QUALCOMM Incorporated
1730 Pennsylvania Ave., NW ■ Suite 850 ■ Washington, DC 20006 ■ Tel: 202.263.0020 www.qualcomm.com

January 30, 2015

Ms. Marlene Dortch
Secretary
Federal Communications Commission
445 12th Street, S.W.
Washington, D.C. 20554

Re: FCC Technological Advisory Council Report on Mobile Device Theft Prevention — ET Docket No. 14-143

Dear Ms. Dortch:

QUALCOMM Incorporated ("Qualcomm") is pleased to provide additional comments on the FCC's Technological Advisory Council Report on Mobile Device Theft Protection, which focused on steps that the Commission, law enforcement and the industry are currently taking, and in the future may take, to reduce smartphone theft.[1]

For the benefit of the FCC and all stakeholders working to curtail the growing problem of mobile device theft, we wish to point out that Qualcomm has developed an innovative technology solution called SafeSwitch™ that provides additional layers of security protection beyond software-only solutions. Our concern is that software-only solutions are susceptible to hacking, and our solution is tied deeply into the device's hardware — the microprocessor chip itself. This provides more robust protection, making it far more difficult and costly for a thief to make a stolen device usable, and thereby break the thieves' "business model" and ultimately deter device theft.

The SafeSwitch technology has been designed to counter means that thieves use to bypass software-only solutions, such as rooting, custom firmware updates, and flash part replacements, in order to steal personal data and resell stolen smartphones. As the FCC TAC Report explains, the SafeSwitch solution "differs from the other solutions in that it's more a component that may be used in the future by device-based solutions. It provides an additional layer of protection by exposing a chipset-level hardware lock when a device is disabled."[2]

SafeSwitch technology, which will be available in Qualcomm's Snapdragon chips in the first half of 2015, allows rightful device owners to remotely disable their devices if they are lost or stolen and subsequently allows these owners to re-enable them if they are found or recovered. As explained in the Qualcomm video linked in Attachment A to this letter, SafeSwitch enables

---

[1] *See* FCC Public Notice, "Comments Sought on Technological Advisory Council Report on Mobile Device Theft Prevention," DA-1828 (Dec. 12, 2014). *See also* Report of Technological Advisory Council (TAC) Subcommittee on Mobile Device Theft Prevention (MDTP) (Dec. 4, 2014) ("TAC Report") at 6.

[2] *See* TAC Report at 40; *see also id*. at 115-16.

full user control, including the ability to: (i) remotely set a device password; (ii) locate and lock a stolen or misplaced device, and (iii) erase and recover sensitive user data.

Qualcomm SafeSwitch hardware, firmware, and software technology is activated during the early boot stage of a device — before the operating system begins to run — and therefore is able to detect hacking attempts, including device wipe attempts and malicious software installations, and thus ensures that only the rightful owner (or another authorized party) can unlock and access the device. Additional details on our SafeSwitch technology are in the White Paper provided in Attachment B to this letter.

Qualcomm is very excited about this innovative multi-layered smartphone security technology and looks forward to working with the industry, law enforcement, and the Commission to deter device theft.

Respectfully,

QUALCOMM INCORPORATED

By: _____

Dean R. Brenner
Senior Vice President, Government Affairs

John W. Kuzin
Senior Director, Regulatory

Attorneys for QUALCOMM Incorporated

Atts:

A: Link to Video: "SafeSwitch Addresses Mobile Security with Kill Switch Solution"

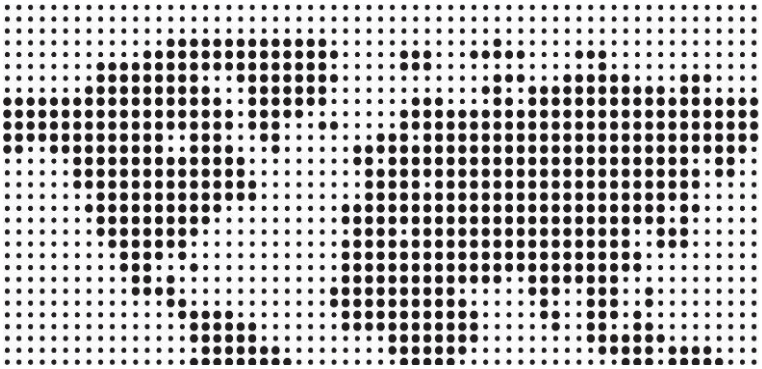
B: Qualcomm White Paper: "Kill Switch: The Benefits of Hardware-based Solutions"

Attachment A

The Qualcomm video: "SafeSwitch Addresses Mobile Security with Kill Switch Solution," *is available at* https://www.qualcomm.com/news/snapdragon/2015/01/05/snapdragon-processors-address-mobile-security-smartphone-kill-switch

Attachment B

Kill Switch: the benefits of hardware-based solutions



Qualcomm Technologies, Inc.
January 2015

1. Abstract

Challenged by the growing problem of cell phone theft, and in the wake of impending regulation and legislation, leading technology vendors were quick to develop solutions that simply prevent locked phones from being reset. In this view, prohibiting thieves from performing a factory reset would ensure that stolen devices always display a lock screen and thereby remain dysfunctional. What's more, since factory reset is a software-triggered operation, it appears possible to safeguard it through software. This approach is tempting in complex product settings where software and hardware vendors typically work in isolation according to rigid interfaces. Consequently, software-only kill switch solutions were announced with the sole focus on factory reset-- from guarding against it to verifying a posteriori that the rightful owner issued it.

One might assume that this software approach would be effective against petty thieves. But that assumption assumes a lack of technical sophistication on the part of the thieves, which, unfortunately, is at odds with real world experiences. The problem is clear. As has been the industry's experience with IMEI blacklisting: introducing partial functionality hurdles does not remove the monetary value of stolen phones and ultimately does not deter cell phone theft. In the case of IMEI, when thieves cannot use stolen devices on local networks, they sell them through online auction websites or on the black market. We believe that demand will remain high for locked devices that can economically be "repurposed" in a lab and thereafter resold. Unfortunately, a stolen phone with one of today's software-only solutions can possibly be repurposed by bypassing the software lock screen through any of a wide variety of attacks: rooting, custom firmware updates, software vulnerability exploits, flash part replacement, etc. In short, software-only solutions, while well-intentioned, do not appear to change the thieves' fundamental economic incentives and, therefore, do not appear likely to deter theft to a substantial extent.

A symptomatic treatment that focuses solely on blocking factory reset, the path of least resistance, is not a comprehensive solution to this issue. Without a doubt, an effective solution must protect that which keeps stolen devices locked. But, such crown jewels are not the factory reset operation, which is more of an incidental narrative. We believe the focus should be on the core elements that cut off phone functionality from unauthorized users, and on making it so expensive and difficult for thieves to repurpose stolen phones that they would no longer have any economic incentive to steal them.

Hereinafter, we describe a technology designed from the ground up to achieve the goal just mentioned—to make it so expensive and difficult for thieves to repurpose stolen phones that they would no longer have any economic incentive to steal them. The technology is designed to do so by addressing both current and foreseeable future security concerns. Qualcomm Technologies, Inc. ("Qualcomm") has productized this technology into a feature known as SafeSwitch™. It works in tandem with commercial kill switch software applications. Its complementary nature furnishes existing solutions with the required security provisions, while supporting other important legacy protections such as IMEI blacklisting to go on uninterruptedly.

With the urgent national, indeed international, need to bring smartphone theft to a stop, Qualcomm decided to make it possible for compatible SafeSwitch™ solutions to be built and released by different leading vendors. By so doing, smartphones powered by other chipsets can be designed with more secure kill switch implementations.

2. Security and privacy through hardware

In order to protect the core elements that cut off smartphone functionality from unauthorized users, we believe that kill switch solutions should comprise of technology that both *a)* knows if the device should be locked and *b)* enforces that lock state.

Software-based approaches address the former by preventing users from resetting the device and clearing its memory. If such measures were exhaustive, then once stolen and deactivated, devices would always "know" if they are locked. As described, this is not necessarily the case with factory reset protection. The second requirement, enforcement, necessitates the software to be present and to operate correctly. However, because this prerequisite constitutes a difficult problem for software, little has been done by contemporary software solutions to contend with it.

With this view of the problem in mind, Qualcomm recommends that all kill switch solutions meet the following technical goal: place locked devices in a persistent low functionality state that cannot be reversed without something which only a trusted party, such as the owner, possesses. Any shortfall in this department, and it could be a matter of time before ill-intentioned security specialists offer feasible means of reactivating locked phones in great quantities.

Qualcomm SafeSwitch™ implements this goal through a "defense in depth" approach that adds two protective hardware layers underneath existing software solutions. With independent monitoring and enforcement mechanisms at multiple layers, the technology is designed to capably discover, contain, and prevent attacks. Moreover, it ties into present kill switch systems, supporting a seamless experience for consumers and industry stakeholders alike.

Firmware Lock is the first protective layer of defense. It is a transparent hardware-based mechanism that operates during power-on to guarantee the invariable form and presence of the overlying kill switch software and writeable data. If the software or data diverge from their certified state, the device locks during power-on. At that point, unlocking the device is not possible without an unlock key which only a trusted party, the owner or the network operator, would possess. Locking the firmware means locking critical software elements, which must never be tampered with. By doing so, kill switch software is granted a sanitized environment to run in, detect potential threats, and enforce device lock when necessary. This objective is met through a proven cryptographic scheme which encrypts critical ingredients unique to each device. Without the unlock key, these components cannot be unraveled and the phone is devoid of foundational elements for completing the simplest boot operation.

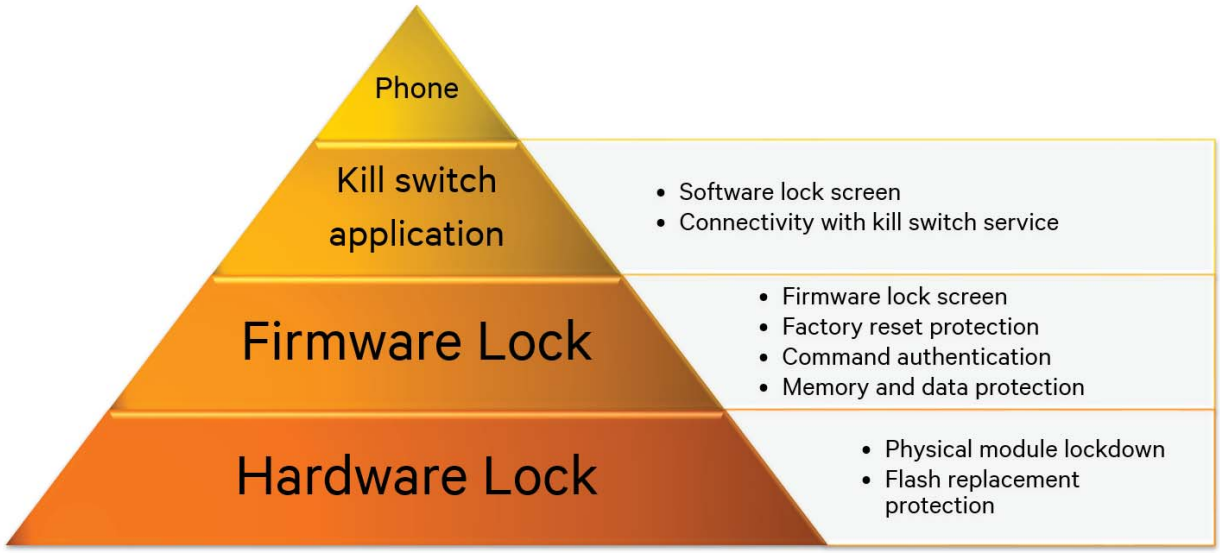
Hardware Lock is the second protective layer of defense. It comes into play when a device is stolen and kill switch software triggers a device lock. Traditionally this would invoke a lock screen that hinders phone functionality. Hardware Lock uses this juncture to carry out an additional function of locking down hardware modules. When locked down, such modules operate in a degraded state, which significantly detracts from the phone's value. For instance, Qualcomm's Hardware Lock is intelligently built into its cellular modem. This blocks stolen devices from placing and receiving standard calls, while still meeting all E911 emergency call and service alert requirements. As a result, they are persistent, isolated and independent of the phone's software. In other words, a stolen phone remains disabled with or without its kill switch software. Similar to Firmware Lock, Hardware Lock can only be disabled through an unlock key, which will reside with a trusted party.

An oft-cited concern over kill switch solutions relates to schemes wherein attackers could gain access to disable the phones of adversaries. SafeSwitch™ employs a hardware-based security platform designed to address this major worry. It uses digital signatures to authenticate incoming kill switch commands as genuine requests originating from a trusted server. This is engineered to ensure that critical kill switch decisions are made and executed by the most trusted and reliable part of the device.

As smartphones evolve to manage greater parts of our lives, so does our reliance on them. As a result, handsets have growing access to personal information, which left unguarded can be harvested by thieves using off-the-shelf software, even when devices are locked or turned off altogether. This is becoming an increasing worry as the scope and value of private data continues to increase at a rapid rate. Deferring data protection to the responsibility of other indeterminate parties is unproductive in the long-term quest to remove economic incentives from phone theft.

With Firmware Lock, SafeSwitch™ provides a state-of-the-art response to this growing personal data and privacy concern. It employs a hardware-based disk encryption system designed to protect all user data from extraction and decryption attacks. Security-related parts of this scheme are engineered on top of trusted hardware foundations, from handling the encryption keys to performing cryptographic decryption of the data. As with other aspects of the solution, this system is compatible with today's operating systems and applications.

Finally, given the competitive landscape and wealth of technological alternatives, the wider industry can now build on Qualcomm's work without necessarily adopting its products. In order to help the ecosystem reach the critical mass required for widespread consumer protection and safety, Qualcomm is doing its part by allowing compatible solutions to be designed and deployed.



Qualcomm's defense in depth security model

QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, CA. 92121-1714 U.S.A.

Copyright © 2015 Qualcomm Incorporated.
All rights reserved.

Not to be used, copied, reproduced in whole or in part, nor its contents revealed in any manner to others without the express written permission of Qualcomm.

This technical data may be subject to U.S. and international export, re-export, or transfer ("export") laws. Diversion contrary to U.S. and international law is strictly prohibited.

QUALCOMM is a registered trademark of QUALCOMM Incorporated in the United States and may be registered in other countries. Other product and brand names may be trademarks or registered trademarks of their respective owners.