Protecting Your Assets

Facts And Tips On Keeping Mobile Payments Safe

(NAPSA)—You may have heard about mobile payments—using your smartphone, tablet or other mobile devices to pay for purchases. Mobile payments can be convenient, but are they safe? After all, smartphones and other mobile devices that can access the Internet are basically personal computers that you carry around with you. You can store your contacts, passwords and other personal information on these devices. In the case of mobile payments, you may be storing financial account information on them—information that someone else could use to make purchases or use for other fraudulent purposes.

Even with a mobile phone that doesn't have Internet access, if it has texting capability it could be used without your permission to charge purchases to your wireless account. So it's wise to guard your mobile device as you would your checkbook or wallet. Consumer Federation of America says that there are many things that you can do, and that industry is doing, to keep your personal information secure when you make mobile payments.

Security Features Built Into the Payment Process

There are many kinds of security features that may be built into the mobile payment process. Look for the answers to some basic questions when you consider using mobile payment applications or wallets.

- What authentication credentials (i.e., password, PIN number, biometric, etc.) does the payment service require to make payments?
- Are your financial account numbers and other sensitive information stored on your device or remotely, and how are they secured? Are the payment account numbers tokenized?
- What account information is transmitted to make the payment?
- Is encryption used to protect your personal information in transmission and storage?

Most mobile payment services require a password or PIN number to open the application. Don't share this information with anyone who doesn't have your permission to make payments using your accounts. Some mobile applications have added the option of using a biometric such as a fingerprint or facial scan to increase the level of protection against an unauthorized person making transactions. Others may email or text message confirmation of payments to double-check and ensure that they were legitimately made.

Your payment account information might be stored in a secure chip on your mobile device or on the server of the payment service itself. In some cases, what's stored on your device is not your actual account number but a substitute for it, either another account number or a "token" that represents your account. This adds another level of security, not only against intruders trying to get your account numbers but from data breaches at points along the payment chain, such as payment processors and retailers, because they only get the substitute numbers. As mobile payments evolve, so will these security features.

When account information is transmitted to make the payment, it is usually encrypted—turned into a code that can only be read by parties along the payment chain that need it and who have the "key" to unlock the code. Retailers and others are also using encryption and security tokens to make account numbers, passwords and other sensitive information that they store unusable if someone illegally accesses it.

There may be additional security features provided by the mobile device operating system, the mobile payment service, the payment provider (such as your payment card issuer) or the merchant.

Tips for Keeping Your Mobile Payment Secure

- Have your mobile device automatically lock when not used within a designated period of time.
- Keep your passwords and PIN numbers to yourself.
- Only download payment apps and other software from sources that you trust, such as your financial institution, a retailer that you do business with, or a trusted app store.
- Protect mobile devices that can access the Internet from hackers and malware by using security software and keeping it updated.
- Be extremely careful when you use free public Wi-Fi.
- NEVER jailbreak or disable the security features of your phone.
- Beware of messages from criminals pretending to be from your financial institution or someone else you trust asking for your account number or other personal information.
- If you receive an email unexpectedly asking you to click on a link or open an attachment, beware. If it's from an unknown source, delete it; if it looks like it's from someone you know, check with the person directly before you do anything.
- Never give access to your device to anyone who contacts you unexpectedly and only deal with tech support companies that you know or whose reputations you have checked out.

For more about how to protect your privacy and security when you make mobile payments, go to www.consumerfed.org/mobilepayments. These new educational materials were produced with a grant from the Digital Trust Foundation.