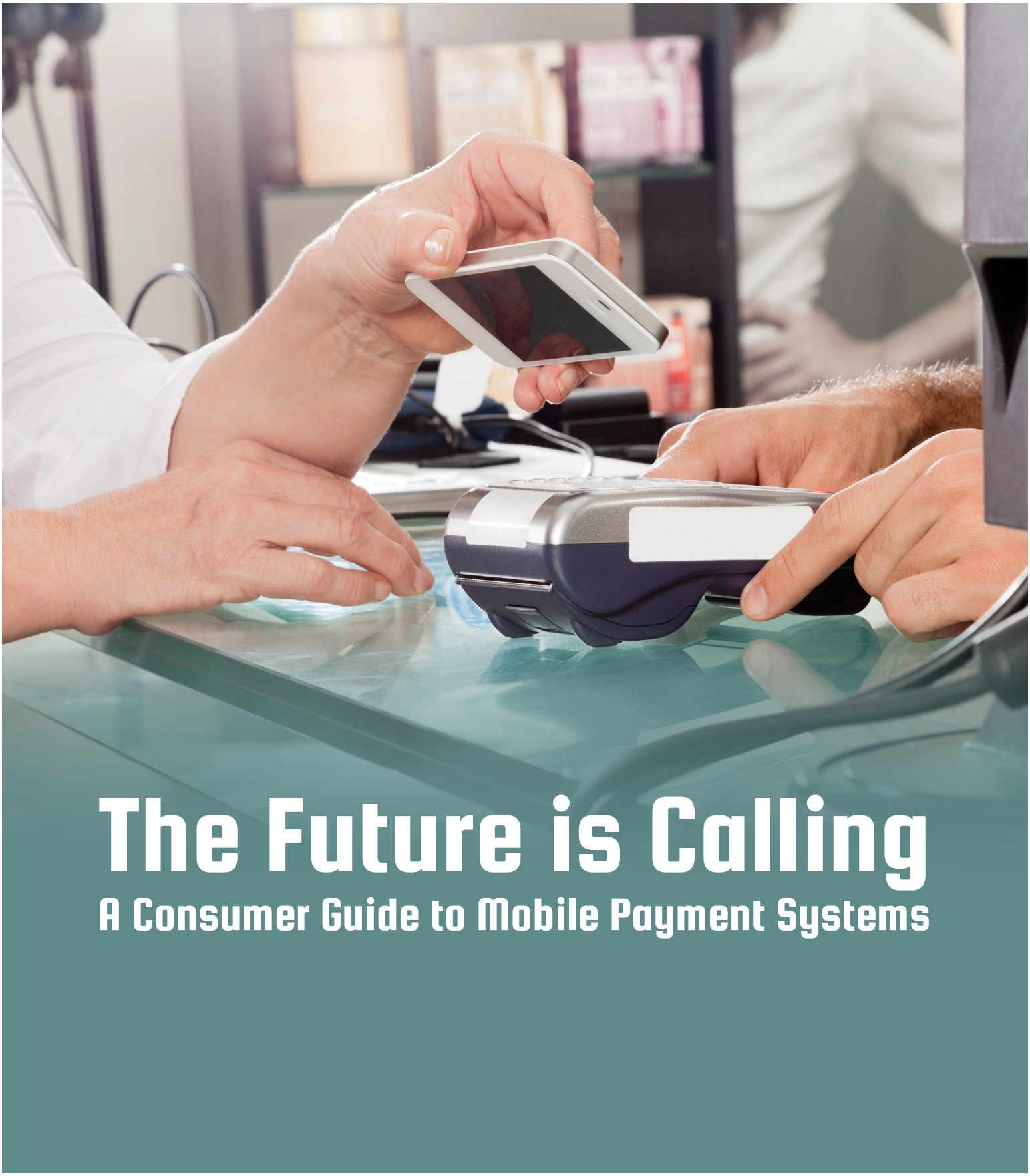


The Future is Calling

A Consumer Guide to Mobile Payment Systems

CALPIRG
Education Fund

The Future is Calling

A Consumer Guide to Mobile Payment Systems

CALPIRG Education Fund

Jonathan Fox

Summer 2013

Acknowledgments

The author wishes to thank Tony Dutzik, Senior Policy Analyst at Frontier Group, Ed Mierzwinski USPIRG Education Fund Consumer Program Director, and Emily Rusch, CALPIRG Education Fund Director, for their invaluable assistance in writing and editing this report.

This report was made possible due to the generous support of the California Consumer Protection Foundation.

The author bears responsibility for any factual errors. The recommendations are those of the CALPIRG Education Fund. The views expressed in this guide are those of the author and do not necessarily reflect those of the funders or those who provided review.

CALPIRG Education Fund offers an independent voice that works on behalf of the public interest. CALPIRG Education Fund, a 501 (c)(3) organization, works to protect consumers and promote good business practices. We examine problems, craft solutions, educate the public, and offer Californians meaningful opportunities for civic participation.

For more information about CALPIRG Education fund or for additional copies of this report, please visit us at www.calpirgedfund.org

Cover photo: Tyler Olson/Bigstock

Layout: Alec Meltzer Print & Web Design

Executive Summary

Businesses constantly look to provide consumers new and easier ways to shop. In addition to cash, checks, and credit cards, consumers across the U.S. will increasingly be able to shop and purchase new products using mobile payment systems on their smart-phones and mobile devices. A poll of 1,000 financial services, technology, telecommunications, and retail executives revealed that 83 percent of those executives believed that mobile payments will "achieve widespread mainstream consumer adoption" by 2015.[1] Mobile commerce in the U.S. is expected to reach $31 billion by 2016, roughly 7 percent of overall electronic commerce sales.[2] While mobile payment systems today present a new world of opportunity for both consumers and business, they also come with some risk.

American consumers are increasingly finding more merchants providing access to mobile payment systems. Today more than 125 million Americans own smartphones, more than 54 percent of the total mobile phone market.[3] The increasing prevalence of smartphones and mobile devices is a key driver for business to adopt new mobile payment systems.

Risks to consumers, unclear rules

As with many new consumer products, the development of mobile payment technology has outpaced the law. Today consumers are familiar with a variety of payment options and associated consumer protections for credit cards, debit cards, checks, and cash. As new technology advances, consumers must have access to the information necessary to make smart financial choices. In a survey, over 90 percent of respondents said they would make a mobile payment if they knew it was secure.[4] The Federal Reserve found that while 87 percent of the U.S. population owns a mobile phone (half of which are smartphones) only about 12 percent of mobile phone owners had used mobile payment services. Concerns revolving around the security of the technology were the primary reason given for not using mobile payments (42 percent).[5]

The introduction of mobile payment systems is proving to be a paradigm shift, with new payment systems challenging old regulatory frameworks. For mobile payments to catch on, consumers must understand the true security concerns surrounding mobile payments and learn the proper ways to keep their finances safe and secure. With the specter of both fraud and financial theft looming, CALPIRG Education Fund set out to answer the following key questions to help consumers use mobile payment systems on their wireless devices with confidence: Are payments secure? Are the relevant dispute processes clear? And what is the state of consumer privacy with mobile payment apps?

This report provides consumers with the information they need to best utilize mobile payment systems in a secure and safe way and concludes with recommendations for policymakers to strengthen consumer protections in the future.[6]

Mobile payments, the Pros & Cons

The key advantages provided to consumers include the following:

1. Mobile payments make it **easier for consumers** to shop while using their personal mobile devices, easily selecting different cards and coupons for different transactions, thus maximizing rewards and card benefits.

2. Mobile payment technologies leverage **built-in security features** on the device and account identifiers to more effectively verify the consumers' identity to provide more secure transactions.

3. Mobile payments made using a credit or debit card account maintain the same level of **consumer protections** associated with those cards by existing laws and regulations.

The key disadvantages of mobile payment systems for consumers include the following:

1. Questions arise as to who maintains control of the data created during transactions. New mobile payment systems make it easier to aggregate separate data to identify consumers, to frame shopping patterns, and to share sensitive consumer data (such as location, gender, shopping habits, and social background) with more businesses.

2. New mobile payment systems blur the traditional relationships and responsibilities between wireless service provider (AT&T or Verizon), mobile payment system providers (ISIS or Google Wallet), and financial institutions (banks and credit card companies).[7]

3. There is the risk that technological barriers will limit interoperability between closed ecosystems, which will restrict consumer choice and increase costs.

Policy recommendations:

For policymakers:

1. As the law now stands, it is not clear how mobile payment system providers themselves should safeguard consumer data. Policymakers should ensure that the introduction of new technologies to the marketplace does not circumvent hard-won existing consumer protections.

For regulators:

1. Regulators should clarify the role and liability mobile payment service providers hold towards consumers in regards to privacy and financial protections.

2. Regulators should prohibit the use of consumers' information collected for the purposes of completing financial transactions and fraud prevention for other purposes, especially marketing purposes.

3. Regulators should urge mobile payment service providers companies to employ necessary security measures to protect consumer's sensitive financial information from loss or misuse.

For business leaders:

1. Mobile payment service providers should pro-actively provide consumers with clear information regarding consumers' financial liability and provide them with a toll-free customer care phone number to contest charges.

2. Mobile payment service providers should implement mandatory safeguards to protect consumer data from unauthorized access.

3. Mobile payment service providers should adopt three principles in their practices:

"Privacy by design" , context-based privacy choices, and full transparency in communicating what data is collected from consumers, who it is shared with, and how it is used.

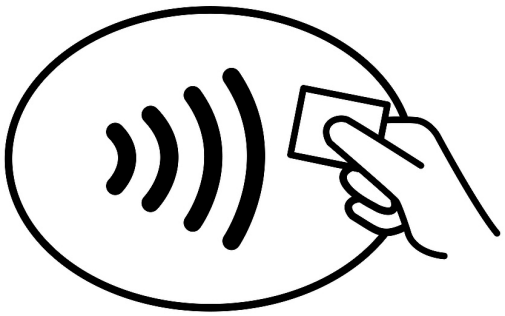
For consumers:

1. Associate credit cards with mobile payment apps to ensure the highest level of financial protection.

2. Alternately, consider loading a pre-paid debit card with limited funds for small purchases.

3. Remember to enable password protection on your mobile device, especially for all financial apps.

4. Bring disputed charges and other complaints to the attention of the card issuer as you would with a normal use of your credit or debit card.



5. When a device with a mobile payment app is lost or stolen, contact the mobile payment service provider to disable the app to prevent unauthorized access.

6. To protect your privacy, be aware of what you are buying and how you pay for it. Remember mobile payments (like most non-cash transactions) are being tracked and monitored.

Mobile Wallet:
An overview of consumer mobile payment technologies

Today's mobile phones are much more than just phones - they are mobile computers, books, and even movie players. Increasingly mobile phones can also function as mobile wallets, holding various credit and debit cards in addition to individual reward cards. While several mobile payments technologies exist, this section focuses on the two most common smart-phone based mobile payments systems available for American consumers - *proximity mobile-payments* and *P-2-P (person to person) mobile-payments*.

I. Proximity mobile payments

"Proximity" mobile payments refer to payments made when you swipe or touch your phone to a check-out terminal to complete a purchase. Here's how it works:

Proximity mobile payments occur at the point of sale, when consumers use a mobile phone with built-in near field communication (NFC) technology to make a purchase. NFC allows two devices in close proximity to each other – usually less than four inches - to communicate via radio waves. NFC technology takes advantage of existing smart card capabilities building on today's ubiquitous payment and wireless network infrastructure. Utilizing the best of both worlds, NFC allows secure in-store mobile payment at merchant locations equipped with NFC-compatible point of sale (POS) terminals.

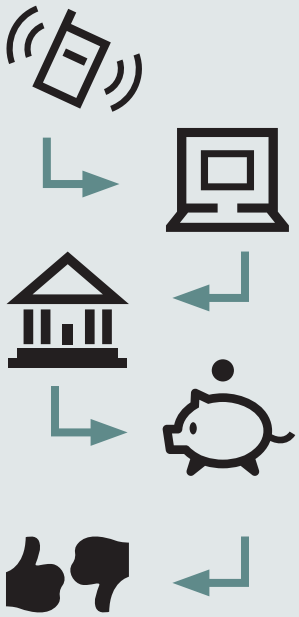
NFC technology often resides in the secure element component of a mobile phone that is used to store and execute sensitive applications while maintaining security and confidentiality. The secure element is a smart card chip that contains a separate microprocessor with an operating system, memory, an application environment, and security protocols.[8]

Google Wallet & ISIS Mobile Wallet [9]

Google Wallet and *ISIS Mobile Wallet* are two leading mobile apps for NFC-enabled smart phones. Using these apps, consumers pre-load payment and loyalty cards onto their NFC-enabled smart phones, and use them to pay in stores with NFC enabled POS systems. Google Wallet is accepted by more than 200,000 merchants across the United States.[10] *ISIS Mobile Wallet* is an initiative driven by T-Mobile, Verizon and AT&T. These mobile operators are pooling their combined subscriber base of more than 200 million consumers[11] (a market share of over 76%) to drive NFC adoption. Currently, ISIS is only available in Salt Lake City, Utah, and Austin, Texas.

How it Works?

Proximity mobile payments take place through the following steps:



1. The customer waves their phone near the POS terminal;
2. The POS terminal reads the phone's NFC chip, receives the phone's serial number and the transaction's unique code and sends this data to the merchant's payment processing system;
3. The payment processing system sends the transaction data to the customer's issuing bank;
4. The issuing bank uses the transaction's unique code to authenticate the phone's validity and the phone's serial number to identify the account from which to authorize payment; and
5. The issuing bank authorizes or declines the transaction to the acquiring bank.

II. P-2-P (person to person)

The second type of commonly available mobile payments in the United States is P-2-P (person to person) systems. These do not require NFC technology, rather, customers use text messaging or mobile apps to make payments any time, any place. This is used when a consumer either sends a text as payment or pays for something using the internet on their phone.

To truly take off, NFC-based payment systems need to become an easy and commonly found payment option for consumers. Merchants must first acquire the necessary NFC enabled infrastructure before consumers can become accustomed to using it. However, merchants will resist paying for the extra expense until enough consumers adopt mobile payments so that they find investment in the system profitable. To overcome this "Chicken & Egg" problem, mobile payment providers have begun subsidizing (to varying degrees) NFC-enabled POS devices to encourage merchants to adopt the technology.

Target Mobile App

Target recently introduced mobile gift card apps that allow customers to load a gift card balance onto their smart phones—without requiring NFC—and make in-store purchases. When consumers are ready to pay in a Target store, they can simply ask the cashier to scan the barcode on their mobile phone screen to deduct from their card balance.

Disputes & Liability

An overview of mobile payment financial protections

Today consumers are accustomed to a variety of payment options –such as credit cards, debit cards, checks, and cash - which provide consumers with different levels of protection. Credit cards provide the highest level of consumer protection, while checks and debit cards provide more control over personal finances but with fewer consumer protections. Cash provides consumers with anonymity and convenience, yet virtually no financial protections. Over time consumers have become accustomed and acquainted (to varying degrees) with these payment systems and the protections they provide. But what about the new forms of mobile payments? Do mobile payments have adequate consumer protections? Are payments secure and are dispute processes clear? The answer depends on the type of payment card consumers choose to use with their mobile payment app.

If a consumer associates his or her credit card with their Google Wallet account, then all parties are subject to the rules and regulations governing credit cards, including liabilities and dispute mechanisms.[12] The same consumer may also choose to load a debit card and a gift card as well onto their Google Wallet account. If the consumer chooses to use those cards instead of a credit card, they face potentially unlimited personal liability. Just like physical wallets, the card we choose to use gives us different levels of consumer protection. Thus a consumer using three different types of card on the same mobile phone will be subject to three different regulatory frameworks depending on the type of card used during a specific transaction.

What rules apply to a gift card loaded onto a mobile payment app?

The Federal Reserve adopted Section 205.20 of Regulation E to implement Section 915's "gift card fee and expiration prohibitions."[13] This prohibition applies to a device with "a chip or other embedded mechanism that links the device to stored funds, such as a mobile phone."[14] Therefore, mobile gift cards such as Target's discussed above are exempt from Regulation E and are subject to weaker gift card statutes and legislation.

Similarly, the way consumers dispute purchases made using mobile payment systems depends on the type of card used during the purchase. For example, if a consumer used their credit card they would contact their card issuer, and if they used a gift card they would contact the card-issuer.

While less common then NFC-enabled or P-2-P payments, direct mobile carrier billing also can be found in today's market. With this atypical form of payment, charges for purchases made via online apps or directly from a phone appear on a consumers' mobile phone bill. Direct

Varying Degrees of Protection

Credit cards: Provide the strongest level of statutory protection, capping personal liability for unauthorized use at $50.[15]

ATM/Debit Cards: A consumer's liability for unauthorized transfers is limited to $50 if reported within two business days, and up to $500 for charges reported after two business days.[16] Some banks offer to extend credit card-like protections to ATM/debit cards, but these are often subject to exceptions and the banks own terms rather then federal legislation.

Pre-paid debit cards and gift cards: There are no federal statutes besides the FTC Act that protect consumers from unauthorized charges if their mobile payment mechanism is linked to a gift card or pre-paid debit card.

Mobile carrier billing: There is no federal legislation specifically protecting consumers who are billed for services through their mobile service provider on their monthly bill. Rather, consumers are dependent on their mobile service providers' terms of service and internal polices, which may vary.

mobile carrier billing is particularly risky for consumers due to limited legal protections and common incidence of fraudulent "cramming" charges on mobile phone bills – during which charges are added to a consumer's monthly bill by a third party without consent or proper disclosure.[17] "Cramming" fraud combined with low levels of protection for consumers opting for mobile carrier billing pose a serious risk to consumer financial safety, and may undermine consumers' trust in mobile carrier billing as a trusted payment option.

Unlike the illegal practice of "cramming", several mobile service providers have agreements with third parties that allow them to place charges directly on consumer's mobile phone bills. For example, Google allows certain Android app purchases to be charged directly to a consumer's mobile phone bill rather than other more secure payment platforms.[18] However, consumers should always avoid paying for mobile services directly on their monthly mobile phone bill since there are no federal protections governing consumer disputes about fraudulent or unauthorized charges placed on mobile carrier bills.[19]

While some mobile payment providers voluntarily provide additional consumer protections that limited their customers' liability for fraudulent or unauthorized charges, this is not standard practice, the level of additional protection offered is not consistent, and such protections exist at the discretion of the mobile payment providers.[20]

Tips for protecting your finances on mobile payment apps

Given the robust technological security mechanisms built into mobile payment systems, consumers can feel confident in shopping with them. Nonetheless, to best protect themselves from financial loss or fraud, consumers should follow these rules when using mobile payment apps:

1. Associate credit cards with mobile payment apps, since they provide the highest level of consumer protection.

2. Alternately, consider loading a pre-paid debit card with limited funds for small purchases onto the mobile payment app. While pre-paid debit cards provide a low level of consumer protection, consumers can limit their balance and thus reduce their exposure to financial loss.

3. Enable password protection on your mobile device, especially for all financial apps.

4. When problems occur (disputed charges, complaints, etc.), bring it to the attention of the card issuer as you would during the normal use of your credit or debit card.

5. When a device with a mobile payment app is lost or stolen, contact the mobile payment service provider (e.g. Google Wallet or ISIS) to disable the app to prevent unauthorized access. In addition, you should also contact the issuer of each of the payment cards loaded onto the mobile payment app.

6. To protect your privacy, be aware of what you are buying and how you pay for it. Remember mobile payments (like most non-cash transactions) are being tracked and monitored.

Data Security & Privacy Protections with Mobile Payments

Data Security Protections

We know consumers are worried about security and privacy protections. When surveyed, over 90 percent of U.S. respondents said they would make a mobile payment if they knew it was secure.[21] A separate survey by the Federal Reserve found that concerns about security were the primary reason (42 percent) keeping consumers from using mobile payments.[22] The good news is that most mobile payments are even more secure than other forms of payment. An obvious difference is that when making a mobile payment, the consumer uses their own device under their control, rather than a public device that can be manipulated or observed by others with criminal intent. The bad news is that consumers have fewer privacy protections with mobile payments.

	Mobile Payment	Credit or Debit Card
Transfer of payment data	✔ End-to-end encryption wherein the entire payment process is encrypted.	✗ At some point in the payment process, financial data is transmitted or stored in an unencrypted form.
Financial identifier	✔ Utilizes dynamic cryptogram authentication technology, whereby unique payment information is generated for each transaction.	✗ The financial information on a card's magnetic stripe that is sent from a merchant to a bank is the same sent each time a consumer makes a payment.
Data interception	✔ If the financial data is intercepted during the transaction, it cannot be used again for another transaction.	✗ If the financial information is intercepted, it can be used repeatedly for other unauthorized transactions.
Data storage	✔ Payment information can be stored on a secure element that is separate from the rest of a phone's memory, and significantly less vulnerable.	✗ Payment information is stored with many different entities, and is vulnerable to interception at various stages.
Password protection	✔ Mobile payment systems offer two stages of protection, requiring a PIN password to sign into payment application and another to make a purchase.	✗ Password is used only once at POS terminal.

Some of the technological data security solutions for mobile payment systems available today include:[23]

1. Storing the payment application and data in the secure element of mobile device.

2. Tamper resistance and secure transaction data transmission using built-in secure element technology to authenticate all communications.

3. Using an additional personal identification number (PIN) to authorize access to the mobile payment app on a mobile device. This is a further layer of protection to prevent un-authorized use if a consumer's device is lost or stolen.

4. Use of dynamic cryptogram authentication technology to protect transaction data already built into mobile payment apps.

Mobile Payments Increase Consumer Tracking and Privacy Risks

In the absence of robust privacy policies, mobile payments allow companies to gather, track, and compile information about consumer spending habits.[27]

The increased quantity of companies involved with mobile payments and the large amount of personal consumer data potentially being collected raises significant consumer privacy concerns. New mobile payment providers, such as Google and ISIS, join the list of players who already gather and consolidate personal and purchase data and give many consumers cause for worry. While mobile payment systems provide strong technological protections from identity theft and other fraud, questions remain regarding how the companies responsible for those systems plan on securing consumer privacy.

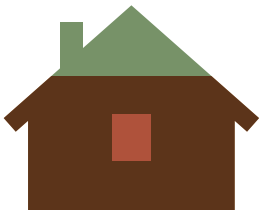
Using a traditional payment system, all parties have an incomplete view of the consumer transaction. [28] Merchants cannot relate purchases to unique and traceable customer identities or monitor shopping behavior (unless consumers use loyalty cards). The payment provider (e.g.

Consumers Want Privacy as They Shop

96% object to stores tracking by phone when they visit without making a purchase[24]

81% object to transfer of phone number to a store when making a purchase[25]

51% object to transfer of email address to a store when making a purchase[26]



81% object to transfer of home address to a store when making a purchase[26]

Under a cloud

How companies combine information about consumers from different platforms.

In Store: Phone transmits location, date, and time of purchase.

Online: searches, email, social networking.

On phone: geo-location of stores I live by and/or frequent.

Visa or MasterCard) also learns very little from an individual transaction – no more than the account number, the amount of the charge, and the merchant's identity. The banks involved (either the merchant's or the consumer's), usually only receives the total amount of the purchase and where the purchase was made.

However with mobile payment systems, companies like ISIS know the time, day, location and type of product purchased, and can combine that information with geo-location data gathered from the consumers' mobile device. Companies like Google can further combine the data gathered via Google Wallet with other information associated with the users' email address and the previous online searches via Google. While some consumers may assume some information is being shared with business they interact with, most do not assume that information from different sources - e.g. in-store shopping, online searches, and geo-location from mobile device - is regularly combined to create consumer profiles. Nonetheless, this is a common business practice. Of concern is a statement by Google in which they indicated that it will not collect an interchange fee on transactions made through Google Wallet.[29] This may suggest that Google sees its profits stream coming not from the revenue and expense sharing arrangements for in-store payments,[30] but from consumer data.

Companies combine different data-points to create meticulous consumer profiles mapping her or his interests, price sensitivity, preferred shopping locations, and shopping habits. On the plus side, business empowered with this robust consumer profile can enhance a consumers' retail experience by providing targeted offers better suited for the consumer. On the downside, these same capabilities also allow business to charge consumers different - often higher - prices for the same product based on the information they have gathered.

Mobile payment systems push the boundaries of existing consumer privacy laws and regulations. For example, after a mobile payment system transfers contact information to the merchant, merchants will be more likely to contact the consumer with sales calls or emails.[31] Under existing privacy rules, mobile payment providers could share consumer information with third parties without the affirmative consent of the consumer. Mobile payment providers could also use it for their own marketing, research, or other purposes.[32]

Such new opportunities to share consumer data have profound consequences for consumer privacy. Notably, it will be increasingly difficult for consumers to avoid "profiling" and being placed in specific consumer marketing "baskets" with limited options and pricing. In addition, it would remove the possibility of shopping anonymously, which many consumers prefer.[33] Widespread consumer data collection could cause consumers embarrassment, lead them to avoid buying certain items, or possibly contribute to mechanisms that institute widespread service and price discrimination.[34]

The Pros & Cons

As noted, mobile payment systems hold many advantages for consumers, alongside with some risks. The key advantages provided to consumers include the following: [35]

1. **Convenience**: Mobile payments make it easier for consumers to shop using their personal mobile devices. Some mobile payment apps can warn consumers in case they have insufficient funds to clear the transaction, thus avoiding overdraft fees. Within most mobile wallet apps, consumers can easily select different cards for different transactions, thus maximizing rewards or favorable interest rates.

2. **Security**: Mobile payment technologies leverage known behavior patterns, built-in security features and account identifiers to more effectively verify the consumers' identity to provide more secure transactions. NFC-enabled devices also meet the high security standards for device communication imposed by financial institutions. If a consumer loses her or his mobile device, mobile wallet applications can be blocked remotely upon request.

3. **Protection**: Mobile payments made using a credit or debit card account maintain the same level of consumer protections associated with those cards by existing laws and regulations.

4. **All the information in one place**: Mobile payment systems can store all the coupons and loyalty cards a consumer acquires on their mobile devices, allowing consumers to use them even if they forget the physical card at home. Mobile payment systems may even be able to trigger localized offers or present new coupons to the consumer in real time while still shopping. Furthermore, a mobile wallet automatically provides a digital receipt, simplifying consumer's ability to return items and track expenses.

The key disadvantages of mobile payment systems for consumers include the following: [36]

1. **Consumer data protection**: With the introduction of new players into the payment process, questions arise as to who maintains control of the data created during transactions. With traditional payment systems, each actor in the transaction chain only had access to partial information. However, new mobile payment systems make it easier to aggregate separate data to identify consumers, to frame shopping patterns, and to share sensitive consumer data (such as location, gender, shopping habits, and social background) with more businesses.

2. **Blurring of relationships**: New mobile payment systems complicate the relationship between the wireless service provider (AT&T or Verizon), the mobile payment system provider (ISIS or Google Wallet), and financial institutions (banks and credit card companies).[37]

3. **Technical barriers to adoption**: In addition to the privacy concerns noted above, there is the risk that technological barriers will limit interoperability between closed ecosystems, which will restrict consumer choice and increase costs. In order to provide consumers with a more robust selection of mobile payment enabled devices, increased cooperation between mobile payment service providers, device manufactures, and wireless service providers is needed.

Policy recommendations:

For policymakers:

1. At present it is unclear whether or not merchants can request personal information when a consumer pays with mobile payments platforms. For example, the California legislature prohibited businesses from, "requiring information that merchants, banks or credit card companies do not require or need." While the existing statutes suggests that mobile payment technologies would be subject to existing payment privacy provisions, as it now stands it is not clear how mobile payment system providers themselves should protect consumer data.

   Policymakers should ensure that the introduction of new technologies to the marketplace does not circumvent hard-won existing consumer protections and that only the personal information necessary to complete transactions and prevent fraud is collected by business from consumers.

For regulators:

1. Regulators should clarify the role and liability mobile payment service providers - such as Google Wallet—hold towards consumers in regards to privacy and financial protection.

2. Regulators should prohibit the use of consumers' information collected for the purposes of completing financial transactions and fraud prevention for other purposes, especially marketing purposes.

3. Regulators should urge mobile payment service providers companies to employ necessary security measures in order protect consumer's sensitive financial information and other transaction data from loss or misuse.

For Business leaders:

1. Mobile payment service providers should voluntarily provide consumers with clear information regarding consumers' liability for fraudulent or unauthorized charges and provide them with a toll- free number to contest charges.

2. Mobile payment service providers should implement mandatory safeguards to protect consumers—such as PIN protection on the mobile payments apps and user-enabled daily spending limits.

3. Mobile payment service providers should adopt three principles in their practices:

   a) "Privacy by design," building into their products procedures that insure minimal data collection consistent with the context of a consumer's interaction with that company, consumer control over their data, transparency, and respect for privacy.

   b) Provide businesses and consumers with simple context-based privacy choices – giving them control over the data collected and how it is used. For example, mobile service providers should allow consumers to opt out from informa-

tion sharing during each transaction.2. This would provide consumers with increased control over their data and the power to choose when they find it appropriate to share their data.

c) Be fully transparent in communicating what data is collected from consumers, who it is shared with, and how it is used.

For Consumers:

Associate credit cards with mobile payment apps, since they provide the highest level of consumer protection.

1. Alternately, consider loading a pre-paid debit card with limited funds for small purchases onto the mobile payment app. While pre-paid debit cards provide a low level of consumer protection, the consumer can limit their balance and thus reduce their exposure to financial loss.

2. Enable password protection on your mobile device and specifically for all financial apps.

3. When problems occur (disputed charges, complaints, etc.), bring it to the attention of the card issuer as you would during a normal use of your credit or debit card.

4. When a device with a mobile payment app is lost or stolen, contact the mobile payment service provider (e.g. Google Wallet or ISIS) to disable the app to prevent unauthorized access. In addition, you should also contact the issuer of each of the payment cards loaded onto the mobile payment app as may be required by the respective banks' service terms and conditions.

5. To protect your privacy, be aware of what you are buying and how you pay for it. Remember mobile payments (like most non-cash transactions) are being tracked and monitored.

Glossary of terms

EFT: Electronic fund transfers

NFC: Near field communication

PIN: Personal identification number

POS: Point of sale terminals

SMS: Short messaging service

Appendix A:
Regulating Electronic Funds

The *Electronic Funds Transfer Act (1978)* and its *Regulation E* are the rules that govern electronic fund transfers (EFT). EFTs include transactions initiated by electronic means, including ATM transfers, debit card transactions, direct deposits and withdrawals, telephone-initiated transfers and online bill payments.[38]

Regulation E requires financial institutions to disclose up-front their terms and conditions for EFTs and limits consumers' liability for unauthorized EFTs up to $50 if they notify the financial institution within two days after learning of the unauthorized transfer or up to $500 if they notify the financial institution after two days, and up to all the money in that account and linked accounts if notification is made after 60 days.[39] When a consumer makes a mobile payment, the card-issuing bank must make the disclosures required by Regulation E and is liable for unauthorized transfers. The bank likely does not cease to be a "financial institution" under Regulation E simply because the customer linked her debit card to her phone. It is still a bank that directly holds the consumer's account and the bank that is ultimately responsible.[40]

However, as the law is written today, Regulation E specifically excludes transfers initiated through a telephone in its definition of an "electronic terminal."[41] While a smart-phone is clearly a phone, it is used today as a computer, something legislators did not take into account when the law was written.

Another relevant regulatory framework is the federal *Truth in Lending Act (1968)* and its *Regulation Z* which govern credit card transactions.[42] Regulation Z also contains provisions to resolve billing errors and limits consumers' liability for unauthorized transactions up to $50. Normally, the issuing bank is subject to Regulation Z because it issued credit to the consumer. As mobile payment systems become more common place, Regulation Z will continue to apply to cards linked to a mobile phone.

Title V of the *Gramm-Leach-Bliley Act* (1999) addresses the privacy of consumer data held by a financial institution.[43] The "Privacy Rule" of Title V requires that a financial institution disclose its privacy policies regarding disclosure of customer's non-public information with affiliates and non-affiliates at the time it establishes its relationship with a customer, and then again annually. A financial institution also must notify consumers of their right to opt out from sharing their information.

Endnotes

1 *Financial Execs Survey: Mobile Payments Going Mainstream by 2015*, Jason Ankeny, FierceMobileContent.com, July 13, 2011, available at http://www.fiercemobilecontent.com/story/financialexecs-survey-mobile-payments-going-mainstream-2015/2011-07-13.

2 *Mobile Commerce Forecast: 2011 To 2016*, Sucharita Mulpuru, 17 June, 2011.

3 *Nielsen: Smartphones Used By 50.4% Of U.S. Consumers, Android 48.5% Of Them*, Ingrid Lunden, Techcrunch, 7 May, 2012. Accessed online at: http://techcrunch.com/2012/05/07/nielsen-smartphones-used-by-50-4-of-u-s-consumers-android-48-5-of-them/

; And *ComScore Reports December 2012 U.S. Smartphone Subscriber Market Share*, 6 February 2013, 2013. Accessed online at: http://www.comscore.com/Insights/Press_Releases/2013/2/comScore_Reports_December_2012_U.S._Smartphone_Subscriber_Market_Share

4 *Mobile payment security concerns put brakes on m-commerce market*, Christopher Brown, 17 March 2011. Accessed online at: http://www.nfcworld.com/2011/03/17/36483/mobile-payment-security-concerns-put-brakes-on-m-commerce-market/

5 *Consumers and Mobile Financial Services*, Board of Governors of the Federal Reserve System, March 2012, available at http://www.federalreserve.gov/econresdata/mobile-device-report-201203.pdf.

6 To note, this report focuses on consumer facing mobile payment systems and not mobile payment processing systems such as "Square", "PayPal Here", or "Intuit GoPayment".

7 *Mobile Payments A study of the emerging payments ecosystem and its inhabitants while building a business case*, Cherian Abraham. Accessed online December 2012 at: http://ftc.gov/os/comments/mobilepayments/561018-00013-82732.pdf

8 A secure element often resides on the SIM card, in an embedded secure element (a dedicated chip on a phone's motherboard), or as an external accessory. Source: *Security of Proximity Mobile Payments*, Smart Card Alliance, May 2009.

9 *Mobile Payments A study of the emerging payments ecosystem and its inhabitants while building a business case*, Cherian Abraham. Accessed online December 2012 at: http://ftc.gov/os/comments/mobilepayments/561018-00013-82732.pdf

10 See Google Wallet FAQ available online at: http://www.google.com/wallet/faq.html

11 *Despite bold moves on mobile payments, long haul ahead*, Matt Hamblen, Computerworld, 19 November, 2010. Accessed online at: http://www.computerworld.com/s/article/9197228/Despite_bold_moves_on_mobile_payments_long_haul_ahead

12 See Appendix A. for a full discussion of the various regulations governing different payments methods.

13 *See* Regulation E § 205.20(a)(2) (effective Aug. 22, 2010) defining a "store gift card" as "a card, code, or other device that is: (i) Issued on a prepaid basis primarily for personal, family, or household purposes to a consumer in a specified amount, whether or not that amount may be increased or reloaded, in exchange for payment; and (ii) Redeemable upon presentation at a single merchant or an affiliated group of merchants for goods or services."

14 See 75 Fed. Reg. 16580, 16585 (April 1, 2010).

15 *See* 12 C.F.R. § 1026.12.

16 However, if consumers do not report unauthorized debit transactions on their bank account within 60 days after their periodic statement is mailed to them, they can face unlimited liability, whether or not the charges result from a lost or stolen card or another electronic transfer. *See* 12 C.F.R. § 1005.6.

17 See *Reply Comment of the Federal Trade Commission in Federal Communications Commission CG Docket No. 11-116 (July 20, 2012), at 5-7 ("FTC Reply Comment")*, available online at: http://www.ftc.gov/os/2012/07/120723cramming comment.pdf.

18 See Google, *"Purchasing Android apps via Carrier Billing,"* available online at*:* http://support.google.com/googleplay/bin/answer.py?hl=en&answer=167794&topic=1046718&ctx=topic

19 This is left up to the discretion of the wireless service provider as stated in the terms of contract. See *Paper, Plastic... or Mobile?: An FTC Workshop on Mobile Payments,* Federal Trade Commission, March 2013, pp.8.

20 FTC staff's research of 19 current U.S. mobile payment providers revealed that three of the seven companies that allowed funding from stored value cards voluntarily provided additional protection that limited their customers' liability for fraudulent or unauthorized charges to $50.31. See *Paper, Plastic... or Mobile?: An FTC Workshop on Mobile Payments,* Federal Trade Commission, March 2013, pp.8.

21 *Mobile payment security concerns put brakes on m-commerce market*, Christopher Brown, 17 March 2011. Accessed online at: http://www.nfcworld.com/2011/03/17/36483/mobile-payment-security-concerns-put-brakes-on-m-commerce-market/

22 See Board of Governors of the Federal Reserve System, *Consumers and Mobile Financial Services*, (Mar. 2012), available at http://www.federalreserve.gov/econresdata/mobile-device-report-201203.pdf.

23 Congressional Testimony of Randy Vanderhoof, Executive Director, Smart Card Alliance, before the U.S. House Committee on Financial Services, Subcommittee on Financial Institutions and Consumer Credit on *The Future of Money: How Mobile Payments Could Change Financial Services*, 22 March, 2012.

24 *Mobile Payments: Consumer Benefits & New Privacy Concerns,* Chris Jay Hoofnagle, Jennifer M. Urban, Su Li, BCLT Research Paper, 24 April, 2012.

25 *Mobile Payments: Consumer Benefits & New Privacy Concerns*, Chris Jay Hoofnagle, Jennifer M. Urban, Su Li, BCLT Research Paper, 24 April, 2012.

26 *Mobile Payments: Consumer Benefits & New Privacy Concerns*, Chris Jay Hoofnagle, Jennifer M. Urban, Su Li, BCLT Research Paper, 24 April, 2012.

27 CALPIRG Education Fund sent both ISIS and Google a letter requesting further information regarding their consumer privacy polices in April 2013. As of June 2013, we received no response.

28 *Mobile Payments: Consumer Benefits & New Privacy Concerns*, Chris Jay Hoofnagle, Jennifer M. Urban, Su Li, BCLT Research Paper, 24 April, 2012.

29 Card Fees Pit Retailers Against Banks, Andrew Martin, New York Times, 16 July, 2009.

30 To illustrate the size of this cost, interchange fees represent the second highest expense (after payroll) at Target stores.

31 Most anti-marketing laws have "established business relationship" exceptions, allowing the merchant to call a customer. See the *Telephone Consumer Protection Act* & Code of Federal Regulations - Title 16 § 310.2(n).

32 *Mobile Payments: Consumer Benefits & New Privacy Concerns*, Chris Jay Hoofnagle, Jennifer M. Urban, Su Li, BCLT Research Paper, 24 April, 2012.

33 Mobile Payments: Consumer Benefits & New Privacy Concerns, Chris Jay Hoofnagle, Jennifer M. Urban, Su Li, BCLT Research Paper, 24 April, 2012.

34 *The Panoptic Sort: A Political Economy of Personal Information*, Oscar H. Gandy, Jr., Critical Studies in Communication & in the Cultural Industries, Westview, 1993.

35 *Mobile Payments A study of the emerging payments ecosystem and its inhabitants while building a business case*, Cherian Abraham. Accessed online December 2012 at: http://ftc.gov/os/comments/mobilepayments/561018-00013-82732.pdf; and *Mobile Payments: Consumer Benefits & New Privacy Concerns*, Chris Jay Hoofnagle, Jennifer M. Urban,Su Li, BCLT Research Paper, 24 April, 2012.

36 *Mobile Payments A study of the emerging payments ecosystem and its inhabitants while building a business case*, Cherian Abraham. Accessed online December 2012 at: http://ftc.gov/os/comments/mobilepayments/561018-00013-82732.pdf

37 *Mobile Payments A study of the emerging payments ecosystem and its inhabitants while building a business case*, Cherian Abraham. Accessed online December 2012 at: http://ftc.gov/os/comments/mobilepayments/561018-00013-82732.pdf

38 *An Overview of Mobile Payments and Their Regulation*, accessed online December 2012 at: http://www.pepperlaw.com/publications_article.aspx?ArticleKey=1813

39 *An Overview of Mobile Payments and Their Regulation*, accessed online December 2012 at: http://www.pepperlaw.com/publications_article.aspx?ArticleKey=1813

40 *An Overview of Mobile Payments and Their Regulation*, accessed online December 2012 at: http://www.pepperlaw.com/publications_article.aspx?ArticleKey=1813

41 Electronic Funds Transfer Act and Regulation E. § 205.2(h).

42 Available online at: http://www.fdic.gov/regulations/laws/rules/6500-1400.html

43 Available online at: http://www.ftc.gov/privacy/glbact/glboutline.htm