October 1, 2012

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

Re: CTIA Stolen Smartphones Quarterly 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 second 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 the 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 has enhanced its privacy and safety communication and incorporated it into new and existing customer communication.

The AT&T sales and support teams have reinforced adding smartphone passwords after activation and provided guidance on downloading apps that help to protect devices and personal information.

AT&T launched a blacklist database of AT&T customers' smartphones in Summer 2012.

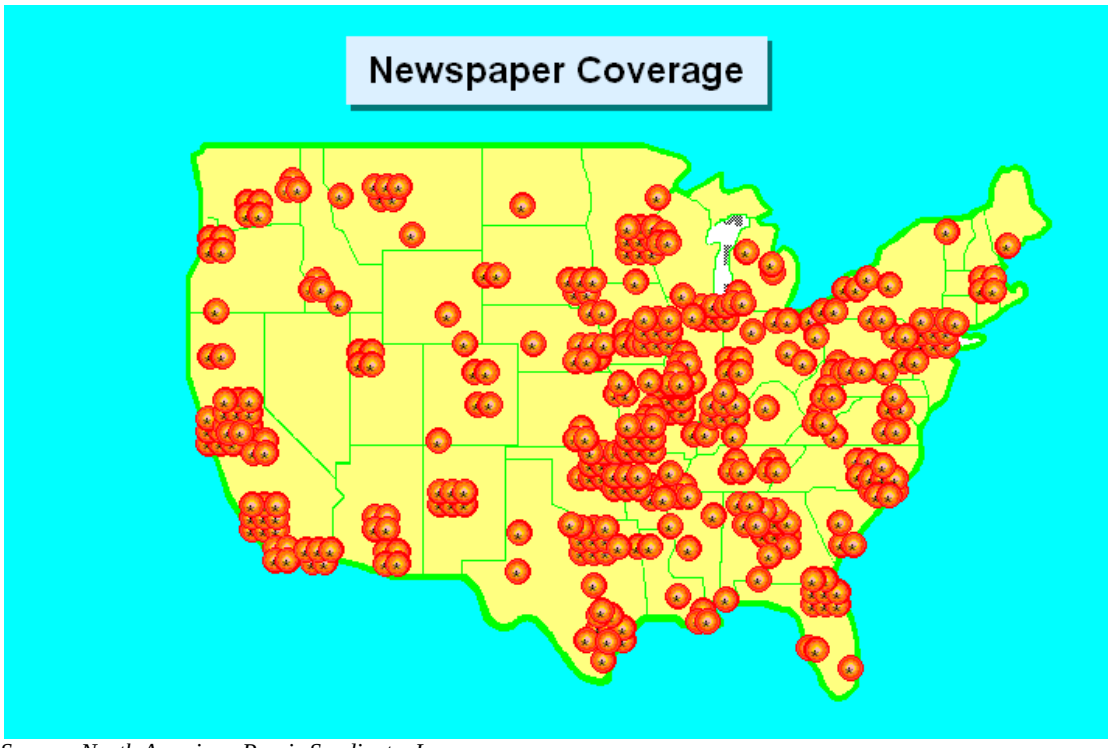
AT&T is on schedule for participation in the implementation of the shared blacklist database blocking capability by October 31, 2012.

CTIA:

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.

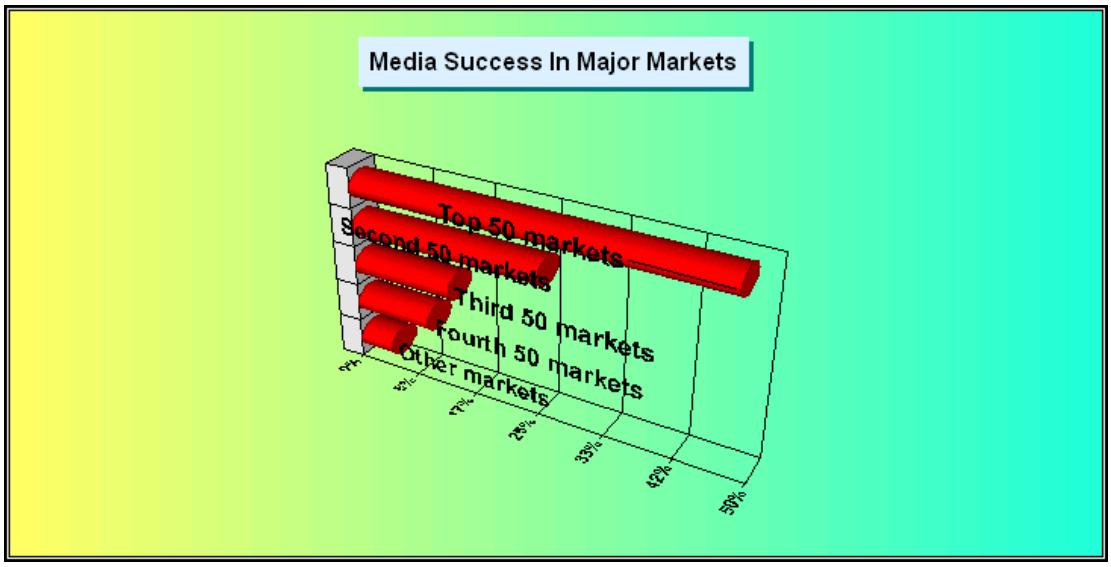
CTIA engaged an advertising agency to develop and produce a Public Service Announcement ("PSA"), which was completed in late September 2012. CTIA will work with the Commission, the law enforcement community, and television broadcast stations throughout the country to encourage placement of the PSA. CTIA President and CEO Steve Largent plans to jointly unveil the PSA with Chairman Genachowski in October 2012 and CTIA will provide a link to the PSA on its website.

In addition, CTIA drafted and broadly distributed to newspapers throughout the country a mat release featuring detailed information about steps that consumers can take to help prevent smartphone thefts and safeguard their user information. As of September 25, 2012, this release generated 1,916 news articles in 49 different states with a readership of 9,597,456. The sites it was on were viewed by 130,483,005 unique visitors per month.



Source: North American Precis Syndicate, Inc.

Approximately 47% of the placements are from the top 50 markets; 25% from the second 50 markets; 13% from the third 50 markets; 10% from the fourth 50 markets; 5% from other markets.



Source: North American Precis Syndicate, Inc.

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 smartphones 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:

- 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 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)

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:

As of June 2012, Sprint Nextel has taken a number of steps to implement the voluntary commitment including: (1) implementing a database that prevents CDMA smartphones that are reported as lost or stolen from being activated or provided service on our 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.

Since June, Sprint also has continued 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 also worked with its total equipment protection vendor Asurion to established the "vanity" URL: http://www.protect2win.com through which Sprint customers can learn about the total equipment protection program and where customers that download the Total Equipment Protection ("TEP") mobile application, which allows customers to locate, lock, and wipe their smartphones, are automatically entered to win $10,000 or one of Sprint's daily $10 gift cards.

In addition, Sprint has continued to communicate via social media with its customers regarding safe smartphone usage. For example:

(1) On August 9, Sprint tweeted its followers two tweets outlining how customers can protect their phones from loss, theft and damages and announcing the "Protect2Win" contest for customers that download Sprint's total equipment protection plan mobile application.
(2) On August 11, 2012, Sprint tweeted its followers on Twitter a message containing information on what to do if a smartphone is lost or stolen including a link to a help page.
(3) On August 29, Sprint posted to Facebook information about the Sprint Guardian applications along with information on helping kids use their smartphones safely and responsibly.
(4) On August 30, Sprint tweeted its followers on Twitter a message containing information on helping kids use smartphones safely and responsibly.

T-MOBILE USA:

T-Mobile USA is making substantial progress to meet the deadlines established for the provisions of the Wireless Industry/FCC Agreement on Handset Theft Mitigation. Below is a summary of T-Mobile USA's current progress on satisfying requirements with deliverables set forth in 2012.

T-Mobile USA is on track to meet the October 31, 2012 date for completion of blocking on own network and is on track for meeting the requirements associated with the common GSM database system.

- T-Mobile USA prevents use of stolen devices internal to its network, and has established connectivity to the GSMA Global IMEI database that is ready for use by other carriers 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 Industry/FCC Agreement.

T-Mobile USA is on schedule to meet the December 31, 2012 deadline to educate consumers about features to secure/lock new smartphones with passwords.

- A significant number of T-Mobile devices have basic locking functionality (user-defined codes or patterns).
- Currently, T-Mobile preloads an application called "Lookout" (with a visible icon) on most Android-based handsets, which allows customers to track or locate misplaced devices.
- Tracking, remote locking, and wiping also is available to customers that elect to sign up with Mobile Security service, which is offered by our partner Asurion that offers handset insurance.

T-Mobile USA is on schedule for the December 31, 2012 deadline to make substantial progress to inform consumers about applications to remotely lock/locate/erase data from smartphones.

- T-Mobile's implementation team is considering options to better educate consumers about applications to remotely lock/locate/erase data from smartphones.
- T-Mobile has begun efforts to provide customers information on safeguarding handsets and handset security offerings as part of the collateral materials (specifically the "Start-up Guide") found in smartphone packaging.

T-Mobile USA began initiating educational initiatives prior to July 1, 2012.

- In June 2012, T-Mobile 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 to the public.

- 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.
- Implementation team is considering other measures to further educate consumers about smartphone theft, protections and preventive measures.

VERIZON WIRELESS:

In May, 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. Verizon Wireless is actively developing a solution for expedited implementation that will prevent use of 4G LTE smartphones that have been reported to the carrier as lost or stolen with different SIM cards.

Verizon also is participating in industry discussions on the development of an industry-wide database to perform a similar function. Moreover, Verizon has obtained access to and begun initial testing of its systems with an existing multi-carrier stolen phone database and plans to participate fully in the database as soon as possible.