile phones.

NEX-TECH WIRELESS:

Nex-Tech Wireless has established a blacklist database for stolen phones that is currently in use by the company to prevent activation of stolen smartphones.

Nex-Tech Wireless continues to develop plans to post information on its website to inform consumers about steps to prevent and respond to cell phone theft. The information will become available online in the coming months.

Nex-Tech Wireless also is developing collateral material on theft prevention strategies to offer consumer tips to lock, locate and erase data from smartphones.

SPRINT NEXTEL:

Sprint continues to make significant progress in implementing the voluntary smartphone commitment, including: (1) implementing a database that prevents CDMA smartphones that are reported as lost or stolen from being activated or provided service on its network; (2) creating vanity URLs for each of its brands featuring detailed information on what to do if a smartphone is lost or stolen, encouraging the use of passcodes, and highlighting several mobile security apps that can track, lock and wipe phones (*e.g.,* www.sprint.com/stolenphone); (3) launching the "Sprint Guardian" application in May 2012 to help customers manage, monitor and protect up to five lines on an account (including the Lookout application to help customers locate, lock and wipe lost/stolen phones); and, (4) communicating with its customers through bill inserts, newsletters, social media, and other media about the lost and stolen list and about how consumers can take steps to help protect their smartphones and personal information.

Sprint is working diligently in support of the GSMA-NA's efforts to implement a U.S. cross carrier LTE IMEI database to help address the lost and stolen smartphone issue. Sprint continues to work internally on developing the infrastructure and procedures needed to implement the LTE database system and is on schedule for a November 2013 roll out.

In addition, since its last report, Sprint established an open enrollment for our Total Equipment Protection ("TEP") program which covers lost, stolen and damaged feature phones, smartphones and mobile broadband cards. The open enrollment was for the month of March 2013, and it was made available to customers regardless of how long they have had their mobile device. Sprint also expanded the TEP program to cover the Apple iPhone.

T-MOBILE USA:

T-Mobile USA continues to make substantial progress to meet the deadlines established for the provisions of the April 10, 2012 Voluntary Initiative on Handset Theft Mitigation. Below is a summary of T-Mobile USA's current progress on satisfying the commitments of the Voluntary Initiative.

T-Mobile USA met the October 31, 2012 deadline for completion of blocking on own network and of meeting requirements associated with common GSM database system. T-Mobile is working to set up processes to meet requirements for an LTE common database by the November 30, 2013 deadline.

- T-Mobile USA prevents use of stolen devices internal to its network, has established connectivity to the GSMA Global IMEI database, and through that mechanism acts on stolen device information from AT&T, and sends stolen device information to AT&T as recommended in the GSMA-NA Report (entitled “Analysis and Recommendations for Stolen Mobile Device Issue in the United States”), and as set forth in the Voluntary Initiative.

- The company is currently working on procedures for participation in a common database designed for LTE smartphones reported by consumers as stolen to prevent operation on LTE networks in the U.S. and on appropriate international LTE stolen mobile smartphone databases.

T-Mobile USA met the December 31, 2012 deadline to educate consumers about features to secure/lock new smartphones.

- As of December 1, 2012, T-Mobile USA began including information on safeguarding handsets and handset security offerings as part of the collateral materials (specifically the “Start-up Guide”) found in certain smartphone “in-box” packaging.

T-Mobile USA is making substantial progress to inform consumers about applications to remotely lock/locate/erase data from smartphones and therefore, has met the December 31, 2012 deadline set forth in the requirements of the Voluntary Initiative.

- A significant number of T-Mobile USA devices have basic locking functionality (user-defined codes or patterns).
- T-Mobile USA preloads an application called “Lookout” (with a visible icon) on several of its Android-based handsets, which allows users to track or locate misplaced devices. The premium version of “Lookout” permits users to remotely lock and/or wipe data from handsets.
- Tracking, remote locking, and wiping are also available to users that elect to sign up with Mobile Security service, which is offered by T-Mobile USA partner Asurion that offers handset insurance.

T-Mobile USA began initiating educational initiatives regarding smartphone theft, protections and preventative measures prior to July 1, 2012.

- In June 2012, T-Mobile USA released a “blog” entry on mobile handset security, referencing T-Mobile resources to obtain additional information.
    - Social media tools were used to help propel messaging on the topic.
- Information for customers to help guard against theft and assist when a phone is lost or stolen can be found at www.t-mobile.com/devicesecurity – including instruction on what to do if a phone is lost or stolen.
- Information for customers about other “Privacy Resources” which includes tips about password security, protection from identity theft and protection of customer proprietary information can be found on the landing page of www.t-mobile.com.
- T-Mobile USA recognized the FCC’s launch of its “Smartphone Security Checker” via social media tools to help further propel messaging regarding the importance of protecting handsets.

VERIZON WIRELESS:

In May 2012, Verizon Wireless began its education campaign by launching a consumer-focused web page on Verizonwireless.com that provides customers with information on the prevention of smartphone theft, the importance of using passwords to protect data on smartphones, and what to do if a smartphone is lost or stolen. The site can be accessed at the following link: (http://aboutus.verizonwireless.com/wirelessissues/phonesecurity.html). The site provides direct links to:

- handset manufacturers' app stores where customers can download anti-theft applications.
- register for the company's Wireless Workshops. These classes are offered online and in stores to new and existing Verizon Wireless smartphone customers and are intended to educate its customers on the wide array of powerful features and applications, including security measures.

In July 2012, Verizon Wireless included information on how to safeguard smartphones and the data on them in the company's monthly newsletter, which is emailed to its customers.

Also, as part of its "welcome email" communications program, Verizon Wireless advises new customers on the availability of passwords and other safety measures to protect the data on their smartphones.

In September 2012, Verizon Wireless launched a new application for Android smartphones called Verizon Mobile Security. Reaffirming Verizon Wireless' commitment to robust security, Verizon Mobile Security helps customers protect their devices from digital threats and equips customers with the power to remotely locate, alarm, lock, and even wipe data from a misplaced or lost device. Developed in partnership with Asurion and McAfee, Verizon Wireless has made this application available in Google Play. Details can be found at: http://www.verizonwireless.com/mobilesecurity.

Verizon Wireless' long-standing commitment to deterring crime includes preventing reactivation on the carrier's network of all smartphones that its customers have reported to it as lost or stolen. When a customer reports a lost or stolen smartphone, Verizon Wireless adds that smartphone to its "negative list" file. Verizon Wireless' "negative list" was developed for phones that use its CDMA network, and helps Verizon Wireless prevent the reactivation of any CDMA smartphone that is compatible with the Verizon Wireless network and has been reported to the carrier as lost or stolen. In November Verizon Wireless supplemented its protections by launching a network solution that prevents ongoing use of 4G LTE smartphones that have been reported to the carrier as lost or stolen, even if an already-active SIM card is inserted into the device.

Verizon Wireless also is participating in the development of an industry-wide database to share information on stolen devices. Moreover, Verizon Wireless plans to begin utilizing the multi-carrier database midyear 2013 and will continue to develop its processes to improve the effectiveness of this shared database.