Mobile Wallet Services Protection

Background

Consumers are increasingly using their smartphones, tablets and other mobile devices as "mobile wallets" to pay for goods and services, downloading software that allows them to complete both mobile and in-person transactions. As the use of mobile wallet services increases, consumers need to protect their smartphones, mobile wallet applications, associated data, and mobile wallet services from theft and cyber attacks.

How to Safeguard Your Mobile Wallet Smartphone

- Consider your surroundings and use your smartphone or mobile device discreetly.
- Do not use mobile wallet services to conduct financial transactions over an unsecured Wi-Fi network.
- Never leave your smartphone unattended in a public place. Don't leave it visible in an unattended car; lock it up in the glove compartment or trunk.
- The police may need your smartphone's unique identifying information if it is stolen or lost. Write down the make, model number, serial number, and unique device identification number (either the International Mobile Equipment Identifier (IMEI) or the Mobile Equipment Identifier (MEID) number). Some phones display the IMEI/MEID number when you dial *#06#. The IMEI/MEID can also be found on a label located beneath the phone's battery or on the box that came with your phone.
- Review the service agreement for the financial account used in your mobile wallet to find out what will happen and who to contact if your smartphone is stolen or lost, or if your mobile wallet application is hacked.
- Monitor the financial account used in your mobile wallet for any fraudulent charges.
- Choose a unique password for your mobile wallet. Should your smartphone be lost or stolen, this may help protect you from both unwanted charges and from theft and misuse of your personal data.
- Install and maintain security software. Apps are available to:
  - ✓ Locate your smartphone from any computer;
  - ✓ Lock your smartphone to restrict access;
  - ✓ Wipe sensitive personal information and mobile wallet credentials from your smartphone; and
  - ✓ Make your smartphone emit a loud sound ("scream") to help you or the police locate it.
- Adjust your "locked screen" display to show your contact information so that your smartphone may be returned to you if found.
- Be careful about what information you store. Social networking and other apps may pose a security risk and allow unwanted access to your personal information and mobile wallet data.

Federal Communications Commission · Consumer and Governmental Affairs Bureau · 445 12th St. SW. Washington, DC 20554
1-888-CALL-FCC (1-888-225-5322) · TTY: 1-888-TELL-FCC (1-888-835-5322) · Fax: 1-866-418-0232 · www.fcc.gov/consumer-governmental-affairs-bureau

What to Do if Your Mobile Wallet Smartphone Is Stolen

- If you are not certain whether your smartphone or mobile device has been stolen or if you have simply misplaced it, attempt to locate the smartphone by calling it or by using the security software's GPS locator. Even if you may have only lost the smartphone, you should remotely lock it to be safe.

- If you have installed security software on your smartphone, use it to lock the device, wipe sensitive personal information, and/or activate the alarm.

- Immediately report the theft or loss to your wireless carrier. You will typically be responsible for any charges incurred prior to when you report the stolen or lost smartphone. If you provide your carrier with the IMEI or MEID number, your carrier may be able to disable your smartphone, your mobile wallet services, and block access to your personal information and sensitive mobile wallet data. Request written confirmation from your carrier that you reported the smartphone as missing and that the smartphone was disabled.

- If your smartphone or mobile device was stolen, also immediately report the theft to the police, including the make and model, serial and IMEI or MEID number. Some carriers require proof that the smartphone was stolen, and a police report can provide that documentation.

- If you are unable to lock your stolen or lost smartphone, change all of your passwords for mobile wallet services and banking accounts that you have accessed using your smartphone service.

For more information about what to do if your wireless device is lost or stolen, and contact information for service providers, go to: **www.fcc.gov/guides/stolen-and-lost-wireless-devices**

For More Information

For information about other communications issues, visit the FCC's Consumer website at **www.fcc.gov/consumers**, or contact the FCC's Consumer Center by calling 1-888-CALL-FCC (1-888-225-5322) voice or 1-888-TELL-FCC (1-888-835-5322) TTY; faxing 1-866-418-0232; or writing to:

Federal Communications Commission
Consumer and Governmental Affairs Bureau
Consumer Inquiries and Complaints Division
445 12th Street, SW
Washington, DC 20554

###

*For this or any other consumer publication in an accessible format (electronic ASCII text, Braille, large print or audio), please write or call us at the address or phone number below, or send an email to **FCC504@fcc.gov**.*

This document is for consumer education purposes only and is not intended to affect any proceedings or cases involving this subject matter or related issues.

Last Reviewed 3/12/14