

Set forth below are the terms of the voluntary industry commitment reached between members of CTIA-The Wireless Association® and the Federal Communications Commission on April 10, 2012:

“Working with the Federal Communications Commission and the Major City Police Chiefs, CTIA-The Wireless Association® and participating wireless companies voluntarily commit to the following four actions to deter smartphone phone theft and protect personal data:

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 all smartphones reported by their customers as stolen from being activated and/or provided service on their own networks. U.S. GSM providers will participate in a common database, using unique smartphone identifying numbers, designed to prevent smartphones reported by their customers as stolen from being activated and/or provided service on the network of another U.S. GSM provider (“GSM database system”). The above database solutions will be implemented by October 31, 2012. The GSM database system will, as operationally and technologically feasible, be made interoperable with appropriate international GSM stolen cell phone databases.

In addition, U.S. wireless providers will participate in a common database, where technologically feasible, of the unique identifying numbers of LTE smartphones reported by customers as stolen, and will implement systems to prevent such smartphones from being reactivated or reused on providers’ LTE networks (“LTE database system”). The LTE database system will, as operationally and technologically feasible, be made interoperable with appropriate international LTE stolen cell phone databases. Wireless industry representatives will continue to communicate with law enforcement representatives participating in industry standards bodies regarding implementation of these commitments.

Milestone: Completion of blocking on own network and of common GSM database system: October 31, 2012. Completion of all other deliverables above: November 30, 2013.

2(A). Notify Consumers of Features to Secure/Lock Smartphones with Passwords.

Smartphone 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.

Milestone: Completion: April 30, 2013.

2(B). Educate Consumers About Features to Secure/Lock Smartphones with Passwords.

Smartphone makers will include information on how to secure/lock new smartphones in-box and/or through online “Quick Start” or user guides.

Milestone: Completion: December 31, 2012.

3. Inform Consumers about Applications to Remotely Lock/Locate/Eraser Data from Smartphones. Wireless providers will inform consumers, including through email or text messages, about the existence of – and access to – applications that can lock/locate/erase data

from smartphones. Wireless providers will educate consumers about how to access these applications, including applications preloaded onto smartphones, in an easy-to-find place.
Milestone: Substantial Progress: December 31, 2012. Completion: April 30, 2013.

4. Educate Consumers about Smartphone Theft, Protections, and Preventative Measures.

The wireless industry will launch a campaign to educate consumers regarding the safe use of smartphones and highlight solutions described in 1 through 3 above through a range of initiatives that will include Public Service Announcements, with media buys, and the use of unique websites, social media, and more.

Milestone: Educational initiatives will begin by July 1, 2012.

Progress Benchmarks

CTIA will publish quarterly updates on its publicly-available website beginning June 30th, 2012, 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.

The Commission may open a proceeding if progress on the above deliverables falls behind schedule.”