

April 11, 2012

The Honorable Henry A. Waxman  
Ranking Member  
Committee on Energy and Commerce  
House of Representatives  
Washington, DC 20515

The Honorable Anna G. Eshoo  
Ranking Member  
Subcommittee on Communications and  
Technology  
Committee on Energy and Commerce  
House of Representatives  
Washington, DC 20515

The Honorable Edward J. Markey  
House of Representatives  
Washington, DC 20515

Dear Ranking Members Waxman and Eshoo and Rep. Markey:

MetroPCS Communications, Inc. (“MetroPCS”) appreciates your inquiry into its policies regarding the important topic of safeguarding customer equipment and wireless handsets, including smartphones. As discussed in greater detail below in response to your specific questions, MetroPCS too is concerned about handset theft and threats against consumer privacy, and accordingly has undertaken a number of actions to deter theft, as well as offering a number of options to its customers to mitigate the potential risks surrounding stolen handsets, and free educational tools on its website that can be used to reduce the risks of, and dangers associated with, handset theft.

MetroPCS provides mobile wireless voice and broadband data service in selected major metropolitan areas in the United States and serves approximately 9.3 million subscribers,<sup>1</sup> making it the fifth-largest facilities based mobile broadband wireless carrier in the United States, based on number of subscribers served. MetroPCS targets a mass market largely underserved by the larger national mobile broadband wireless providers. MetroPCS’ service plans are differentiated by being more affordable, predictable and flexible than the more complex long-term plans offered by many of its competitors, and currently begin at \$25 per month for unlimited voice and text on a nationwide basis, and \$40 per month for voice, text and data on a nationwide basis, including all applicable taxes and regulatory fees. MetroPCS allows customers to use its unlimited wireless service in MetroPCS’ coverage areas, as well as in its extended service areas through various roaming arrangements, under its flat-rate monthly service plans. Customers pay for service in advance, without a credit check. As a no-contract provider, MetroPCS must continually provide services that its customers value and desire, as each of its customers can easily move to a different wireless provider at any time without fear of early termination fees.

---

<sup>1</sup> As of December 31, 2011.

Many of MetroPCS' customers use the advanced smartphones that are available on MetroPCS' CDMA and 4G LTE networks, and MetroPCS considers it important that these and all other MetroPCS customers feel safe and secure using their handsets. As noted below, MetroPCS offers a number of avenues for consumers to protect against handset theft, as well as have the ability to protect their personal data and privacy in the event of handset theft.

While MetroPCS appreciates the efforts of local law enforcement to stop criminal activity related to stolen wireless devices, it cautions against additional Federal regulation. Because the retail market for wireless services is quite competitive, wireless companies must differentiate their services in order to compete and to provide services that customers want. For example, MetroPCS has adopted, without government intervention, the policies referenced in this response in order to offer consumers options that allow them the ability to remove personal data from lost or stolen handsets remotely. MetroPCS believes promoting increased competition in the wireless industry by allowing differentiation, rather than additional regulation or one-size-fits-all approaches, is the best way for consumers to have the best types of services available – and offerings to allow consumers the ability to control personal data on their wireless handsets is no exception.

Moreover, there is clear proof that the wireless industry as a whole is taking the threat of wireless device theft seriously, and is taking action to prevent it. Yesterday, the Federal Communications Commission (“FCC”), along with several national wireless carriers, announced the creation of a nationwide database that will ensure providers can prevent the use or resale of smartphones that have been reported lost or stolen.<sup>2</sup> This effort will create a national “blacklist” database for wireless devices that have been reported lost or stolen, and ensure that criminals cannot steal from the customer of one carrier and sell the device to be operated on another network. MetroPCS currently anticipates participating in this important voluntary, industry-led effort to reduce or prevent wireless device theft.

MetroPCS is pleased to respond to the questions you posed in your March 23, 2012 letter:

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

MetroPCS takes the theft or loss of customer wireless handsets very seriously and takes numerous steps to discourage such efforts. MetroPCS maintains both a “whitelist” and a “blacklist” of handsets uniquely identified by mobile equipment identifier (“MEID”) number, electronic serial number (“ESN”) and international mobile equipment identity (“IMEI”) number. MetroPCS only allows handsets with an MEID/ESN/IMEI on the whitelist – i.e., those handsets that have been approved by MetroPCS – to be activated on the MetroPCS network. Furthermore, any handset that is reported to MetroPCS as lost or stolen has its MEID/ESN/IMEI placed on the MetroPCS blacklist, which prevents such handset from being activated or used on the MetroPCS network. This policy was undertaken by MetroPCS specifically to discourage the use of stolen handsets. As noted above, MetroPCS also anticipates expanding its program by

---

<sup>2</sup> See “FCC Chairman Genachowski Joins Senator Schumer, D.C. Mayor Gray, State Police Departments, and Wireless Carriers to Announce New Initiatives to Combat Massive Smartphone & Data Theft,” FCC Release (Apr. 10, 2012), *available at* [http://transition.fcc.gov/Daily\\_Releases/Daily\\_Business/2012/db0410/DOC-313509A1.pdf](http://transition.fcc.gov/Daily_Releases/Daily_Business/2012/db0410/DOC-313509A1.pdf).

participating in the national blacklist database recently announced by the FCC and other wireless carriers, which will further protect MetroPCS' and other carriers' customers from wireless device theft. If a customer reports a phone as lost or stolen, it is MetroPCS' policy to direct the customer to file a report with local law enforcement. In addition, as detailed below, if the customer presents matching government-issued identification at a MetroPCS-owned store, MetroPCS will assist law enforcement in using the phone's and our networks' capabilities to locate the phone for law enforcement.

MetroPCS also takes steps to educate its customers on how they can use their MetroPCS handsets safely and securely by publishing a primer entitled "Phone safety and security," which is made available on its website and is easily linked to when viewing any phone selection.<sup>3</sup> Indeed, the safety and security guide is available under the "Learn" tab for every phone available on the MetroPCS website, ensuring that it is widely available and conveniently located for all MetroPCS costumers. This guide offers customers practical advice on how to safeguard their handsets and personal data, such as: (i) how to choose and maintain a secure password; (ii) how to stay safe when using a public WiFi hotspot; (iii) proper precautions to take when downloading apps; and (iv) basic phone safety. By arming its customers with these basic handset safety tools, MetroPCS is working to mitigate the potential losses associated with a stolen handset and also to minimize handset theft by making MetroPCS handsets more difficult to access, and therefore less attractive to criminals.

Moreover, as noted in further detail below, MetroPCS also offers its customers a "lock and wipe" technology that it considers helpful deterrent to theft, through its Metro Total Protection<sup>SM</sup> app.<sup>4</sup> This offering allows customers themselves, without MetroPCS' direct involvement, to locate lost handsets, lock handsets remotely to protect and secure sensitive customer information and to erase customer information remotely to protect sensitive information of the handset owner and others. A number of our customers have taken advantage of this program.

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

Yes. In an effort to stay ahead of the issues facing the company and its customers, MetroPCS regularly monitors developments in the wireless industry. MetroPCS' programs have expanded as the type of handsets and information stored on handsets have changed. For example, a number of years ago MetroPCS first utilized its blacklist to deter theft. MetroPCS has now launched Metro Total Protection, which provides customers even greater protection. MetroPCS also commits significant time and resources to tracking the issues that impact its customers, both internally and through its participation in collaborative industry groups. In this manner, MetroPCS strives to keep itself aware of how advanced technologies may impact the likelihood of handset theft, and consistently cooperates with other carriers should a new or unexpected handset theft tactic arise.

<sup>3</sup> See MetroPCS "Phone safety and security" guide (included as Attachment A), available at [http://www.metropcs.com/assets/user\\_guides/GeneralPhoneSecurity.pdf](http://www.metropcs.com/assets/user_guides/GeneralPhoneSecurity.pdf).

<sup>4</sup> See MetroPCS "Metro Total Protection App" fact sheet (included as Attachment B), available at [http://www.metrototalprotection.com/public/metrorecovery/total\\_protection\\_app\\_mg.html](http://www.metrototalprotection.com/public/metrorecovery/total_protection_app_mg.html).

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?*

MetroPCS, upon customer request, can disable MetroPCS service to any handset at any time wherever located. Further, MetroPCS, upon notification that a handset is lost or stolen can add the handset to the blacklist to prevent that handset from being activated or used on MetroPCS' networks. In many instances, provided that the wireless device is turned on and upon presentation of proper government-issued matching identification, MetroPCS also has the ability to provide location information to law enforcement or customers whose wireless handset has been lost or stolen. A national blacklist will allow MetroPCS to extend this program to lost or stolen handsets of customers or other carriers.

In addition, MetroPCS offers Metro Total Protection, which allows for customer-initiated "lock and wipe" of handsets. MetroPCS agrees that this sort of "lock and wipe" technology may be a helpful deterrent to theft, and offers this service to its customers through its Metro Total Protection app. Metro Total Protection is available both as a standalone app and as part of the MetroGUARD<sup>SM</sup> comprehensive phone protection plan.<sup>5</sup> Metro Total Protection offers a number of important security features to subscribers, including the ability to:

- Remotely locate a handset using the phone's GPS unit, which may provide law enforcement or others with helpful location information;
- Sound a remote handset alarm to deter theft in the act or inform others that the handset is stolen;
- Lock a handset remotely to protect and secure sensitive customer information contained on the handset; and
- Erase contacts remotely to protect sensitive information of the handset owner and others.

By using the Metro Total Protection and MetroGUARD features, MetroPCS customers can feel more secure storing sensitive information on their handsets. Similarly, potential criminal activity may be limited as potential thieves become aware that many MetroPCS phones can be locked and wiped remotely. Certain MetroPCS phones also have integrated "lock and wipe" mechanisms and many with the Android operating system can be password locked by the user. In addition, it is MetroPCS' understanding that there are several Android apps available through the Google Play market that perform similar functions, some of which may be free or offer limited free trial periods. Thus, users have a number of options available to them to protect their handset and any sensitive data contained therein. MetroPCS believes that the above applications provide a significant benefit to customers as a theft deterrent, as well as additional protections of their personal information.

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

---

<sup>5</sup> See MetroPCS "MetroGUARD" fact sheet (included as Attachment C), available at <http://www.metrototalprotection.com/public/metrorecovery/metroguard.html>.

Yes. MetroPCS cooperates with law enforcement to retrieve lost or stolen handsets, and MetroPCS has an excellent record of doing so. If duly authorized law enforcement officials request MetroPCS' assistance in retrieving a lost or stolen handset, MetroPCS would, subject to customer identification, consent and permission, gladly provide to law enforcement information in MetroPCS' possession, including location information, that may help to retrieve lost or stolen handsets.

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.*

No. As discussed above, MetroPCS takes efforts to guard against handsets which have been reported to MetroPCS as stolen from being reactivated on its network. MetroPCS only activates handsets on its network with an MEID/ESN/IMEI that appears on the MetroPCS whitelist. A wireless device whose MEID/ESN/IMEI appears on MetroPCS' blacklist at the time of an attempted activation (for example, because it has been reported to MetroPCS as lost or stolen) is prohibited from being activated on the MetroPCS network. When the national blacklist database is operational MetroPCS will be able to extend this program to lost or stolen handsets of customers of other carriers.

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 mentioned above, MetroPCS already uses such a program with respect to handsets on its own networks which are reported as lost or stolen to MetroPCS. MetroPCS also understands that the Commission has recently announced a national blacklist database. MetroPCS submits that the best course of action to mitigate the problem of wireless device theft is to promote these voluntary industry coordination efforts. These efforts demonstrate that voluntary industry solutions are already well-established, and Congress should simply encourage the continued development of these industry-led blacklisting programs. MetroPCS respectfully submits that Congress should only encourage voluntary intra-industry cooperation that will allow wireless providers to solve problems flexibly and adapt as criminal behavior may change or grow more technically sophisticated over time.

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

As is evident by the wide variety of programs and solutions available to consumers to limit wireless device theft, which have been driven by wireless competition, much already is being done to protect consumers. Given these significant steps, the best course of action would be for Congress to foster competition and to encourage the continuation of industry-led efforts, such as those undertaken by MetroPCS, and to educate consumers. Perhaps most importantly, an informed consumer is an empowered consumer. Customers simply are unable to take advantage of the myriad protections against handset theft if they are unaware of them. Strong local law enforcement, combined with industry efforts to educate its own consumers about the options

available to them, go a long way towards putting the topic of handset theft in the forefront of consumers' minds. MetroPCS looks forward to working with Congress and others in the wireless industry on voluntary solutions to better protect consumers from handset theft and to continue the competitive market that drives such solutions.

Sincerely,

A handwritten signature in cursive script that reads "Doug S Glen". The signature is written in black ink and is positioned to the right of the word "Sincerely,".

Doug Glen  
Senior Vice President, Corporate  
Development  
MetroPCS Communications, Inc.

# **ATTACHMENT A**

# Phone safety and security

**metro**PCS.  
Wireless for All.

Helpful tips to keep you safe and your phone secure.  
For additional details, please refer to your phone's user guide.

#### How to Choose a Secure Password

- Avoid using words or phrases that have personal significance because they are less secure.
- You should mix letters and numbers.
- Try to memorize the password, and avoid writing it down.
- The longer the password, the more secure it generally will be.
- Do not use the same password for everything that requires one.
- You should change your password regularly and not share it with others.

#### Tips to Keep You Safe at a Public Hotspot

- Never leave your phone unattended—not even for a moment.
- Do not allow your phone to automatically join the nearest network. Instead, manually select the hotspot when you connect.
- Make sure you are on a legitimate hotspot by checking with the host to confirm the network name and connection process.
- Try to minimize the amount of sensitive, personal data you store on your laptops and mobile devices.
- Do not engage in online banking or trading at a public hotspot.
- Turn off your Wi-Fi connectivity when you are not using it.

#### Precautions When Downloading Apps

- Approve the installation of the software instead of using automatic download.
- Read the comments in the Market before you download an app.
- Check the rating for an app. Use caution when downloading apps with low ratings.
- Before downloading an app, scroll down to the "About the developer" section after first selecting an app in the Market, then hit "View more applications." Look through the apps this person or team has developed.
- Read through the permissions your desired app will request from your phone to perform its job.

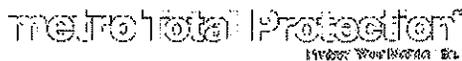
#### Basic Phone Safety

- Never use a battery that is not approved for use with your phone since this could damage the phone and/or battery and might cause other more serious battery-related issues like leakage, fire or explosion.
- Do not expose the battery charger or adapter to direct sunlight or use it in places with high humidity, such as a bathroom.
- Never place your phone in a microwave oven as this will damage your oven and will likely cause the battery to explode.
- Never store your phone in temperatures less than -4°F or greater than 122°F.
- Do not dispose of your battery by fire or with hazardous or flammable materials.
- When riding in a car, do not leave your phone or set up the hands free kit near the air bag. If wireless equipment is improperly installed and the air bag is deployed, you may be seriously injured.
- Do not use a hand-held phone while driving.

### Basic Phone Safety (continued)

- Do not use the phone in areas where its use is prohibited. (For example: on aircraft or in school zones)
- Do not use harsh chemicals (such as alcohol, benzene, thinners, etc.) or detergents to clean your phone. This could cause a fire.
- Do not drop, strike, or shake your phone severely. It may harm the internal circuit boards of the phone.
- Do not use your phone in high explosive areas as the phone may generate sparks.
- Do not damage the power cord by bending, twisting, pulling, or heating. Do not use the plug if it is loose as it may cause a fire or electric shock.
- Do not place any heavy items on the power cord. Do not allow the power cord to be crimped as it may cause electric shock or fire.
- Do not handle the phone with wet hands while it is being charged. It may cause an electric shock or seriously damage your phone.
- Do not disassemble the phone.
- Do not place or answer calls while charging the phone as it may short-circuit the phone and/or cause electric shock or fire.
- Make sure that no sharp-edged items such as animal's teeth or nails, come into contact with the battery. This could cause a fire.
- Store the battery out of reach of children.
- Be careful that children do not swallow any parts (such as rubber plugs, earphone, connection parts of the phone, etc.) This could cause asphyxiation or suffocation resulting in serious injury or death.
- Unplug the power cord and charger during lightning storms to avoid electric shock or fire.
- Only authorized personnel should service the phone and its accessories. Faulty installation or service may result in accidents and consequently invalidate the warranty.
- Some emergency phone numbers, such as 911, can be called under any circumstances, even when your phone is locked. Your phone's preprogrammed emergency number(s) may not work in all locations, and sometimes an emergency call cannot be placed due to network, environmental, or interference issues.

# **ATTACHMENT B**



Home MetroGuard One Powerful App

# One Powerful App

## Phone Protection

- Overview
- Deductibles
- Claim Documentation
- In-Store Payment Locations
- Shipping
- FAQs
- Terms and Conditions

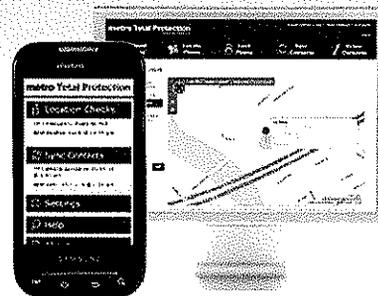
## Mobile App

- Overview
- One Powerful App
- Download Mobile App
- Phones Supported
- FAQs
- Support Forum

## metro Total Protection app

All the great features of MetroGUARD and MetroBACKUP in one powerful app!

- ▶ Locate phone
- ▶ Sound phone alarm
- ▶ Lock phone
- ▶ Erase contacts remotely
- ▶ Backup and restore contacts
- ▶ Manage contacts online



### Metro Total Protection<sup>SM</sup> App

We've combined all the great features of MetroGUARD and MetroBACKUP into a single app that allows you to choose the perfect level of protection.

With the MetroGUARD features, you get alarm, locate, lock, and remote erase capabilities. Best of all, these mobile app features are available at no additional cost to MetroGUARD subscribers.

With the MetroBACKUP features, you get automatic and wireless backup, simple contact transfer/restore and online contact management. The MetroBACKUP features can be downloaded by all MetroPCS subscribers with supported Phones at any time for just \$1.00 / mo.

**DOWNLOAD MOBILE APP**

#### Want to add the MetroBACKUP feature?

Adding backup, restore and online contact management to your MetroGUARD account is fast, simple and costs just \$1.00 per month.

1. Launch the Metro Total Protection App from your phone
2. From the main menu click "Add Backup"
3. Confirm the \$1.00 / mo. charge to complete the upgrade

[Mobile App Terms and Conditions](#) | [Mobile App Privacy Policy](#) | [Contact](#)

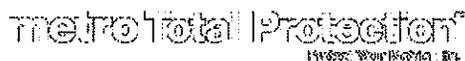
© 2002-2011 MetroPCS Wireless Inc. All Rights Reserved.  
© Asurion Mobile Applications, Inc. All Rights Reserved.

MetroGUARD insurance is underwritten by Old Republic Insurance Company and is administered by Asurion Insurance Services, Inc. who is the agent and provides claim servicing under this program. Total Protection app is a service provided by Asurion Mobile Applications, Inc. and is not an insurance product. MetroBACKUP is a service provided by Asurion Mobile Applications.

\*Deductible, claim limits, and replacement equipment do not apply to MetroBACKUP features



# **ATTACHMENT C**



Home MetroGuard MetroGuard Overview

# Overview

## Phone Protection

Overview

Deductibles

Claim Documentation

In-Store Payment Locations

Shipping

FAQs

Terms and Conditions

## Mobile App

Overview

One Powerful App

Download Mobile App

Phones Supported

FAQs

Support Forum

## metroGUARD

- ✓ Comprehensive phone protection
- ✓ Fast and convenient replacement
- ✓ Save money should the unexpected happen
- ✓ Beyond insurance with new mobile app



### Protect Your Phone With MetroGUARD SM

- ▶ Comprehensive coverage against loss, theft, damage (including water damage) and out-of-warranty malfunction
- ▶ Fast and convenient replacement
  - Claims can be filed 24/7 online or by phone
  - Next business day delivery of phone replacements (If claim completed and approved by 10:00PM Eastern time) View shipping schedule
- ▶ Save money should the unexpected happen
  - No high replacement costs if you experience a loss
  - You're covered for less than 20 cents a day
- ▶ Beyond Insurance
  - With a compatible phone, download the Metro Total Protection app to sound an alarm, locate and lock your lost phone, and remotely erase your contacts

MetroGUARD is only available on the day on which you activate service or upgrade to new equipment.

[FILE A CLAIM](#)

[RESUME A CLAIM](#)

[TRACK A CLAIM](#)

#### Here's what to expect...

1. Enter your personal info.
2. Confirm your phone's make/model
3. Tell us what happened and where to ship your replacement phone.
4. Pay your deductible.
5. Receive your phone as quickly as the next business day.

### MetroGUARD SM now includes the Metro Total Protection SM mobile app

#### Mobile app features include:

- ▶ Locate your phone on a map
- ▶ Sound an alarm from a misplaced phone, even if it's set to silent or vibrate.
- ▶ Lock a missing phone to secure your privacy
- ▶ Remotely erase contacts from a lost device
- ▶ You can add MetroBACKUP at any time for just \$1/mo. [Learn More](#)

[DOWNLOAD MOBILE APP](#)

Free with metroGUARD

