

ARTICLES

ECONOMICS

▶ The Net Effects of the Proposed Durbin Fee Reductions on Consumers and Small Businesses

RISK AND SECURITY

▶ Managing the Risks and Security Threats of Mobile Payments

BUSINESS

▶ Processors: Connecting the Dots for Payments Growth?

LAW AND REGULATION

▶ Response: U.S. v American Express, et al. – Making Everything Out of Something

DEVELOPING COUNTRIES

▶ Electronic Payments in India: Looking Back and Surging Forward

▶ [Comment on the Articles on PYMNTS.com](#)

AUTHORS

James Contardi

David S. Evans

Bill Gajda

Tracey Kitzman

Robert Litan

Upendra Namburi

Richard Schmalensee



Managing the Risks and Security Threats of Mobile Payments

by Bill Gajda (Head of Global Mobile Product at Visa Inc.)
February 2011



RISK AND SECURITY

Introduction

Over the past decade, mobile phones have emerged as one of the most ubiquitous technologies in human history. Today, billions of people in virtually every corner of the world have mobile phones. These devices shape their interaction with their communities, countries and economies.

At the same time, the consumer financial services industry has spread the benefits of electronic payments across the planet. By linking financial institutions, cardholders and millions of merchants around the world, global payment networks are facilitating commerce in ways and in places previously unimagined.

Given the parallel spread of these technologies, it has long been assumed that convergence would inevitably occur. Indeed, much evidence has pointed in this direction. Yet, as this new frontier of personal empowerment and commercial facilitation takes hold, there remains a great deal of uncertainty about how these mobile payment systems will operate. The most important question is how they will be made secure.

Mobile Payments

In order to understand where mobile payments are headed and the security challenges that should be addressed, we must first define what we mean by "mobile payment." At the most basic level, we can separate mobile payments into 1) Mobile as Payment Devices to initiate payments by a consumer; and 2) Mobile as Acceptance Devices to accept payments by a merchant.

Mobile as Payment Devices

The use of a mobile phone to initiate payment mirrors what we are familiar with today. The fundamental difference is that instead of payment with a card, mobile payments use a mobile phone. Mobile payments at the physical point-of-sale (POS) and in the eCommerce environment are defined by the industry as "proximity payments" and "remote payments," respectively.

Proximity payments are remarkably intuitive and similar to today's payment methods. Instead of using a card to make a payment, the consumer uses their mobile phone. There are many different technologies that can be proposed for proximity payments. Yet contactless technology, referred to as NFC (Near Field Communication), is emerging as the de facto technology standard. The great benefit to NFC is that it is backwards compatible with existing payment and transit card contactless standards, and much of the infrastructure is already deployed around the world. A short-range radio signal is transmitted between the phone and terminal, initiating the payment and allowing it to be processed through the traditional card processing networks and systems.

ARTICLES

ECONOMICS

▶ The Net Effects of the Proposed Durbin Fee Reductions on Consumers and Small Businesses

RISK AND SECURITY

▶ Managing the Risks and Security Threats of Mobile Payments

BUSINESS

▶ Processors: Connecting the Dots for Payments Growth?

LAW AND REGULATION

▶ Response: U.S. v American Express, et al. – Making Everything Out of Something

DEVELOPING COUNTRIES

▶ Electronic Payments in India: Looking Back and Surging Forward

▶ **Comment on the Articles on PYMNTS.com**

AUTHORS

James Contardi

David S. Evans

Bill Gajda

Tracey Kitzman

Robert Litan

Upendra Namburi

Richard Schmalensee



Unlike proximity payments, remote payments do not require the consumer to be in the store or even in the same country as the merchant. Instead, remote payments bring the convenience of online shopping to a person's mobile device.

Some of the most common types of remote payments include:

- Message-based: when a consumer sends a text message or code and a premium is charged to the consumer's phone bill;
- Browser-based: similar to a computer-based eCommerce experience – the consumer completes a Web form; and
- App-based: when the consumer uses a vendor-sponsored application to find and purchase good or services.

Mobile as Acceptance Device

In addition to replacing cards for payments, mobile phones are also beginning to be used as portable POS devices. In the world of smartphone applications, software is emerging to allow small merchants or individuals to subscribe to payment services where they accept card payments via key-entered card data on their mobile phone. Mobile phone accessories are also emerging that add a magnetic stripe or chip reader to a mobile phone, so that card data can be entered electronically as with a traditional POS device. Mobile acceptance opens the way to a future where acceptance is "everywhere you want acceptance to be."

Today, we are seeing mobile acceptance expanding everywhere, from gardeners to pizza delivery parlors, bringing the mobility and convenience of electronic payments to merchant segments that were traditionally reliant on cash and checks.

At the same time, the use of mobile phones as payment and acceptance devices will also open up new opportunities and channels, such as person-to-person (P2P) money transfer, where a

SPONSORED ADVERTISEMENT

FINOVATE SPRING
SAN FRANCISCO • MAY 10 & 11 2011

ARTICLES

ECONOMICS

▶ The Net Effects of the Proposed Durbin Fee Reductions on Consumers and Small Businesses

RISK AND SECURITY

▶ Managing the Risks and Security Threats of Mobile Payments

BUSINESS

▶ Processors: Connecting the Dots for Payments Growth?

LAW AND REGULATION

▶ Response: U.S. v American Express, et al. – Making Everything Out of Something

DEVELOPING COUNTRIES

▶ Electronic Payments in India: Looking Back and Surging Forward

▶ **Comment on the Articles on PYMNTS.com**

AUTHORS

James Contardi

David S. Evans

Bill Gajda

Tracey Kitzman

Robert Litan

Upendra Namburi

Richard Schmalensee



mobile phone can be used to initiate or accept transfers between individuals.

Mobile Payments Benefits

Mobile payment synthesizes the technology of mobile phones with the demands of consumers and marketing needs of merchants. Understanding the basics of mobile payments, we can now turn our attention to why mobile payments matter: the enormous benefits this technology holds for consumers and merchants, alike.

Consumer Benefits

The convergence of mobile technology and electronic payments holds the promise of an enhanced shopping experience followed by unprecedented convenience and control of payment options.

The mobile phone, with its connectivity to the Internet, allows the consumer to research purchases and compare prices. Furthermore, consumers can share favorite products with friends via social media. Merchants also can deliver promotional opportunities, including digital coupons.

Once ready to purchase, the consumer has the option of conducting a transaction at the physical store with proximity contactless or at an online merchant via remote payments. Newer phones have been announced that will include contactless NFC technology, which can mean less hassle in the checkout line, greater control of financial information and the convenience of having payment card and mobile phone consolidated into a single tool.

If the consumer decides to purchase the goods with an online retailer instead, the mobile device can also be used to facilitate that transaction in a variety of ways. One example is online wallets, which are frequent in eCommerce and emerging in mobile. Consumers store their payment card information in an easily accessible online location, which is then used for simple,

“ **The convergence of mobile technology and electronic payments holds the promise of an enhanced shopping experience...** ”

one-click style payments. In addition, shoppers can conduct transactions wherever they take their mobile devices, rather than firing up a computer at home to experience the convenience of online shopping.

The mobile device can further facilitate post transaction convenience of having the receipts



ARTICLES

ECONOMICS

▶ The Net Effects of the Proposed Durbin Fee Reductions on Consumers and Small Businesses

RISK AND SECURITY

▶ Managing the Risks and Security Threats of Mobile Payments

BUSINESS

▶ Processors: Connecting the Dots for Payments Growth?

LAW AND REGULATION

▶ Response: U.S. v American Express, et al. – Making Everything Out of Something

DEVELOPING COUNTRIES

▶ Electronic Payments in India: Looking Back and Surging Forward

▶ **Comment on the Articles on PYMNTS.com**

AUTHORS

James Contardi

David S. Evans

Bill Gajda

Tracey Kitzman

Robert Litan

Upendra Namburi

Richard Schmalensee



stored securely on the mobile device for tracking and customer service purposes, making paper slips tucked in a wallet obsolete.

Opportunities for Merchants

Merchants are also poised to unlock enormous value, as these tools become more secure and ever-present. Mobile payments allow merchants to reach their customers through multiple touch points simultaneously. For example, an electronic coupon delivered to a phone can be shared via social networking and used instantly or integrated directly into the digital wallet to be used in the next purchase. The ability to determine the location of a consumer through geo-location functions adds another dimension to integrated marketing. Done securely and with the right privacy protections in place, this can make marketing much more efficient and targeted, reaching consumers where they are most likely to be receptive.

The overall value is also tremendous. In 2005, the British marketing research firm Juniper Research predicted that total transactions via mobile devices would be \$155 million that year and top \$10 billion by the end of the decade. Not only did mobile payments exceed that forecast tenfold, reaching \$100 billion in 2010, but the total for digital and physical goods are expected to reach \$630 billion by 2014.

The future of mobile payments is robust. Consumers are poised to realize enormous benefits, and merchants to gain unrivalled opportunity. But in order for any of this promise to be fulfilled, the fundamental issue of security will need to be vigilantly addressed.

Security of Mobile Payments

Whenever a new payment technology is introduced, new challenges are sure to emerge as well. Fortunately, most of the security concerns associated with mobile payments are either identical or very similar to ones already faced and addressed by the payment industry. As has been the case in the past, addressing those threats must be the shared responsibility of all stakeholders.

The most apparent safety concern is protecting personal data that either is stored in or flows through a mobile device – payment account numbers, PINs, security codes, passwords, etc. Exposure of personal information over a wireless network can leave the consumer feeling vulnerable to theft. As a result, mobile payments have a higher hill to climb to assuage consumer concerns about security and privacy.

Some of these challenges to mobile payments are highlighted below:

Proximity Payments

Proximity payments are based on the EMV standard and therefore face the fewest security challenges. Use of an EMV-approved chip ensures that a mobile proximity payment delivers the same end-to-end security offered by a smartcard-enabled payment. Maintaining the same security between the card and mobile worlds for this type of transaction delivers tremendous benefits to the entire payments ecosystem. Other types of proximity payments that rely on barcodes or other new means of payment security and authentication represent entirely new security and risk models that will face a significant challenge in delivering a secure, efficient

ARTICLES

ECONOMICS

▶ The Net Effects of the Proposed Durbin Fee Reductions on Consumers and Small Businesses

RISK AND SECURITY

▶ Managing the Risks and Security Threats of Mobile Payments

BUSINESS

▶ Processors: Connecting the Dots for Payments Growth?

LAW AND REGULATION

▶ Response: U.S. v American Express, et al. – Making Everything Out of Something

DEVELOPING COUNTRIES

▶ Electronic Payments in India: Looking Back and Surging Forward

▶ **Comment on the Articles on PYMNTS.com**

AUTHORS

James Contardi

David S. Evans

Bill Gajda

Tracey Kitzman

Robert Litan

Upendra Namburi

Richard Schmalensee



and cost-effective solution.

The main challenge for proximity contactless payment is standardization and integration. Today, hundreds of new mobile devices hit the market every year, each offering innovative options and ways to communicate and access payment information stored on the chip. Lack of technology standards in the industry can lead to attacks, particularly if manufacturers of the mobile device, mobile networks that sell and enable these mobile phones and issuers that issue the payment chip used on these devices do not work together. Actors across the industry must implement defensive measures to secure the entire value chain and ensure the proper implementation of the mobile proximity payment ecosystem.

Remote Payments

Like our personal computers, remote payments typically rely on software-based security that is susceptible to many threats due to the openness of the mobile platforms. The mobile phone today has the ability to execute all types of applications, ranging from instant messaging and social media to games and even online banking and trading.

That ability to execute applications, unfortunately, extends to viruses and malware as well. While we do not see as many viruses and malware targeting mobile platforms today, we expect that to change once there is increased adoption and penetration of mobile payments by consumers.

In fact, there are already companies developing and selling antivirus software for smartphones today. A recent [article](#) published by Dow Jones Newswires noted that “[a]nti-virus companies with strong sales in the PC universe, like AVG or rival Trend Micro., are moving to fill that potentially lucrative niche, with a focus on protecting sensitive financial data – the No.1 target for developers of malicious software.”

In reality, there are few differences when you compare a PC and a mobile phone-based eCommerce transaction. The key differences and challenges are:

SPONSORED ADVERTISEMENT

MERCHANT RISK COUNCIL 10
CELEBRATING 10 YEARS OF INDUSTRY COLLABORATION

ARTICLES

ECONOMICS

▶ The Net Effects of the Proposed Durbin Fee Reductions on Consumers and Small Businesses

RISK AND SECURITY

▶ Managing the Risks and Security Threats of Mobile Payments

BUSINESS

▶ Processors: Connecting the Dots for Payments Growth?

LAW AND REGULATION

▶ Response: U.S. v American Express, et al. – Making Everything Out of Something

DEVELOPING COUNTRIES

▶ Electronic Payments in India: Looking Back and Surging Forward

▶ **Comment on the Articles on PYMNTS.com**

AUTHORS

James Contardi

David S. Evans

Bill Gajda

Tracey Kitzman

Robert Litan

Upendra Namburi

Richard Schmalensee



- **Software:** The world of PC-based eCommerce is based almost entirely on standardized Web software on Microsoft Windows, MacOS or Linux operating systems. The same cannot be said about mobile, since the platforms are still evolving rapidly with frequent changes to the operating systems and a wide variety of underlying hardware architectures.

- **Internet connection:** Where the risk in the PC world is limited to the amount of time the computer is switched on and connected to the Internet, with smartphones, that window of exposure is now greatly increased, as the phone is a device we typically keep switched on even while we sleep.

- **Scams:** Comparable to the e-mail phishing attacks that trick victims into divulging personal information via a computer, scammers can easily extend these tactics to the mobile channel. In fact, since the mobile device can also communicate via voice, text or data, fraudsters suddenly find they have even more avenues to conduct attacks. We are starting to see such PC-style attacks make their way into smishing (SMS text phishing) and vishing (voice phishing).

Without a doubt, there are major issues that must be addressed to ensure the safety of mobile payments. Leaders in the industry, who understand the potential value for merchants and customers, have already taken several steps to remedy these concerns. The good news is that we are not starting from zero:

- The payments industry requires all entities that process, transmit or store payment information adhere to the Payment Card Industry Data Security Standards (PCI DSS). Furthermore, the Payment Application Data Security Standards (PA-DSS) applies to software applications used to accept payment data. The fundamental principles behind these standards would be equally applicable to the mobile space. In fact, there might even be opportunities to further enhance these standards to incorporate new

“ **We are starting to see such PC-style attacks make their way into smishing (SMS text phishing) and vishing (voice phishing).** ”

capabilities brought about by the mobility and connectivity of mobile devices. This is something that Visa is actively working on today.

- As we have defined earlier in the article, mobile payments might be a new channel, but the risk and risk management activities associated with the channel is very similar



ARTICLES

ECONOMICS

▶ The Net Effects of the Proposed Durbin Fee Reductions on Consumers and Small Businesses

RISK AND SECURITY

▶ Managing the Risks and Security Threats of Mobile Payments

BUSINESS

▶ Processors: Connecting the Dots for Payments Growth?

LAW AND REGULATION

▶ Response: U.S. v American Express, et al. – Making Everything Out of Something

DEVELOPING COUNTRIES

▶ Electronic Payments in India: Looking Back and Surging Forward

▶ **Comment on the Articles on PYMNTS.com**

AUTHORS

James Contardi

David S. Evans

Bill Gajda

Tracey Kitzman

Robert Litan

Upendra Namburi

Richard Schmalensee



to that of contactless transactions (proximity payments) and eCommerce transactions (remote payments). Almost all existing fraud mitigation processes and tools we have to keep fraud at an all-time low (less than 6 cents for every \$100) will apply to the mobile channel as well. In fact, with new information offered by the mobile devices (e.g., location information), there is an opportunity to further enhance some of these risk tools to incorporate these new information streams. For example, if the mobile transaction was conducted in Los Angeles while the mobile network tells us that the phone is located in Boston, it creates an immediate red flag.

- Proximity payments are based on the same protocol and technology used in contactless cards today. These contactless transactions introduce a dynamic authentication element for each transaction. As a result, even if the transaction data were compromised, it cannot be reused to successfully conduct a fraudulent transaction at the point of sale without detection. In fact, the use of a mobile device further strengthens the security of this transaction type. The consumer has full control over when to enable the NFC interface for the transaction, leaving it largely disabled when the user is not using it for payments.

Next Steps

Across the industry, from consumers and financial institutions to mobile network operators and payment brands, significant yet achievable steps are necessary to ensure mobile payments are safe. Additionally, while the industry constantly updates security measures, it is important that merchants and service providers keep their consumers up to date. Staying ahead of possible attacks will be critical in safeguarding personal information.

Fortunately, from a risk management perspective, the industry is well-positioned to bring mobile payments to market safely.

Consumers

Consumer education and awareness will be a critical element to secure mobile payments. With new payment capability, mobile phones will carry more value than the cost of the phone itself and will need to be treated with extra caution. Put simply, consumers will need to start treating their mobile phone with the same zealous protection as they do their wallets. Examples of consumer tips include:

- Use some form of password or passcode to access the payment application on the phone.
- Never share confidential or private information, especially if you did not initiate the communication. If you are in doubt, call your issuer.
- Ensure that any text messages you receive from your financial institution originated from the correct phone number or short code.
- Only download mobile applications from trusted sources.
- Report to the financial institution immediately if your phone containing your financial

ARTICLES

ECONOMICS

▶ The Net Effects of the Proposed Durbin Fee Reductions on Consumers and Small Businesses

RISK AND SECURITY

▶ Managing the Risks and Security Threats of Mobile Payments

BUSINESS

▶ Processors: Connecting the Dots for Payments Growth?

LAW AND REGULATION

▶ Response: U.S. v American Express, et al. – Making Everything Out of Something

DEVELOPING COUNTRIES

▶ Electronic Payments in India: Looking Back and Surging Forward

▶ **Comment on the Articles on PYMNTS.com**

AUTHORS

James Contardi

David S. Evans

Bill Gajda

Tracey Kitzman

Robert Litan

Upendra Namburi

Richard Schmalensee



information is lost or stolen.

Payment Brands

The payment brands play a critical role in the development of this emerging channel by understanding the underlying risk structure of payments, and in fact, already having the processes and countermeasures in place to address a large number of potential threats. At the same time, the brands should continue to promote the adoption and development of mobile payment by ensuring that risk management practices are extended to the channel. Specifically, they should:

- Ensure that payment-related security standards are reviewed and revised so that they stay relevant and applicable to the mobile channel.
- Continue to build partnerships and bridge the relationship between the financial institutions and the mobile network operators in introducing secure payment solutions to the industry.
- Continue to update and track the certification of third-party applications and devices.

Mobile Network Operators

Mobile network operators also have an important role to play. Today, the first point of interaction for consumers in this new channel is typically the mobile service provider. Hence, that provides a perfect opportunity for operators to:

- Include mobile security software (e.g., mobile antivirus) as part of the default suite of applications loaded onto new mobile devices.
- Ensure that mobile phones used in proximity payments are certified and meet the requirements of the payment brands.

SPONSORED ADVERTISEMENT



NAPCP COMMERCIAL
Card and Payment Conference

EDUCATION • NETWORKING • EXPO

12th Annual • Las Vegas • April 11-14, 2011

National Association of Purchasing Card Professionals

ARTICLES

ECONOMICS

▶ The Net Effects of the Proposed Durbin Fee Reductions on Consumers and Small Businesses

RISK AND SECURITY

▶ Managing the Risks and Security Threats of Mobile Payments

BUSINESS

▶ Processors: Connecting the Dots for Payments Growth?

LAW AND REGULATION

▶ Response: U.S. v American Express, et al. – Making Everything Out of Something

DEVELOPING COUNTRIES

▶ Electronic Payments in India: Looking Back and Surging Forward

▶ **Comment on the Articles on PYMNTS.com**

AUTHORS

James Contardi

David S. Evans

Bill Gajda

Tracey Kitzman

Robert Litan

Upendra Namburi

Richard Schmalensee



- Provide general consumer education on mobile security.

Financial Institutions

Financial institutions will be instrumental in the security process, particularly in terms of fraud detection and prevention. To ensure the safety of their customers, financial institutions will need to:

- Adapt existing security methods, fraud prevention alerts and the tracking of spending trends to react to potential mobile-based fraud.
- Review existing back-office processes in support of the emerging mobile channel.
- Ensure that software applications are certified and meet the requirements of the payment brands.

Vendors in the Mobile Payment Space

Vendors represent the frontline in defending against potential threats to consumers. To both ensure they are authorized by the industry and trusted by potential consumers, vendors will need to:

- Ensure that all relevant requirements in PCI DSS and the PCI PA-DSS are met, including the installation of EMV-compliant POS systems.
- Encrypt sensitive data without relying on mobile protocols, such as GSM and CDMA. Instead, the mobile application should provide end-to-end encryption as part of the product functionality.
- Control and limit the distribution channel to trusted sources where consumers can easily differentiate its authenticity.

Taken together, these coordinated actions that bring together phone manufacturers, mobile network operators, mobile application developers, payments networks, issuers, acquirers and merchants are making considerable progress. Working cooperatively and sharing responsibility for the ultimate security of the system is opening the door to a vastly expanded future for mobile payments.