Daniel R. Hesse
Chief Executive Officer

Sprint Nextel
6200 Sprint Parkway
Overland Park, KS 66251

April 11, 2012

Representatives Waxman, Eshoo, and Markey
United States House of Representatives
Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515-6115

Re: Sprint Procedures for Lost and Stolen Cell Phones

Representatives Waxman, Eshoo, and Markey,

Thank you for your letter of March 23, 2012, and the opportunity to provide you more information regarding Sprint's policies and procedures addressing the loss and theft of cell phones. Sprint shares your concern about protecting consumers from the hazards and liabilities associated with cell phone loss and theft. In response, Sprint has developed a robust program to prevent unauthorized use of lost phones and to deactivate devices that are reported stolen. In addition, Sprint provides its customers a number of tools they can use to help protect themselves from the hazards that can accompany the loss or theft of a cell phone.

When a Sprint customer reports a Sprint-branded cell phone (CDMA or CDMA/WiMAX) lost or stolen, the first step Sprint takes is to check the account for fraudulent or unusual use and then place a lost or stolen restriction on the customer's account, which blocks all voice, text, and data use. That restriction remains on the account until the customer contacts us to let us know they have located the device, would like to activate a replacement device, or discontinue service. If the customer is replacing the lost or stolen device or discontinuing service, we place the lost or stolen device's electronic serial number (ESN) or mobile equipment identifier (MEID) in our Lost/Stolen database, which prevents the phone from being reactivated on the Sprint network.[1]

[1] Devices disabled in this manner can still be used to call 911 in case of emergencies.

dan.hesse@sprint.com *Office: (913) 794-1100* *Fax: (913) 794-1505*

In addition to Sprint's CDMA cell phone network, Sprint also operates an iDEN cell phone network in the US. Unlike CDMA devices, Sprint's iDEN phones employ SIM cards that contain customer account information and can be removed from iDEN devices. Sprint's process for disabling iDEN devices that are reported lost or stolen, however, is nearly identical to the process for Sprint's CDMA phones and Sprint does disable both the SIM card and the device based on unique numerical identifiers. Because the iDEN technology is unique, these phones cannot be activated on any of the other large national carrier's networks. Likewise, CDMA phones cannot be activated on AT&T or T-Mobile's networks, which operate using the GSM standard. Accordingly, the Sprint Lost and Stolen database is very effective in preventing stolen phones from being reactivated on the Sprint network.

In addition to implementing network and billing system protections to ensure that stolen phones are not misused or reactivated, Sprint also provides its customers with programs and applications that can help a consumer minimize the potential cost associated with a lost or stolen phone. For example, all Sprint smartphones have security settings or available applications that allow the customer to establish password protection or a "swipe" lock that will prevent the device from unauthorized use.

Sprint also encourages our customers to use applications that can track, lock, wipe, and even recover their personal information. For example, Sprint's Total Equipment Protection (TEP) plan partner Asurion, offers TEP customers a protection application that allows users to find a lost or stolen device, remotely lock the device, and erase stored personal data. The protection application also allows users to retrieve the device's data by periodically transferring that data to a remote server to be synchronized with the device. The application is available for many Sprint phones including 24 Android devices, 9 Blackberry devices, and 12 feature phones.

In the March edition of Sprint's e-newsletter for customers and in recent bill inserts, Sprint included a section on smartphone security, encouraging customers to consider downloading two of the industry's leading security applications that provide locate, lock, wipe, and recover capabilities, McAfee Mobile Security, which supports Android, Blackberry, and Symbian devices, and Lookout Mobile Security, which supports Android and iPhone devices. Similarly, in early April, Sprint began offering smartphone customers easy access to Norton Mobile Security Lite, a fully featured smartphone security application, via Sprint's "Sprint Zone" icon or the Sprint tab in Google Play.[2] Moreover, all Apple devices sold by Sprint come preloaded with an application that provides locate, lock, wipe, and recover functionality.

[2] See, http://newsroom.sprint.com/article_display.cfm?article_id=2231&view_id=7800.

To address the financial cost of lost and stolen phones, Sprint encourages our customers to participate in our TEP. Through the TEP, which is available for almost all of our smartphones and feature phones, customers can obtain replacement phones with the payment of a modest deductible when their phone is lost, stolen, or damaged. This program saves customers who have lost their phone or had one stolen from having to incur the full cost of a replacement phone.

Finally, as announced recently by the Chairman of the FCC, Sprint is working with a large group of CTIA members, mobile operators, operating system developers, and handset manufactures on a voluntary multiple point approach to deter phone theft and protect consumers. Through this effort, companies have agreed to notify smartphone purchasers of the importance of using a password to protect their devices, inform consumers on how to download smartphone security software, work towards technical solutions to prevent lost or stolen smartphones from being reactivated on their networks, and further educate consumers on the safe use of smartphones through a range of initiatives that may include a Public Service Announcement and the use of unique websites, social media, and more. Sprint has already implemented many elements of the plan including providing lost and stolen phone information on the website sprint.com/stolenphone.

Answers to Specific Questions

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

As outlined in greater detail above, Sprint provides consumers with numerous levels of protection in the event their phone is lost or stolen. While Sprint does not require its customers to use passwords, use location applications or purchase insurance, we make these services generally available and take steps to educate consumers about their importance.

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

Sprint has a large team of professionals dedicated to security and fraud prevention. The Corporate Security department within Sprint regularly evaluates security and anti-fraud measures affecting all aspects of our business to ensure that Sprint is one step ahead of changing criminal and other nefarious efforts. Nevertheless, criminal elements can be very creative and no one solution can address all criminal activity. A multiple solutions approach is required to combat cell phone loss and theft.

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 phone theft. What are your views on this technology as a deterrent to theft?

As described above, Sprint already has in place procedures and processes to disable phones that are reported lost or stolen and prevent them from being reactivated on our network. Similarly, we provide customers applications that can be used to locate, lock and wipe data from their phones remotely and security features that restrict access by unauthorized users. While these are important deterrents they will not eliminate theft. Smartphones are inherently valuable devices that can be used for many purposes even if they are not activated on a carrier's network. These are in essence small computers with intrinsic value even if disabled. Indeed, these phones have value even when disassembled for parts.

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

Sprint works cooperatively and in coordination with law enforcement on the national, state, and local level on a wide variety of issues including security and fraud prevention efforts and has a dedicated law enforcement assistance team. If a customer gives written authorization to provide information on a stolen phone to law enforcement, Sprint can trace a phone (provided the phone is still operating) and provide the location to law enforcement. Sprint has a standard form it provides to law enforcement for these purposes.

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.

Sprint does not reactivate phones that have been reported lost or stolen except when a customer subsequently finds a lost phone. In such cases the customer is required to provide substantive authentication that they are the owner of the phone and a current Sprint customer. If a customer provides authentication and the phone's unique numerical identifier is associated with the customer's account, Sprint may reactivate the phone.

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 to a local carrier. This has significantly reduced cell phone theft in Australia. Would a similar program work in the United States?

Sprint currently maintains a "negative" database that prevents stolen phones from being reactivated on its network. Unlike Australia, mobile carriers in the U.S. use multiple, competing mobile technologies and a variety of different spectrum bands to provide service. Phones designed and developed for use on one carrier's network typically do not function properly or at all if migrated to another carrier's network. Most US carriers either discourage strongly or prohibit non-carrier mobile devices to be registered on their networks due to the significant customer care issues that arise as a result of the non-carrier phone's poor performance. Accordingly, a program in the United States similar to the program in Australia may not have the same value.

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

Consumer education regarding safe smartphone use is the best way to discourage smartphone theft. Most cell phone thefts are crimes of opportunity. Consumers should treat their phones as valuable personal belongings and should exercise care in using them in public environments in a way that may attract thieves or facilitate theft. In addition, consumers should be encouraged not to purchase second hand phones without checking with the device's carrier that the ESN or MEID has not been placed on a carrier's lost/stolen list. For example, consumers considering buying a second hand Sprint device can call Sprint customer care to verify that a second hand device is not on Sprint's lost/stolen list. Educating customers on the steps they should take before purchasing a second hand device would help reduce the market for lost or stolen phones and lead to a reduction in "second victims," i.e. those who unknowingly buy a lost or stolen phone only to discover that the carrier has the phone's ESN or MEID on its lost/stolen list.

Please do not hesitate to contact me if you have any questions regarding the above.

Sincerely,