Global Knowledge®

Expert Reference Series of White Papers

Five Security Concerns with Mobile Payment Systems

Five Security Concerns with Mobile Payment Systems

James Michael Stewart, CISSP, CEHv3-8, CHFIv3-8, Security+, Global Knowledge Instructor

Introduction

With the popular adoption of Apple Pay, mobile payment systems have finally started to become commonplace. Although numerous mobile payment schemes have existed for years, only a few devices and limited number of retailers ever supported them. Now that many more consumers are interested in using mobile payments, it is important to evaluate just how secure or reliable such payment schemes are. Before you link your finances to a mobile device in order to make impulse purchases, there are five primary issues you need to consider.

Linking Your Finances to Mobile Payment Systems

Most mobile payment systems require that you link one or more of your existing financial accounts to the mobile payment system. They might require your credit card, debit card, ATM card, or even a direct link to your checking account. This linking allows the mobile payment system to apply the charges for purchases immediately to your existing financial account. Obviously this makes purchases convenient, but is that really the best move for you financially?

If a mobile payment system is able to place charges onto your accounts immediately, you should have a few concerns:

- If a fraudulent charge occurs, how difficult is it to get the charge canceled?
- If a fraudulent charge occurs and money is taken from my account, how hard is it to get my money back?
- If a duplicate charge occurs, what is required to get the duplicate charge(s) removed?
- Can I set a maximum per-charge ceiling? Or a ceiling for charges on a daily, weekly, or monthly basis?
- Does the mobile payment system have a per-charge transaction confirmation?
- Will the ease and convenience of mobile payments cause me to impulse spend? Can my finances handle that?
- If I decide to stop using the mobile payment system, how challenging is it to divorce my financial account from the payment system?

You need to investigate any mobile payment system prior to joining to obtain answers to these questions. If you are not satisfied with those answers, then don't use that mobile payment system.

There are some mobile payment systems that do not link directly to your existing financial accounts; instead you deposit money into them, similar to a gift card. These types of payment systems are less likely to cause significant harm to your finances in the event of a security breach, especially if you only deposit a small amount of money into the account, which you can handle losing if things go wrong.

My caution here may seem overblown in light of the proclamations from various mobile payment system vendors who claim they have the best security. It is important to realize that not all mobile payment systems are using the same security, thus they cannot all be the best at securing your financial and personal information. Over the last

four or five years, numerous mobile payment systems have been compromised or shown to have weaknesses. Some of these breaches only revealed the users' names and contact information, while a few have revealed credit card and bank account numbers. When selecting a mobile payment system, be sure to review several options and look for information about recent hacks and updates. Just because a system was hacked in 2012, does not necessarily mean it has the same weaknesses today. But it is your responsibility to make sound decisions when it comes to your finances. Don't be uninformed. To find out about recent concerns, perform a few Internet searches using the phrase "mobile payment" along with one of the following: attacks, hacks, exploits, vulnerabilities, weaknesses, updates, security, or patches.

Of the questions I suggested you ask, one of the most important is in regard to transaction confirmation. If a purchase is made without a confirmation process, then if your phone's identity is compromised or someone is able to mimic you payment signals, a hacker could then use your digital wallet to make purchases. With a per-transaction confirmation, you would have the opportunity to block a purchase by denying any transaction that you are not actively participating in. A transaction confirmation could be some sort of instant on-screen prompt or take place via SMS messaging. For larger purchases a phone call or email based confirmation might be available. Be sure to only use a mobile payment system with transaction confirmation.

While not directly threatening your finances, it is important to realize that even the robust Apple Pay solution is not without problems. No compromise of existing accounts has yet occurred, however, thieves are using Apple Pay to help make transactions against stolen credit cards. This is not a flaw in Apple Pay itself, it is instead a symptom of the poor credit card transaction mechanism currently implemented by banks and the fact that most banks do not confirm that the user of a credit card in Apple Pay is the actual rightful owner of that card at the time the card is loaded into Apple Pay. (For more information on this concern, please visit: http://www.droplabs.co/?p=1204 "Smart Mouse Traps and Lazy Mice"). There is a solution on the horizon for this issue; the use of chip and PIN credit cards is just beginning to roll out in the United States. Hopefully within three years or so, the majority of credit card issuers will have switched to this more secure system, as has the rest of the world.

Benefits and Protection Differences between Individuals and Businesses

Mobile payment systems are available for use by individuals and for businesses. As an employee or a business owner, you might be tempted to tie your business account (i.e., credit card, debit/ATM card, or bank account) to a mobile payment system. Before you do, keep this in mind: the law provides significant protection against loss and theft on personal accounts but very little protection for business accounts.

According to the FTC (http://www.consumer.ftc.gov/articles/0213-lost-or-stolen-credit-atm-and-debit-cards), liability for a lost or stolen credit card tops out at $50. This protection is even better for a credit card that is stolen before you receive it and use it; in that situation your loss is $0. An ATM or debit card is protected, but not quite as well. If a loss or theft occurs and you report it before charges take place, your loss is $0. If you report within two business days of the charges, your loss is capped at $50. If you report the issue in more than two business days but less than 60 days, then your loss is capped at $500. Any issues reported (or not) in more than 60 business days are fully your responsibility.

These protections make a good case of using a credit card instead of a debit or ATM card. They also make it clear that you need to be reviewing your accounts regularly for fraudulent activity. I would recommend checking the transactions on a credit card about once a week, but for an ATM or debit card once every two days.

While these are great protections for individuals, these protections do not apply to businesses. Business protections are defined under the Uniform Commercial Code (UCC) (http://www.law.cornell.edu/ucc). The UCC was initially published in 1952 with some amendments added over the years. Generally, businesses are held liable or responsible for losses, whether to their bank account, credit cards, or debit/ATM cards. In most cases, a bank will hold the business responsible for any fraudulent charges or withdrawals made prior to the time of the reporting of the loss or breach. In some cases, businesses have been held responsible for transactions occurring after the reporting. The UCC states that a business must show due-diligence in order to reduce their liability in the event of a financial fraud or attack against their accounts. If you are a business owner or are an employee and wish to use a business account on a mobile payment system, I recommend contacting your bank and asking for written information about your responsibilities and liabilities. If you are uncomfortable with the level of risk that using a business account imparts, then consider using a personal financial account for mobile payment instead.

The Trade-Off between Security and Convenience

Mobile payment systems are the future of retail transactions. Carrying around a pocket full of credit cards, ATM cards, and debit cards (not to mention the plethora of store loyalty cards) is a pain. Credit cards are easily lost or stolen, their bulk adds up when stacked in a wallet, and they often leave your sight when making a transaction (such as at a restaurant or when the point of sale [POS] device is behind the sales counter). A mobile payment solution rids you of the task of carrying around credit cards, saves space in your pocket or purse, and never leaves your possession when making a transaction. A mobile device can be lost or stolen, but unlike a credit card, it can have on-device security configured (such as a screen lock with password and storage encryption) and support remote tracking and remote wiping. Thus, mobile payments might be a better solution . . . eventually.

My concern is that many of the mobile payment systems available today do not provide sufficient security. There are lots of issues that a mobile payment user must face such as:

- When storing a credit, ATM, or debit card in a mobile payment system, is your account at risk of eavesdropping or compromise? In other words, how easy is it for hackers to break into your mobile payment account and learn your card numbers?
- Can this be attempted against an online service or must an attack occur on or against my mobile device?
- Is the mobile payment app on my mobile device at risk from malicious code infections?
- If I root my device, how does this affect the security of the mobile payment app?

If a mobile payment system stores your financial information on the device, then it is at risk of eavesdropping when being transmitted for a purchase and it is at risk at all times from malware infection of the mobile device. If the mobile payment system stores your financial information in an online service database, then attacks could be waged against that service without needing to attack on or through your mobile device. If you choose to root your phone, your device has an increased risk of malware infection as a wide range of malware can only infect a device if rooted. Often, not rooting is a more secure configuration to maintain, especially if using a mobile payment system.

When selecting a mobile payment system, you should consider several important security items:

- Is the mobile payment app always active once the mobile device boots or is it only active when its app is launched?
- Does the mobile payment app time out or become disabled after a timeout idle period or does it stay operating in the background after use?
- Does the mobile payment app require a login, PIN, or other mechanism to authorize its launch?
- Does the mobile payment app require a confirmation when a transaction is attempted?
- Does the mobile payment app display the amount being charged before the transaction can be processed?

It is again upon you, the user, to consider the security and the protections a mobile payment system offers. If you are not satisfied with your findings after investigating these concerns, you should probably not use that mobile payment system. If a system seems to provide satisfactory (i.e., secure) answers to these issues, then it might be worth using without putting you and your money at risk.

Many mobile payment systems have focused on ease of use rather than security of transaction. This is often touted as reduced friction—the concept of making the purchase transaction process as streamlined as possible. Unfortunately, the more friction-less the process, the more likely you will make accidental purchases, have fraudulent purchases made on your account, or make more impulse purchases. I do not want a mobile payment system that is so simple that just the act of waving my phone within inches of a POS device allows the transaction. I want a payment system that requires me to intentionally launch or active the system and then still require a per-transaction confirmation after viewing the charge amount.

Digital Payment Issues

Digital payments are the future of monetary transactions. We are slowly moving into the future where physical currency will continue to fade into disuse and plastic will become overly cumbersome by comparison to digital payment systems. Mobile payments will become the norm, but they are currently supported only by a minority of merchants.

Over the last four to five years, the availability of functional mobile or digital payment systems has remained rather stagnant. There have been many developments and improvements to the systems, but very slow adoption. This has changed since Apple announced and released its solution, Apple Pay. With the popularity of Apple mobile devices, the use of Apple Pay is widely available on the device in customer's pockets, thus with this demand, merchants are eager to meet those expectations with supply (i.e., support mobile payments at their POS). There have been some kinks in the recent Apple Pay adoption, such as some other digital/mobile payment groups attempting to ink non-competition deals with merchants, but these prohibitions will not last. As Apple Pay adoption increases, so does the increase of other technologically similar mobile payment systems, such as those based on NFC (like Google Wallet).

So, commerce of the future will be driven by digital and mobile payment systems. But that future is still many years off. Today, it is still a challenge to use mobile payments even at merchants that accept them. Salespersons are not always trained thoroughly on mobile payments and may not fully understand what technologies their POS accepts nor what contractual obligations their company has to accept or reject certain payment systems. For now, you still need to be prepared to pay with plastic or cash in the event that the mobile payment system is unavailable or just doesn’t work as expected. If you are a serious advocate of mobile payments and want to advance their use, I need to make one request: if a salesperson is unable to get a mobile payment mechanism to function, be polite and offer to use an alternate method of payment. Don't berate the person for not knowing how to get the new system working and don't waste the time of others behind you in line. If you must complain, ask to speak with a manager (after your transaction is complete), and then calmly explain your frustration to the person who should have the authority to seek out a resolution.

Generally, you will find that mobile payment options are more secure, robust, and convenient than using traditional means of legal tender, whether paper or plastic. Anything you might currently carry in your wallet is at risk of being lost or stolen. Once someone else has your cash in hand, there are no security restrictions on its use. Also, the thief might use your plastic during the time between the theft and the moment you report the loss to the bank. Your mobile device should have a screen lock and is likely trackable via GPS, so there are greater security protections on your mobile device. However, it is your responsibility to ensure that those security features are enabled and properly configured.

What about Customer Service after the Sale?

One of the most frustrating experiences we all encounter is when there is a need to contact customer service. I hate calling customer service. It always seems like I have to explain myself several times to different representatives. Then I'm told about solutions, which were obvious to me to begin with and which I have already tried, which don't work. I'm often treated as if I don't know what I'm doing and the fact that I have a problem is a personal affront to the customer service representative (CSR). I don't want to imagine the frustrations we will have when there is a problem to be resolved with a mobile payment system in the mix.

The good news is that if you link a personal credit card to a mobile payment system, then all the benefits of using that credit card will be retained whether you use the plastic itself, use it online or use it in a digital or mobile payment system. Thus, the protections against fraudulent transactions are retained as well as your ability to dispute transactions quickly either via the bank's website, mobile app, or over the phone. Furthermore, if your credit card extends or doubles product warranties then that benefit is retained as well.

However, while these benefits are intended to extend to all uses of your credit card account that does not necessarily dictate that obtaining or using those benefits is simple or easy. Be prepared to face challenges when disputing a mobile payment transaction. You might find yourself in the middle between the disinterested parties of the merchant, mobile payment provider, and the bank that issued the credit card. While the law dictates your protections and rights, the technology and the contracts between the various entities can make exercising your rights or benefiting from the protections maddening.

While your bank should allow you to dispute a charge, if they only communicate with the mobile payment provider, they may be informed that the transaction seems legitimate to the provider. Only by communicating with both the mobile payment provider and the merchant is such a claim of legitimacy verified. If the merchant does not show a record of an intended purchase but the mobile payment provider does, this could indicate a fraudulent transaction. If you suspect a conflict or a lack of communication between the merchant, mobile payment provider, and the bank, you may need to get involved. Print out copies of your statements. Contact the merchant to inquire about any invoices or receipts they may have in relation to the disputed charge. Review the agreement you made with your credit card bank and the mobile payment provider—if you don't know what you agreed to nor the rights or privileges those contracts provide, then you won't be able to defend your position adequately.

Another concern is that of returns. What if you need to return a product to a merchant? Does a mobile payment system make that seamless or complicated? Again, reviewing the returns policy of the merchant will be your best starting point. You need to know the parameters of returns, such as condition, time since purchase, requirements for receipt, etc. You might discover that while you can return merchandise, you might not be able to get a charge refunded back to your credit card or ATM/debit card. You might have to accept store credit or credit in the mobile payment system (which might be limited to that merchant, thus similar to store credit), which might be only be usable against any other transaction from any other supporting/supported merchant. Always ask for documentation regarding a return and the amount and means of the refund. Once you have returned the merchandise, you have no remaining leverage to get your money back without documentation.

When using a mobile payment system, how challenging is it to obtain a refund when you are dissatisfied with a non-returnable item, such as service or a meal? You need to be aware of the refund policy of the merchant and the policy of handling and processing refunds of your mobile payment system as well as the credit/ATM/debit card. Until you have a need for a return or a refund, you won't know exactly how challenging or simple this process will be. However, you need to be prepared to advocate for yourself. Be informed, keep your receipt records, and monitor your accounts.

One additional concern is that of processing errors. When merchant charges you the wrong amount or causes a double transaction, who should you contact first in resolving these problems? Generally, start with the merchant. Inform them of the processing error and be sure to inform them that a mobile payment system was used for the transaction. You might be the first person to have such an issue with the merchant (or at least handled by this specific salesperson), so be patient. Ask what their process is for resolving processing errors and whether they can provide you with documentation of your resolution.

Conclusion

As you can see, I don't have all the answers in regard to mobile payment systems. They have solid promise to become the dominant means of financial transactions, but there are some hurdles to overcome. Apple Pay might be the dominant force today, but Google Wallet and others are not far behind. The year 2014 was when digital and mobile payment systems became known to a wide range of the general population, while only techno-enthusiasts were aware of the options in the four to five years prior. Thus, mobile payment systems are not new, but customers and merchants are quickly adopting them now that they have become popular. It still remains your responsibility to thoroughly research any mobile payment option before implementing it. It is your money and you have the burden of ensuring that it has the best protection possible.

As an Android user, I've not worked directly with Apple Pay, but I have used a few of the options available on Android devices. Not every attempt to make a purchase using a mobile payment system went through smoothly or at all. I've had to pull out my wallet after a few failed attempts in making a purchase using my phone. I've also had to return a product and resolve a double charge issue. So, I'm familiar with the hassles that the current systems levy on the customer. So, I have a few final suggestions to maximize your security and benefits while minimizing some of the downsides of using a mobile payment system:

- Use a dedicated credit card for the mobile payment system that is not used for any other purpose.
- Monitor your credit card statement online or through an app at least once a week.
- Do not use an ATM or debt card and NEVER link a checking account directly to a mobile payment system.
- Double-check the amount before confirming any transaction.
- Keep your mobile device secured with storage encryption, screen lock with password/fingerprint/face recognition, and do not root your device.
- Do not attempt to use two different mobile device payment solutions on the same device. Uninstall the app controlling one system before installing the app to control another solution.

These steps will only help you if you do your research and select from the best and most secure mobile payment solutions. I do encourage you to try out mobile payments, as you might find them a benefit to your common purchases, such as beverages, meals, public transportation, etc. But, never overlook the fact that you are linking money to your mobile device. The further away you separate your financial transactions from physically holding dollar bills, the easier it is to spend and treat money like points in a video game. Don't get caught up in spending what you can't afford to spend. Otherwise, see you at the checkout counter.

Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge through training.

- Cybersecurity Foundations
- Cyber Security Compliance & Mobility Course (CSCMC)
- Computer Hacking Forensic Investigator (CHFI) v8

Visit **www.globalknowledge.com** or call **1-800-COURSES (1-800-268-7737)** to speak with a Global Knowledge training advisor.

About the Author

James Michael Stewart has been working with computers and technology for over thirty years. His work focuses on security, certification, and various operating systems. Recently, Michael has been teaching job skill and certification courses, such as CISSP, ethical hacking/penetration testing, computer forensics, and Security+. He is the primary author of *CISSP Study Guide, 6th Edition; CompTIA Security+ Review Guide: SY0-401; Security+ Review Guide, 2nd Edition (SY0-301)*; *CompTIA Security+ Training Kit (Exam SY0-301)*; and *Network Security, Firewalls, and VPNs*.

Michael has also contributed to many other security-focused materials including exam preparation guides, practice exams, DVD video instruction, and courseware. In addition, Michael has co-authored numerous books on other security, certification, and administration topics. He has developed certification courseware and training materials as well as presented these materials in the classroom.

Michael holds a variety of certifications, including: CISSP, CEH, CHFI, and Security+. Michael graduated in 1992 from the University of Texas at Austin with a bachelor's degree in philosophy. Despite his degree, his computer knowledge is self-acquired, based on seat-of-the-pants hands-on "street smarts" experience. You can reach Michael by email at michael@impactonline.com.