

Mobile Wallet Services Protection

Many consumers use their smartphones, tablets and other mobile devices as mobile wallets to pay for goods and services, downloading software that allows them to complete both online and in-person transactions. As our use of mobile wallet services increases, so does the need to protect mobile devices, wallet apps and associated data from theft and cyber attacks.

How to safeguard your mobile wallet

- 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 or visible in an unattended car.
- 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 app to find out what will happen and who to contact if your smartphone is stolen or lost, or if your mobile wallet 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.
 - ✓ Make your smartphone emit a loud sound ("scream") to help you or the police locate it.
- Be careful about the information you store on your mobile device. Social networking and other apps may pose a security risk and allow unwanted access to your personal information and mobile wallet data.

What to do if your mobile device is stolen

- If you are not certain whether your smartphone or mobile device has been stolen, or if you have simply misplaced it, try locating 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 reporting 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, report the theft to the police immediately – including the make and model, serial and IMEI or MEID number. Some service providers 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

Consumer Help Center

For more information on consumer issues, visit the FCC's Consumer Help Center at www.fcc.gov/consumers.

Accessible formats

To request this article in an accessible format - braille, large print, Word or text document or audio - write or call us at the address or phone number at the bottom of the page, or send an email to fcc504@fcc.gov.

Last Reviewed 10/31/16

