12920 Southeast 38th Street
Bellevue, WA 98006

Honorable Henry A. Waxman, Ranking Member
Honorable Anna G. Eshoo, Member
Honorable Edward J. Markey, Member
U.S. House of Representatives
Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515

Dear Distinguished Members of Congress:

I am writing in response to your letter dated March 23, 2012 regarding wireless handset theft. We fully agree with your concerns – not only does the theft of sophisticated and expensive wireless devices potentially endanger our customers and cause them monetary loss; T-Mobile USA, Inc. itself loses millions of dollars every year as a result of stolen devices. And, we spend even more on replacing stolen devices, helping customers that are the victims of crime, and establishing loss prevention programs. We are very motivated to put an end to this problem, although we caution that there is no simple fix and that many of the processes we have instituted or are looking into have serious privacy, technical, and competitive implications. Moreover, because today's thieves are very resourceful, a one-size-fits-all regulatory solution could aggravate the situation.

Below we answer your specific questions.

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

   T-Mobile USA has a number of policies in place that relate to device theft or loss, but it is also important to understand the basic framework of our technology. T-Mobile USA's network operates on the Global System for Mobile (GSM) communications standard, which is widely used both domestically and internationally. GSM technology pairs a device, identified by an International Mobile Equipment Identifier (IMEI), with a Subscriber Identity Module (SIM), which identifies the user. While both the IMEI and the SIM card information are provided to our network, it is only the SIM card that is required to gain access to the network. The result is that GSM enables users to insert their SIM card into any compatible GSM device – whether purchased from us or a third party - to access a GSM network. While this technology provides customers with tremendous flexibility to choose their own device, it also presents some unique challenges for GSM providers who are trying to combat domestic and international fraud and theft.

Our first step to deterring theft comes when we are notified of a missing or stolen device. T-Mobile USA takes steps to immediately suspend service on the account, which disables the SIM card and prevents it from registering on a GSM network. Suspension protects the customer from unwanted service charges while the device is missing. Customers can then contact us to reactivate service if they locate the device or to activate a new the SIM card that can be paired with a new or replacement device.

If our customers have elected to subscribe to the Mobile Security service offered by our partner Asurion, they can remotely locate a lost or stolen device. This service also allows our customers to remotely lock or wipe personal information from the device to prevent access and use by third parties. The Mobile Security service is also paired with an insurance product that helps our customers to replace lost and stolen devices.

T-Mobile USA also pre-loads an application called Lookout on most of our devices that use the Android operating system. Lookout, like many other applications available to customers through the Android Marketplace, provides additional layers of security similar to what can be found in the Mobile Security service. By activating the Lookout service customers can track and locate lost or misplaced devices as well as remotely lock or wipe data from a stolen device. Many Original Equipment Manufacturers (OEMs) are creating and pre-loading similar applications onto new devices. These services provide customers with additional options to protect and recover their devices in the event they are lost or stolen.

T-Mobile USA also requires OEMs to include basic locking functionality on all devices and with all operating systems. These locking features require users to enter a user-defined code or pattern to unlock the device and gain access to its content. This locking feature is the first line of defense to prevent unauthorized use of or access to a device, and we strongly encourage all of our customers to take advantage of this technology.

Our website also provides information to customers about password security, protection from identity theft, protection of customer proprietary network information, managing marketing preferences, protection against phishing and anonymous callers, device applications supporting location-based services, and instructions on what to do if a phone is lost or stolen, including suspending the line. The website also provides important tools that help our customers to facilitate reloading important contacts and contact information onto their replacement or new devices.

Finally, we have recently developed the technology that allows T-Mobile USA to block the use of particular devices on our network based on the IMEI of the device. The ability to IMEI block only prohibits the device from working on our own domestic network. Unfortunately this presents a significant weakness in deterring theft, as stolen devices can still operate on other GSM networks both domestically and internationally. Accordingly, we only use it on a limited basis, but, as discussed below, we are working toward an industry-wide solution that addresses the shortcomings of the current system.

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

T-Mobile USA makes every effort to stay ahead of criminals that prey on our customers and our company. Internally, our loss and fraud prevention and engineering groups continually evaluate our policies and develop new ways to protect consumers and the business. We also work closely with other carriers, law enforcement groups, both at the local and national level, as well as a variety of standards bodies and industry associations, to develop and update our theft deterrent policies. T-Mobile USA currently is part of a GSMA working group that is looking at creating an international database of stolen devices, as well as a newly-formed CTIA working group that brings large and small U.S. carriers to the table to develop industry-wide policies.

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?**

To be an effective deterrent, the technology to remotely disable mobile devices would have to be foolproof and adopted worldwide. It is neither at this point. Today, if T-Mobile USA remotely disables a device, thieves can still easily use the stolen device on the network of any other GSM carrier by inserting a SIM card from another carrier. Furthermore, the technology exists to spoof the device's IMEI, which can permit the device to be used on a GSM network in spite of efforts to block it from a network level. It is also important to point out that even if a GSM device could be rendered useless in the U.S., many thieves ship stolen phones outside the country where they still retain their value and can operate on other GSM-based networks. T-Mobile USA is currently working with GSMA to develop an international solution to this problem, but to provide a meaningful disincentive to theft, carriers, large and small, in all countries would have to buy into it and block IMEIs of stolen devices on their networks.

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

T-Mobile USA cooperates fully with law enforcement, both on the creation of theft deterrent polices and the case-by-case recovery of stolen phones. For example, the New York City Police Department contacted us recently to assist it in a broad investigation into stolen T-Mobile USA devices. Through the use of lawful subpoenas, we helped identify and provide a list of the phones and the users of those devices to further that investigation. In the process of this investigation, we also worked out procedures with the NYPD to quickly and efficiently handle the legal process for future requests. As a result, the NYPD has been successful in apprehending many wireless device thieves. We have started to work with other law enforcement agencies, including Baltimore, Maryland, to create similar processes, and the results have been positive.

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.**

GSM carriers like T-Mobile USA do not "activate" phones on our network in the traditional sense because customers can simply insert an activated SIM in any GSM-compatible device and it will work on our network if it is not on our blocked list. Accordingly, we have no way

of knowing that a device that could have originally been purchased from another carrier is stolen. As noted above, as part of GSMA, we are evaluating the creation of an international stolen phone database, which if developed, would allow T-Mobile USA and other carriers to institute an industry-wide solution.

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 noted above, T-Mobile USA is looking into just such a "blacklisting" program in coordination with GSMA. Unlike Australia, which presumably does not have the same problems with overseas shipment of stolen phones, however, an effective program in the U.S. would have to be global in nature as well as industry-wide. Blacklisting phones simply for T-Mobile USA , or even for all GSM carriers in the U.S., would not provide a meaningful deterrent to the theft of T-Mobile USA phones in this country.

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

   T-Mobile USA takes the problem of wireless device theft very seriously, and we will continue to explore ways to protect consumers in the most effective way possible. As noted above, we are working closely with GSMA and CTIA to develop theft deterrent technologies and policies across the industry. In addition, we have implemented a number of options for consumers to protect sensitive data on phones even if the phones fall into the hands of thieves and fraudsters. We also intend to continue our cooperation with law enforcement to bring thieves to justice. As thieves become more and more sophisticated, so must our opposition to their methods. A static solution will not work and nor will a solution that is broadcast to the world.

Thank you for the opportunity to present our views on this important issue.

Best regards,

Philipp R. Humm
CEO and President
T-Mobile USA, Inc.