December 28, 2012

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

APPLE:

Apple provides information to educate consumers about features to secure/lock iPhones with passwords and applications to remotely lock/locate/erase data from Apple smartphones. Most recently, Apple coordinated with CTIA and the FCC in the December 18, 2012 launch of the FCC's "Smartphone Security Checker" checklist. The Smartphone Security Checker initiative prominently highlighted key elements of the April 2012 Stolen Smartphones Initiative, including setting PINs and passwords, utilizing apps / services that enable remote location and wiping, backing up and securing data, and reporting a stolen smartphone. The checklist Apple iOS checklist includes consumer-focused information regarding:

- using passcodes with iOS devices;
- setting up "Find My iPhone," locating a device on a map, locking and tracking a device;
- how iCloud Backup works, what data is backed up, and how Backup uses iCloud storage; and
- understanding data protection.

AT&T:

AT&T first launched its blacklist database of AT&T customers' smart phones over the Summer of 2012.

AT&T is pleased to announce that it has implemented the shared blacklist database blocking capability as of October 31, 2012.

AT&T continues to educate customers on how to add smartphone passwords after activation and provide guidance on downloading apps that help to protect devices and personal information.

AT&T enhanced its privacy and safety communication and incorporated it into new and existing customer communication.

CTIA:

In November 2012, 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 56,000 times on CTIA's YouTube channel alone. CTIA issued a joint Press Release with Chairman Genachowski and CTIA President and CEO Steve Largent announcing the new PSA and new, 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 will 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.

In coordination with the FCC, the National Cyber Security Alliance, the U.S. Department of Homeland Security, Blackberry (Research in Motion), Lookout Mobile, and others, CTIA participated in the December 18, 2012 launch of the consumer-focused "Smartphone Security Checker" checklist and live Twitter discussion. The Smartphone Security Checker initiative prominently highlighted key elements of CTIA's April 2012 Stolen Smartphones Initiative, including setting PINs and passwords, using security apps and services that enable remote location and wiping, backing up and securing data, and reporting a stolen smartphone.

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:

In addition to deploying and maintaining a database of electronic serial numbers ("ESNs") that are reported by its customers as stolen, Cellcom has taken the following key steps to address the educational components of the Voluntary Initiative:

- Updated the auto-generated "Welcome" email that is sent after every smartphone application to include a link to Cellcom's mobile security page (October 2012).
- Used the homepage of Cellcom's website to promote the use of a mobile security application and encourage the use of a password (October/November 2012).
- Internally polled employees to gauge current habits, including the use of a password and security apps. (November 2012).
    - 31% of employee respondents use a password voluntarily.

    - 33% of respondents use a password because it is required with corporate email.
    - 36% do not use a password.
- Included an article in Cellcom's quarterly customer newsletter about steps to take before and after a consumer's phone is missing (November 2012).
- Shared the YouTube clip of CTIA's "The Five Stages of Losing a Smartphone" PSA on Facebook, Twitter and employee intranet. (November/December 2012).
- Sent an e-blast to review the importance of using a password (December 2012).
- Sent an e-blast to encourage the use of a mobile security application (December 2012).
- Used Twitter to share consumer protection tips (December 2012).

Cellcom previously took the following key steps to further educate consumers about features to secure/lock its smartphones with passwords and applications to remotely lock/locate/erase data from its smartphones.

- Created a new category on the 'Entertainment & Apps' tab of Cellcom's web site and posted preloaded and easy-to-use apps to remotely lock/locate/erase data from a smart phone. (July 2012)
- Media pitch – Announced Cellcom's participation in the April 10, 2012 Voluntary Initiative. Included a quote from Pat Riordan as CTIA's Chairman of the Board and also as Cellcom's President/CEO. Reviewed proactive steps consumers can take to protect personal information and outlined what to do if a phone is suspected to be lost or stolen. (September 2012)
- Posted links on Cellcom's Facebook page to mobile security apps. (August 2012)
- Posted CTIA video(s) on Cellcom's Facebook page. (August 2012)
- Internally promoted steps to protect personal information and what to do if a phone is missing. (September 2012)
- Internally posted CTIA videos. (August/September 2012)

HTC:

HTC provides information through its website and user guides to consumers on how to secure and lock new phones. HTC provides security instructions in its user guides for all of its smartphones. While the instructions may vary slightly from one device to another, the smartphone user guides generally contain a specific section for

security. At a minimum, this section provides step-by-step instructions for setting a screen lock password. It may also include other instructions, such as how to protect a SIM card with a PIN, how to enable child safety features, or how to encrypt data on the device.

The device user guides are included in the packaging with the devices and are also available online at HTC's website. Additionally, HTC's support website (http://www.htc.com/www/support/) includes a "How-to" section for each device that provides instructions on security features. HTC is on schedule to meet the Voluntary Initiative's April 30, 2013, deadline for notifying users via a smartphone upon activation or soon thereafter of the smartphone's capability of being locked and secured with a password.

MOTOROLA:

Motorola provides consumers with educational information on its website and in device user guides on device security. Specifically, Motorola includes information and instructions on how to secure and lock new phones, backup personal data, and how to use security features to remotely locate and wipe a Motorola device (*e.g.*, through a Motorola online account such as MOTOBLUR where available). Motorola includes these security instructions in its smartphone user guides and at its support website (www.motorola.com/support).

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.

NOKIA / MICROSOFT:

Nokia includes information in its quick start guides regarding how to set and change screen lock passwords through the Settings functions in its smartphones. Nokia includes detailed descriptions of device security features in its online guides for each smartphone it sells in the U.S., including instructions on how to:

- set and change the device security code;
- change the SIM Card PIN code;
- locate, lock and delete all data remotely from a lost or stolen phone, including through Microsoft's "Find My Phone" feature (available at www.windowsphone.com/). Microsoft's "Find My Phone" feature enables a consumer to:
  - Locate a phone on a map:
  - Make a phone ring, even if silent mode is switched on;
  - Lock a phone, and set it to show a message, so it can be returned to the owner;
  - Delete all data from the phone remotely.
  - (The available options may vary).

These descriptions are easily accessed on Nokia's consumer website by typing "security," "lost" or "stolen" in the general search bar on the website.

Nokia Customer Care personnel are trained to assist consumers to implement security features on their devices as well as to assist them in the event that their device is lost or stolen.

Most recently, Microsoft coordinated with CTIA and the FCC in the December 18, 2012 launch of the FCC's "Smartphone Security Checker" checklist. The Smartphone Security Checker initiative prominently highlighted key elements of the April 2012 Stolen Smartphones Initiative, including consumer-focused Windows Phone user guide information regarding setting PINs and passwords, utilizing "Find My Phone" to enable remote location and wiping, backing up and securing data, and reporting a stolen smartphone.

RESEARCH IN MOTION:

Research in Motion ("RIM") provides information to educate consumers about features to secure/lock its smartphones with passwords and applications to remotely lock/locate/erase data from its smartphones.

RIM has added instructions for setting a password to its in-box user guides. RIM also provides the option to secure/lock smartphones following the set up wizard where consumers can personalize features. By April 30, 2013, RIM will introduce an option to set a password as part of the guided setup.

In addition, RIM offers its "BlackBerry Protect" app, which advances the Voluntary Initiative's efforts to educate consumers about apps that can track/lock a device or remotely wipe a device's data.

Most recently, RIM coordinated with CTIA and the FCC in the December 18, 2012 launch of the FCC's "Smartphone Security Checker" checklist. The Smartphone Security Checker initiative prominently highlighted key elements of the April 2012 Stolen Smartphones Initiative, including setting PINs and passwords, utilizing apps / services that enable remote location and wiping, backing up and securing data, and reporting a stolen smartphone. The checklist generated for the Blackberry OS includes consumer-focused information regarding:

- password security for the BlackBerry smartphone;
- setting up BlackBerry Protect and changing automatic backup options; and
- how to turn on location tracking, view your device location, turn on deletion protection and delete all data from your lost device.

SAMSUNG:

Samsung provides information to educate consumers about features to secure/lock its smartphones with passwords and applications to remotely lock/locate/erase data from its smartphones. In conjunction with wireless providers, Samsung has implemented notices in its manuals/quick-start guides provided with devices and available on-line to inform users how to secure/lock new smart phones.

SPRINT NEXTEL:

Sprint has made 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, (3) launching the "Sprint Guardian" application, 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 continues to work diligently in supporting 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 to maintaining the vanity URLs noted above, Sprint has continued to communicate via social media, email, and text messages with its customers regarding safe smartphone usage. For example, in November, Sprint sent text messages and email to prepaid customers reminding them that their smartphones may contain confidential data and directing them to new URL's with information on steps customers can take to protect themselves and their data.

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 requirements with deliverables slated for 2012.

T-Mobile USA met the October 31, 2012 deadline for completion of blocking on its own network and of meeting requirements associated with the common GSM database system.

- 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 April 10th Voluntary Initiative.

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 April 10th Voluntary Initiative.

- A significant number of T-Mobile USA devices have basic locking functionality (user-defined codes or patterns).
- Currently, 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.

- Recently, T-Mobile USA began preloading on select devices Lookout's Automatic App Security product, which is automatically activated when the device is powered on (scanning app downloads and performing other periodic device scans) thus, eliminating the need for a user to register.
- 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, 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.
- Most recently, 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 2012, 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 in early 2013 and will continue to develop its processes to improve the effectiveness of this shared database.