Daniel S. Mead
President & Chief Executive Officer

verizonwireless

Verizon Wireless
One Verizon Way
VC44E006
Basking Ridge, NJ 07920

Phone 908 559-1078
Fax 908 766-3790
Dan.mead@verizonwireless.com

April 11, 2012

The Honorable Henry A. Waxman
U.S. House of Representatives
2204 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Anna G. Eshoo
U.S. House of Representatives
205 Canon Building
Washington, D.C. 20515

The Honorable Edward J. Markey
U.S. House of Representatives
2108 Rayburn House Office Building
Washington, D.C. 20515

Dear Representatives Waxman, Eshoo, and Markey:

Thank you for your letter outlining your concerns about stolen mobile devices. Verizon Wireless has a long history of protecting our customers, including taking action to stop illegal telemarketing calls, spam text messages, and pretexting to obtain customer information. In addition, we have worked closely with Public Safety on a number of projects such as 911, Amber Alerts, Wireless Priority Service, and wireless emergency alerts. Verizon Wireless' long-standing commitment to deterring crime includes preventing reactivation on our network of all devices that our customers have reported to us as lost or stolen. And most recently we demonstrated our commitment to protecting our customers by playing an instrumental role in developing an industry-wide initiative to combat wireless device theft that was announced yesterday. My response to your questions below provides details regarding Verizon Wireless' long-standing commitment to these goals.

1. What company policies and guidelines do you currently have in place that relate to cell phone theft or loss?

Customers can and do contact Verizon Wireless any time of day or night to report a device as lost or stolen by:

- calling Customer Service toll-free at (800) 922-0204; or
- accessing our website at www.VerizonWireless.com.

The landing page of the Verizon Wireless website includes a prominent section labeled "Lost or Stolen Device." By clicking on this section, the customer may review a video explaining how to suspend and reactivate service on a lost or stolen device. After logging into her account, the customer may select "I Want To Suspend or Reconnect Service" on the first screen and follow the prompts. (See screenshots 1-4).

Once a customer contacts us, we suspend service on that device so that it can no longer connect to our network.

Further, Verizon customers are able to remotely locate and lock their smart devices using web-based applications provided by the device operating system (e.g., Apple or Google) or other third party providers, such as device insurance companies. For example, Verizon Wireless customers may purchase insurance from Asurion to replace/repair lost, stolen, or damaged devices. Verizon Wireless' "Total Equipment Coverage" package includes Asurion's insurance, an extended warranty, and access to Asurion's "Mobile Recovery" application. When downloaded to the device from MyMobileRecovery.com, this application allows customers to:

- locate a lost device (location shown geographically on a map);
- sound a phone alarm to find a lost device;
- remotely lock a device to secure the customer's data; and
- remotely wipe a device's contact list.

Verizon Wireless' long-standing commitment to deterring crime includes preventing reactivation on our network of all devices that our customers have reported to us as lost or stolen. When a customer reports a lost or stolen device, we add that device to our "negative list" file. Our "negative list" was developed for devices that use our CDMA network, and helps Verizon Wireless prevent the reactivation of any CDMA device, including the iPhone 4 and iPhone 4S that are compatible with the Verizon Wireless network, that has been reported to us as lost or stolen. Devices that access our new 4G LTE network are SIM card-based. While our "negative list" will prevent the activation of new service on a 4G LTE device that has previously been reported to us as lost or stolen, it will not currently prevent a customer from placing an active SIM card in a stolen 4G LTE device and then using the device. We are developing a solution that will prevent use of 4G LTE devices that have been reported to us as lost or stolen with different SIM cards.

2. Do you have an evaluation process to ensure that these policies keep up with advancing technologies and changing criminal tactics?

Yes. Verizon is a leader in securing networks and technology and is constantly working to stay abreast of advancing technologies, see response to Question 1 above, and changing criminal tactics, see response to Question 4 below.

3. Law enforcement and others have suggested that the ability to disable remotely mobile devices would reduce or eliminate resale value and thus lessen the incentive for cell phone theft. What are your views on this technology as a deterrent to theft?

As described above, Verizon Wireless does not allow devices that our customers have reported to us as lost or stolen to be activated on our network, thus reducing the value of the device to criminals. The ability to render the device completely useless does not currently exist and, in any event, presents significant customer care concerns. For example, even if the capability existed, we would hesitate to irreversibly render an expensive customer device completely useless due to the possibility that a device reported as lost or stolen may be later recovered.

4. Does your company cooperate with law enforcement to retrieve lost or stolen phones? If so, how?

Verizon Wireless has a team of professionals devoted to addressing theft and fraud and assisting law enforcement, including in connection with lost or stolen devices. For instance, Verizon Wireless has procedures in place and works with law enforcement to locate stolen devices. Verizon Wireless also supports law enforcement efforts to investigate mobile device theft, has donated mobile devices for use by law enforcement in investigations, and affirmatively reports device theft that is suspected to be the result of organized crime. Moreover, if law enforcement notifies us that it has recovered a device belonging to one of our customers, we would facilitate its return to the customer

5. If your company has knowledge that a specific phone has been reported stolen, do you allow such a phone to be subsequently reactivated with a different phone number? If yes, please explain?

No, Verizon Wireless never knowingly allows a stolen phone to be activated on our network. As described above, we are currently able to prevent the activation of a stolen CDMA phone, including the iPhone 4 and iPhone 4S models that are compatible with the Verizon Wireless network, through our "negative list," and we are aggressively working to develop a solution to address certain limitations we have when a customer, without Verizon Wireless's interaction or knowledge, places an active SIM card into a stolen 4G LTE device.

6. Australia has implemented a cell phone "blacklisting" program in which phones that have been reported stolen are placed on a list and cannot be reactivated if an individual brings them in to a local carrier. This has significantly reduced cell phone theft in Australia. Would a similar program work in the United States?

As announced jointly by the FCC, CTIA and members of the law enforcement community yesterday, Verizon Wireless is committed to and actively participating in the development of industry standards for a common database of stolen LTE devices so that a lost or stolen device originally activated on one carrier's network cannot be activated on another carrier's network. The details of this cooperative voluntary initiative are included in Exhibit 1.

7. What more can be done to protect consumers? Please include any additional insights that you believe we might find helpful or relevant.

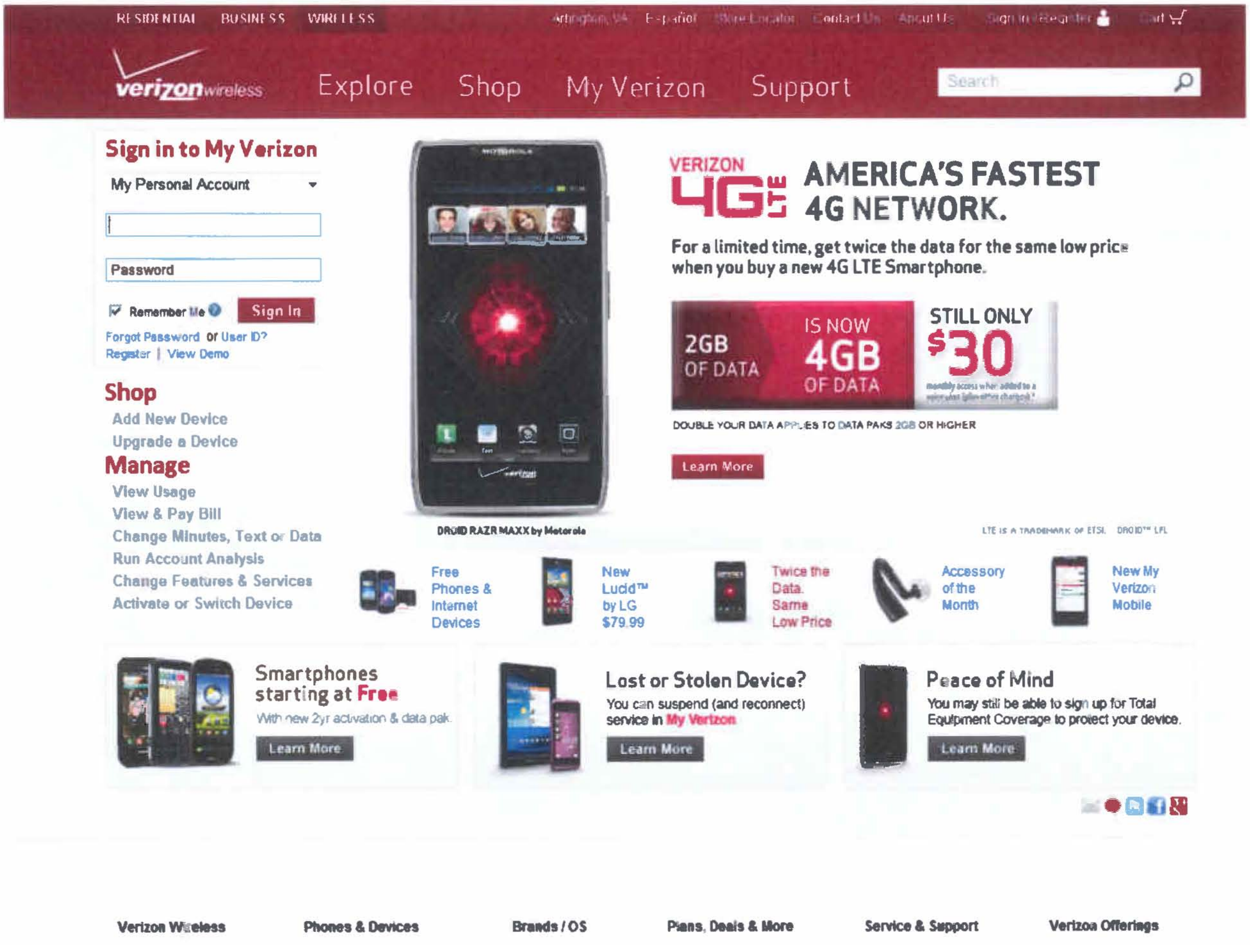
Verizon Wireless is constantly working to better educate our customers to provide the best customer experience. For example, in our free Wireless Workshops offered in stores and online, Verizon Wireless experts teach customers about the features and functions of the devices and services we offer. As part of many of these courses, our instructors teach students how to set up passwords on their devices, and some courses teach about applications that allow customers to remotely locate, lock, and wipe content from devices. Further, as more fully described in the cooperative voluntary initiatives agreed to by Verizon Wireless and other wireless industry participants yesterday, Verizon Wireless will provide additional information to our customers to alert them to and improve their understanding of the various tips and tools available to them, such as passwords and applications, to prevent and mitigate the harms associated with mobile device loss and theft.

Thank you for providing this opportunity to explain Verizon Wireless' commitment to reducing mobile device crime and fraud. Please let myself or Peter Davidson know if you have further comments or concerns.

Sincerely,

Screen Shot #1

http://www.verizonwireless.com/b2c/index.html



Sign in to My Verizon

My Personal Account

Password

☑ Remember Me Sign In

Forgot Password or User ID?
Register | View Demo

Shop

- Add New Device
- Upgrade a Device

Manage

- View Usage
- View & Pay Bill
- Change Minutes, Text or Data
- Run Account Analysis
- Change Features & Services
- Activate or Switch Device

DROID RAZR MAXX by Motorola

VERIZON 4G LTE AMERICA'S FASTEST 4G NETWORK.

For a limited time, get twice the data for the same low price when you buy a new 4G LTE Smartphone.

2GB OF DATA IS NOW 4GB OF DATA STILL ONLY $30 monthly access when added to a [illegible]

DOUBLE YOUR DATA APPLIES TO DATA PAKS 2GB OR HIGHER

Learn More

LTE IS A TRADEMARK OF ETSI. DROID™ LFL

Free Phones & Internet Devices

New Lucid™ by LG $79.99

Twice the Data. Same Low Price

Accessory of the Month

New My Verizon Mobile

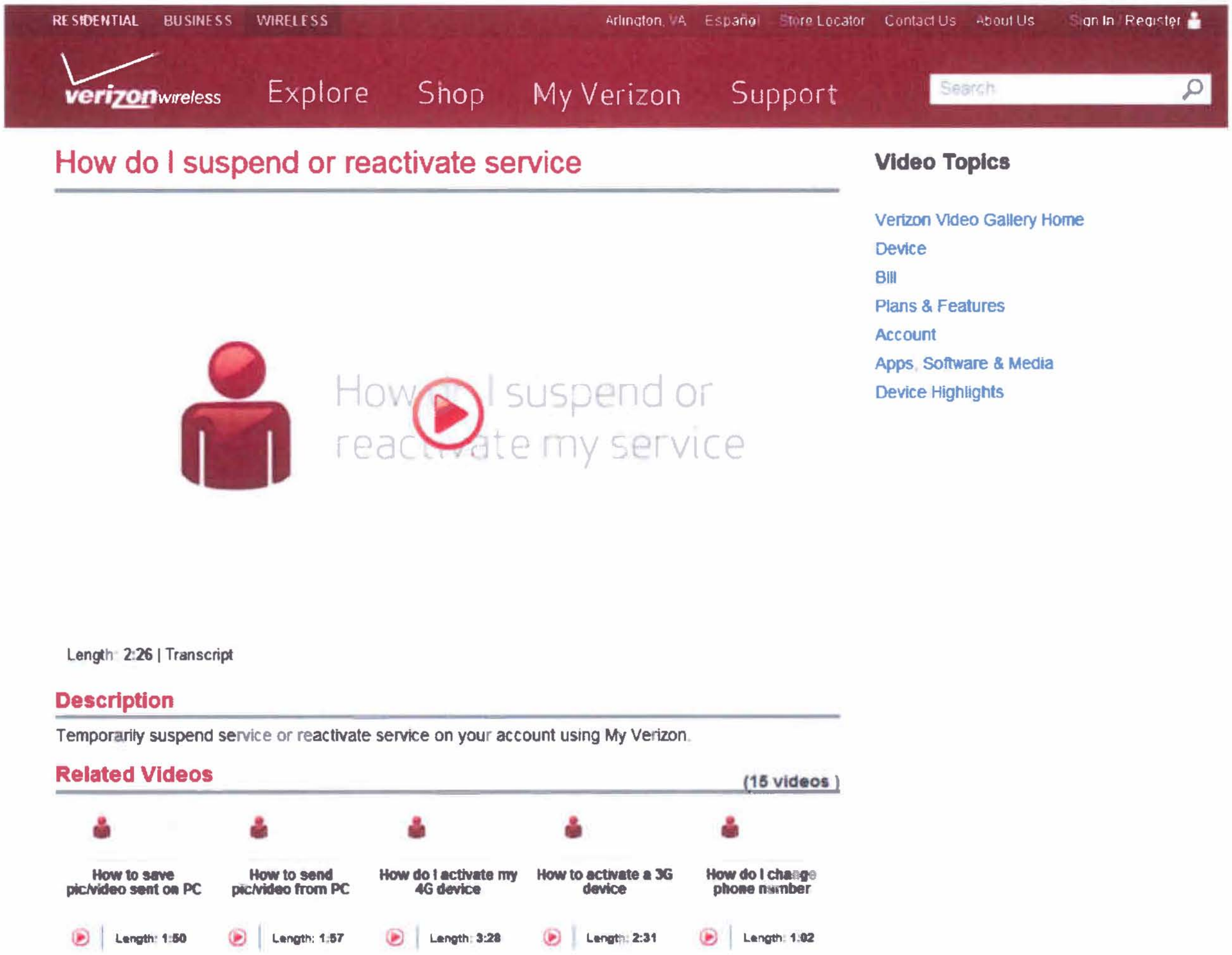
Smartphones starting at Free
With new 2yr activation & data pak
Learn More

Lost or Stolen Device?
You can suspend (and reconnect) service in My Verizon
Learn More

Peace of Mind
You may still be able to sign up for Total Equipment Coverage to protect your device.
Learn More

Verizon Wireless | Phones & Devices | Brands / OS | Plans, Deals & More | Service & Support | Verizon Offerings

SCREEN SHOT #2
https://videos.verizonwireless.com/How-do-I-suspend-or-reactivate-svc/v/1MBBH0VJ/



How do I suspend or reactivate service

Length: 2:26 | Transcript

Description

Temporarily suspend service or reactivate service on your account using My Verizon.

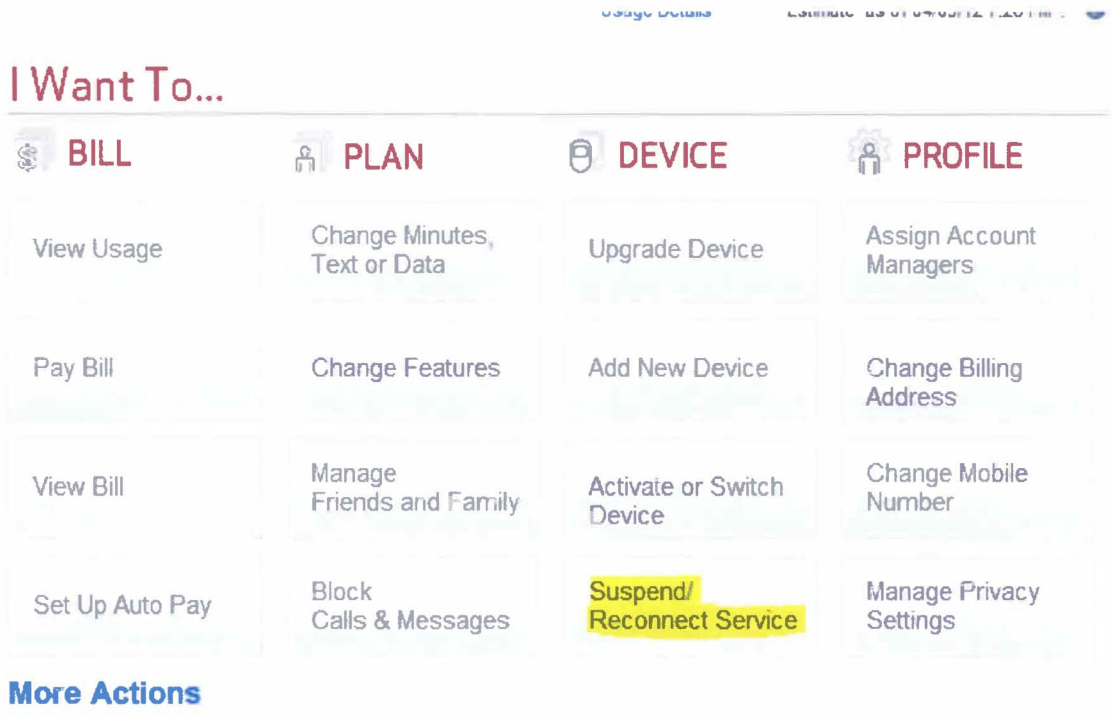
Related Videos (15 videos)

How to save pic/video sent on PC	Length: 1:50
How to send pic/video from PC	Length: 1:57
How do I activate my 4G device	Length: 3:28
How to activate a 3G device	Length: 2:31
How do I change phone number	Length: 1:02

Video Topics

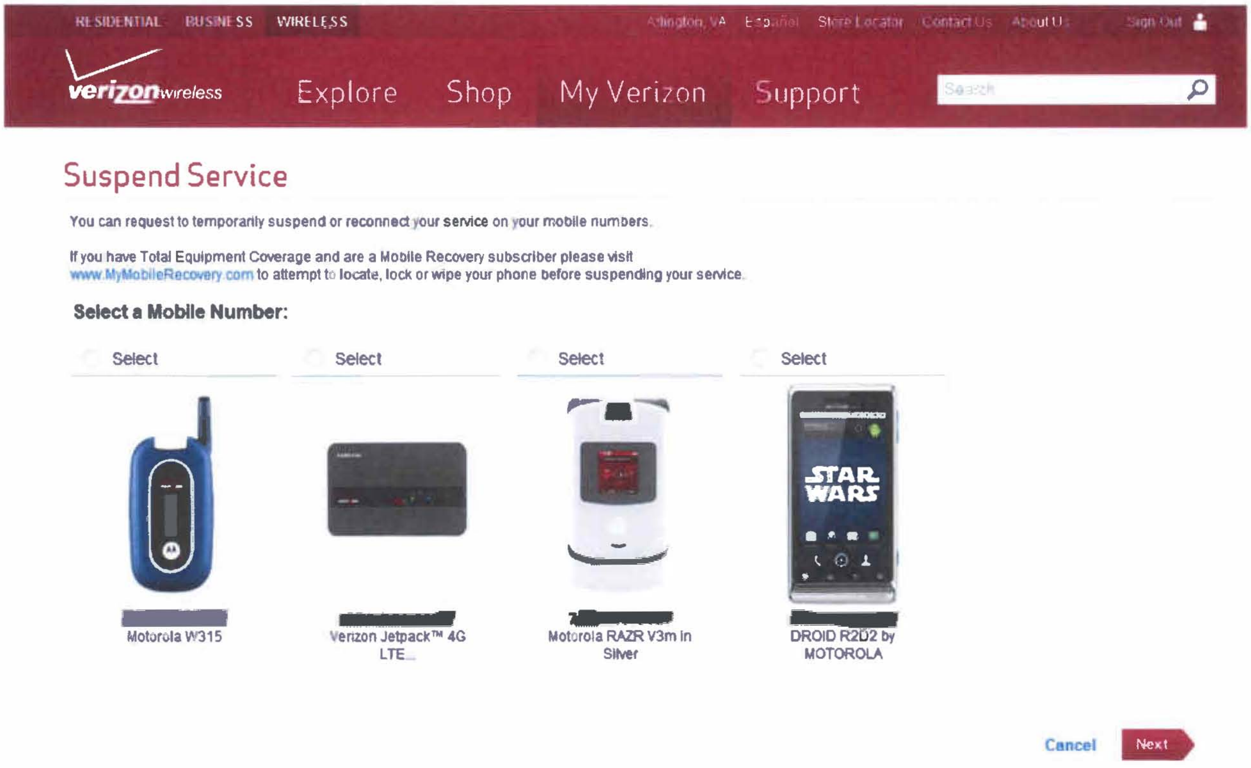
- Verizon Video Gallery Home
- Device
- Bill
- Plans & Features
- Account
- Apps, Software & Media
- Device Highlights

Screen Shot #3
https://ebillpay.verizonwireless.com/vzw/secure/router.action



SCREEN SHOT #4

https://ebillpay.verizonwireless.com/vzw/accountholder/services/suspendResumeService.action



Suspend Service

You can request to temporarily suspend or reconnect your service on your mobile numbers.

If you have Total Equipment Coverage and are a Mobile Recovery subscriber please visit www.MyMobileRecovery.com to attempt to locate, lock or wipe your phone before suspending your service.

Select a Mobile Number:

○ Select ○ Select ○ Select ○ Select

[redacted]
Motorola W315

[redacted]
Verizon Jetpack™ 4G LTE...

[redacted]
Motorola RAZR V3m in Silver

[redacted]
DROID R2D2 by MOTOROLA

ATTACHMENT 1

NEWS RELEASE

April 10, 2012
Contact: Amy Storey
202.736.3207

CTIA Public Affairs
A Department of **CTIA–The Wireless Association®**

U.S. Wireless Industry Announces Steps to Help Deter Smartphone Thefts and Protect Consumer Data

Washington, D.C. – CTIA-The Wireless Association®, together with participating wireless companies, today announced they have worked with government officials and law enforcement to develop four steps to help deter smartphone thefts and protect consumer data. These four voluntary industry commitments by CTIA and our participating members will effectively address this issue while continuing to evolve as new wireless products and services become available.

The four steps are:

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.

"CTIA and its members have always been strong advocates for the safety and protection of America's wireless users. Today's announcement is yet another example of our industry's continued dedication to advance public safety and enhance the security and protection of our customers. By working closely with law enforcement, these four steps will help deter smartphone theft and keep America's wireless users safe," said Steve Largent, President and CEO, CTIA-The Wireless Association.

Beginning June 30, 2012, CTIA will publish quarterly updates on its website and submit a copy to the Federal Communications Commission, detailing progress, benchmarking milestones and indicating completion by industry and provider of the following deliverables: implementation of databases, information about applications to locate/lock/erase data from smartphones and efforts to educate consumers about smartphone theft, protections and preventative measures.

For more information, please visit: www.ctia.org

###

CTIA-The Wireless Association® (www.ctia.org) is an international organization representing the wireless communications industry. Membership in the association includes wireless carriers and their suppliers, as well as providers and manufacturers of wireless data services and products. CTIA advocates on behalf of its members at all levels of government. The association also coordinates the industry's voluntary best practices and initiatives, and sponsors the industry's leading wireless tradeshows. CTIA was founded in 1984 and is based in Washington, D.C.