July 1, 2013

Kris Monteith, Acting Bureau Chief
Consumer and Governmental Affairs Bureau
Federal Communications Commission
445 12th Street, SW
Washington, D.C. 20554

Re: CTIA Stolen Smartphones Status Update

Dear Ms. Monteith:

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, with completion 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: Michael Carowitz
Charles Mathias

Attachment

APPLE:

Apple introduced a new Find My iPhone Activation Lock feature in the new iOS 7 (http://www.apple.com/pr/library/2013/06/10Apple-Unveils-iOS-7.html) that requires your Apple ID and password before you can turn off Find My iPhone, erase data or re-activate a device after it's been remotely erased. Apple expects that this feature, requiring a valid Apple ID and password to activate an iPhone should act as a powerful theft deterrent.

AT&T:

In the Summer of 2012, AT&T deployed a database that prevents both GSM and LTE stolen wireless device subscribers from accessing the AT&T network. On October 31, 2012 AT&T and T-Mobile successfully established connectivity to the global GSMA database and began sharing stolen device IMEIs to encompass the majority of GSM US coverage.

AT&T continues to share and block reported stolen wireless devices derived from the GSMA and its own database since the summer 2012. As new participating wireless service providers begin accessing these submissions, regional guidelines specific to North American sharing policies will be introduced. To this end, AT&T has initiated contact with other providers to discuss and coordinate best practices under the guidance of the Contributing Network Operator User Guide, to make it specific to North America.

BLACKBERRY:

BlackBerry has satisfied the April 30, 2013 commitment that "[s]martphone makers will implement a system to notify/inform users via the new smartphones upon activation or soon after of the smartphones' capability of being locked and secured from unauthorized access by setting a password."

A device password icon appears in the "Setup Buffet," which is automatically presented to the user at the end of the out of box experience of BlackBerry 10 devices.

CTIA:

CTIA worked with smartphone makers 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. All smartphone maker signatories to the Initiative have met this benchmark.

Further, on June 10th, CTIA provided to the FCC the following documents addressing stolen phones (attached hereto):

(1) A Fact Sheet on Wireless Provider Databases;
(2) A Fact Sheet explaining why a permanent, message-based "Kill Switch" is inadvisable;
(3) Three Improvements to Address Smartphone Safety;
(4) A List of Third Party Anti-Theft (locking, wiping and tracking) Applications; and
(5) An Overview of the GSMA IMEI Database Access Policy for Law Enforcement Agencies and Trusted Third Parties.

In addition, on June 13th, representatives from CTIA, Apple, Microsoft, Motorola/Google, and Samsung met with the New York State and San Francisco Attorneys General to discuss additional potential solutions to assist law enforcement with the issue of phone theft. CTIA explained that carriers, device manufacturers, operating system providers, app developers and content creators all have taken a number of steps to help consumers in the event their devices are stolen. CTIA stressed that the best solution to address this issue is a holistic one. Consistent with this Voluntary Initiative, CTIA explained that consumers must be aware of their surroundings and use the apps, tools and features to remotely lock, wipe and track their devices. CTIA also emphasized the need to identify and prosecute thieves aggressively and make it illegal for those who try to manipulate devices' identification numbers by passing Senator Schumer's bill.

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:

- **Mobile security page on Cellcom's website: www.cellcom.com/security** The homepage for Cellcom's website features a link on mobile security to educate customers on how to protect their smart phone and personal information. This includes encouraging customers to use a pass code to lock their devices, using a mobile security app, and backing up photos, videos, contacts and emails. Recommendations are also given to assist customers who have a missing phone. Links are provided to CTIA's website for more detailed information on how to set a password and to view a comprehensive list of anti-theft protection apps.

- **Mobile security section on the Entertainment & Apps page of Cellcom's website:**

Highlights mobile security apps for Android, Blackberry and Windows devices, as well as for tablets.
    - http://www.cellcom.com/entertainment/android_mobilesecurity/
    - http://www.cellcom.com/entertainment/tablet_mobilesecurity/
    - http://www.cellcom.com/entertainment/Blackberry_mobilesecurity/
    - http://www.cellcom.com/entertainment/windowsmobile_mobilesecurity/
- **Auto-generated "Welcome" email** that is sent after every smartphone purchase includes a link to Cellcom's mobile security page.

- **Passwords** are encouraged during sale of a smartphone.

HTC:

HTC regards phone theft as a serious issue and has worked closely with its business partners to meet its obligations under the Voluntary Initiative. As required by the Voluntary Initiative, HTC has implemented notifications to users during the initial device setup of the smartphone's capability of being locked and secured by a password for all phones receiving FCC certification on or after April 30, 2013.

New HTC Android smartphone models include a screen during the initial device setup that will inform users that they can set a password to prevent unauthorized access through the Security sub-menu in the device Settings menu. This notice also includes a link that users can press to go directly to the password setup screen. New Windows Phone models include a message immediately after the initial device setup process informing users that they can set a password to prevent unauthorized access. HTC is working to add this notification to some existing smartphone models during scheduled software updates so that new devices sold in those product lines may provide the notification during initial device setup.

HTC also provides step-by-step instructions for password locking and other included security features (*e.g.*, data encryption) via its website and user guides. Additionally, HTC trains its customer care representatives to help customers set the password on their device. Beyond its commitment to the Voluntary Initiative, HTC will continue to explore options for improving device security and reducing phone theft.

MICROSOFT / NOKIA:

Microsoft has met the Voluntary Initiative's April 30, 2013 benchmark. Specifically, Microsoft implemented a process for notifying users of a smartphone with Microsoft's Windows Phone 8 operating system of the device's capability of being locked with a password. Immediately after completion of the device setup process, a message (generated by the operating system) appears in the user's short messaging

service application containing a link to the Windows Phone welcome site. Upon clicking the link, the user accesses a web page featuring capabilities, including the ability to use a lock screen password. Clicking on a "learn more" link presents the user with specific instructions regarding how to set a password through the smartphone's settings.

MOTOROLA:

Motorola has satisfied the April 30, 2013 commitment to implement a system to notify/inform users via new smartphones upon activation or soon after of the smartphones' capability of being locked and secured from unauthorized access by setting a password. Specifically:

One hour after setup following activation of a phone, the following notification appears, which includes a link to activate the device administrator:

"Protect your phone: You can locate, lock and even wipe your phone when you link to a Google account and sign in at www.motorola.com/support. It's really simple."

If the user has not set a PIN/Password within 10 days of initial setup of the phone, a notification will be made in the notification bar stating: "PROTECT YOUR PHONE. Touch here to set up a pattern, PIN, or password."

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.

SAMSUNG:

Samsung has embedded into the GALAXY S4 device a technology solution in partnership with a third party. The solution cannot be removed by a factory reset once the app is installed by the consumer and activated. When a protected Samsung GALAXY S4 is stolen, the third party Recovery Services Team can work with law

enforcement globally to get the device back. Users can also remotely lock their device to make it inoperable, locate their device or wipe the internal memory on the device to protect personal data. This technology solution will be available early this summer and details about product and pricing will be announced shortly.

Samsung will continue to look for opportunities to innovate in security and phone theft deterrent technologies.

SPRINT NEXTEL:

In the second quarter of 2013, Sprint has continued to work aggressively towards educating our customers on smartphone safety and implementing systems to help curb smartphone theft. For example, Sprint now includes in every customer bill the following bill message:

> "Sprint encourages you to set a phone passcode or lock to help prevent unauthorized access. See your phone's user guide for instructions. Also consider downloading a security app for your phone. Report stolen phones to Sprint to protect your account. For more information visit sprint.com/stolenphone."

All new Sprint devices include step-by-step directions in the applicable user's guide on how to lock the devices and information on applications for locating and protecting lost/stolen devices. Sprint also sends monthly e-letters to customers that include information on using Lookout Mobile Security and other similar applications to track and remotely protect a lost or stolen device.

Sprint's outreach also includes our prepaid customers. All new prepaid customers now receive SMS messages directing them to Boost or Virgin Mobile web pages dedicated to helping customers in handling lost/stolen smartphones, encouraging the use of passcodes and highlighting the benefits and availability of mobile security applications.

Of course, Sprint is continuing to work diligently to implement the national LTE lost/stolen database and is on track to meet the implementation date.

T-MOBILE USA:

T-Mobile USA ("T-Mobile") continues efforts to help deter mobile handset theft. The company prevents use of stolen devices internal to its network. In addition, T-Mobile has established connectivity to the GSMA Global IMEI database, and through that mechanism acts on stolen device information 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 wireless industry/FCC agreement on handset theft mitigation (FCC PROTECT Initiative). The company is on track for meeting the requirements for an LTE common database by the November 30, 2013 deadline.

A significant number of T-Mobile USA devices have basic locking functionality with passwords (user-defined codes or patterns). The company has engaged in efforts to educate consumers about these features and has informed consumers about applications to safeguard handsets via remotely locking/locating/erasing data from smartphones. T-Mobile preloads "Lookout" (with a visible icon) on a substantial number of its Android-based handsets. Customers also have access to premium versions of "Lookout" that permit users to remotely lock and/or wipe data from handsets. Furthermore, tracking, remote locking, and wiping are available to users that elect to sign up with "Mobile Security" service, which is offered through T-Mobile US handset insurance partner, Asurion.

T-Mobile has taken steps to educate consumers about smartphone theft protections and preventative measures in general, as well as its product offerings, through blogging, social media tools, and its website.

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 GSMA database to share information on stolen devices. Moreover, Verizon Wireless plans to begin utilizing the multi-carrier database by the fall of this year and will continue to develop its processes to improve the effectiveness of this shared database. In addition, Verizon Wireless is investigating options to share with others its database of stolen CDMA devices to extend the effectiveness of that database.