



8410 W. Bryn Mawr Ave
Chicago, IL 60631
www.uscellular.com

April 11, 2012

Hon. Henry A. Waxman
Ranking Member
House Energy & Commerce Committee
2125 Rayburn House Office Building
Washington, DC 20515

Hon. Anna G. Eshoo
Ranking Member
Subcommittee on Communications and Technology
House Energy & Commerce Committee
2125 Rayburn House Office Building
Washington, DC 20515

Hon. Edward J. Markey
House Energy & Commerce Committee
2125 Rayburn House Office Building
Washington, DC 20515

Dear Congressmen Waxman & Markey & Congresswoman Eshoo:

In response to your letter dated March 23, 2012, U.S. Cellular Corp offers the following responses your questions:

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

We currently have a policy prohibiting the activation of non-U.S. Cellular devices on our network under any circumstance. This effectively eliminates the risk of using stolen cell phones from other carriers on our network.

For U.S. Cellular devices, we currently have the ability to mark specific devices by their electronic serial number/MEID in our billing and activation systems as being lost or stolen within the US Cellular market in which this has been reported. Our current billing and activation system has had to be modified over time to accommodate the growth in our business and our expansion into new markets. Once a handset is reported lost or stolen the device cannot be activated within that market.. Because our billing and activation systems is not integrated across markets– and we have 6 of them presently – it is possible for these devices to be activated in one of our other markets. U.S. Cellular is in the process of a multi-year project to update our back-office operating systems. Our new system enhancements will effectively prohibit any U.S. Cellular device reported to us as being lost or stolen from being activated anywhere on

our network. We are currently scheduled to begin field implementation in Q1 2013 and to be complete by Q4 2013.

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

We are constantly reviewing and revising our policies to ensure that they keep up with changes in our business, in technology, and in customer needs. We have an internal policy review board that is responsible for this process. We also have a Fraud Detection group who, among other things, monitor suspicious transactions and trends to help us guard against misappropriated devices .

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?

All phones sold today come with the ability for the user to lock the phone. Additionally, device applications exist on all major smartphone operating systems (Android, Windows Phone, and iOS) to enable users to remotely locate, lock, and wipe the contents of the device. Many of these products are available free of charge and can be found in the major application marketplaces. We are also aware of sophisticated tools that may be available that may be able to override some of these capabilities. We agree with law enforcement that use of these applications will have some effect on the resale marketplace if widely adopted by consumers but to what degree we do not know.

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

Consistent with legal requirements and privacy rules, we assist law enforcement with any requests we receive from them regarding investigations into stolen phones.

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.

See answer to item one above.

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?

We do not know but it seems reasonable to assume that similar results would be seen in the United States but for GSM devices only . It is important to note that Australia and most of Europe depend primarily on GSM cellular networks. In the US, we have GSM and CDMA networks. GSM networks are fundamentally designed for interoperability. The technology allows a user to simply replace the SIM card in the phone for one carrier with the SIM card for another carrier. This fundamental portability does not exist in CDMA networks like the one operated by U.S. Cellular and certain other US carriers. While technically possible, it is difficult to make a CDMA phone from one network operate on another

network. Doing so requires access to specialized software on the device and the ability to update that software through a computer or specialized device. This fundamental difference in the ease of transferring GSM phones compared to the relative difficulty of CDMA phones is reflected in the market prices for GSM phones being higher than CDMA and as a consequence we believe that GSM phones have greater resale value to criminals than CDMA phones .

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

Beyond the items discussed above, we believe it is important for consumers to be cognizant of their surroundings and to keep devices in pockets and/or bags when not in use. If a device is stolen, report it to your wireless provider immediately and to local police authorities.

If you have any questions regarding these responses, please feel free to contact me for further information.

Sincerely,



John C. Gockley
Vice President – Legal & Regulatory Affairs