An ISACA
Emerging Technology
White Paper
November 2011

ISACA®
Trust in, and value from, information systems

Mobile Payments: Risk, Security and Assurance Issues

Abstract
Mobile payments as a financial transaction medium emerged around a decade ago. Adoption was slow due to the nature of the mobile technology supporting the concept. However, recent significant advances on the technology front have made this area one of burgeoning growth in the financial services sector. Services-based and text-based payment and proximity device communications are appearing worldwide. Widespread use of smartphones and consumer comfort with mobile devices for more than communication are the principal drivers of a resurgent and increased interest in mobile payments. In addition, advances in software and hardware security techniques have made trusted financial transactions possible from these devices. This white paper examines the current state and nature of the mobile payments market, some of the relevant enabling technologies, and looks at the relevant risk, security and assurance issues that security and audit professionals will want to consider when developing and evaluating mobile payment services.

ISACA®

With 95,000 constituents in 160 countries, ISACA (*www.isaca.org*) is a leading global provider of knowledge, certifications, community, advocacy and education on information systems (IS) assurance and security, enterprise governance and management of IT, and IT-related risk and compliance. Founded in 1969, the nonprofit, independent ISACA hosts international conferences, publishes the *ISACA® Journal*, and develops international IS auditing and control standards, which help its constituents ensure trust in, and value from, information systems. It also advances and attests IT skills and knowledge through the globally respected Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) and Certified in Risk and Information Systems Control™ (CRISC™) designations. ISACA continually updates COBIT®, which helps IT professionals and enterprise leaders fulfill their IT governance and management responsibilities, particularly in the areas of assurance, security, risk and control, and deliver value to the business.

Disclaimer

ISACA has designed and created *Mobile Payments: Risk, Security and Assurance Issues* (the "Work") primarily as an educational resource for governance, security and assurance professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, governance and assurance professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

Reservation of Rights

ISACA

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
E-mail: *info@isaca.org*
Web site: *www.isaca.org*

Mobile Payments: Risk, Security and Assurance Issues

Acknowledgments

ISACA wishes to recognize:

Project Development Team
Nikolaos Zacharopoulos, CISA, CISSP, Geniki Bank, Greece, Chair
Milthon Chavez, Ph.D., CISA, CISM, CGEIT, CRISC, ISO27000LA, CIFI, MCH Consultoria Integral/C.I.R.O., USA
Mohamad Hammoud, Path Solutions, Kuwait
Cristian Pigulea, CISA, Endava Romania SRL, Romania
Dionysios Travlos, CISA, Greece
Peter Van Mol, CISA, Atos Worldlinenv, Belgium
GautamVora, CISA, TDK Corporation, USA
Mahmoud Yassin, CISA, CRISC, CISSP, ITIL, PMP, National Bank of Abu Dhabi (NBAD), UAE

Expert Reviewers
Prashantsinh V. Jethwa, CISSP, CBCI, RBS Group, England
Fundile Ntuli, MCSSA, Ubank, South Africa
Hari Ramamurthy, CISA, CGEIT, ACA, Leading System Consultants Inc., Canada

ISACA Board of Directors
Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retired), USA, International President
Christos K. Dimitriadis, Ph.D., CISA, CISM, CRISC, INTRALOT S.A., Greece, Vice President
Gregory T. Grocholski, CISA, The Dow Chemical Co., USA, Vice President
Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, Vice President
Niraj Kapasi, CISA, Kapasi Bangad Tech Consulting Pvt. Ltd., India, Vice President
Jeff Spivey, CRISC, CPP, PSP, Security Risk Management, USA, Vice President
Jo Stewart-Rattray, CISA, CISM, CGEIT, CRISC, CSEPS, RSM Bird Cameron, Australia, Vice President
Emil D'Angelo, CISA, CISM, Bank of Tokyo-Mitsubishi UFJ Ltd. (retired), USA, Past International President
Lynn C. Lawton, CISA, CRISC, FBCS CITP, FCA, FIIA, KPMG Ltd., Russian Federation, Past International President
Allan Neville Boardman, CISA, CISM, CGEIT, CRISC, CA (SA), CISSP, Morgan Stanley, UK, Director
Marc Vael, Ph.D., CISA, CISM, CGEIT, CISSP, Valuendo, Belgium, Director

Knowledge Board
Marc Vael, Ph.D., CISA, CISM, CGEIT, CISSP, Valuendo, Belgium, Chairman
Michael A. Berardi Jr., CISA, CGEIT, Nestle USA, USA
John Ho Chi, CISA, CISM, CRISC, CBCP, CFE, Ernst & Young LLP, Singapore
Phillip J. Lageschulte, CGEIT, CPA, KPMG LLP, USA
Jon Singleton, CISA, FCA, Auditor General of Manitoba (retired), Canada
Patrick Stachtchenko, CISA, CGEIT, Stachtchenko & Associates SAS, France

Guidance and Practices Committee
Phillip J. Lageschulte, CGEIT, CPA, KPMG LLP, USA, Chairman
Ramses Gallego, CISM, CGEIT, CCSK, CISSP, SCPM, 6 Sigma, Quest Software, Spain
Meenu Gupta, CISA, CISM, CBP, CIPP, CISSP, Mittal Technologies, USA
Yongdeok Kim, CISA, IBM Korea Inc., Korea
Perry Menezes, CISM, CRISC, Deutsche Bank, USA
Mario Micallef, CGEIT, CPAA, FIA, Advisory in GRC, Malta
Salomon Rico, CISA, CISM, CGEIT, Deloitte, Mexico
Nikolaos Zacharopoulos, CISA, CISSP, Geniki Bank, Greece

Acknowledgments *(cont.)*

ISACA and IT Governance Institute® (ITGI®) Affiliates and Sponsors
American Institute of Certified Public Accountants
ASIS International
The Center for Internet Security
Commonwealth Association for Corporate Governance Inc.
FIDA Inform
Information Security Forum
Information Systems Security Association (ISSA)
Institute of Management Accountants Inc.
ISACA chapters
ITGI France
ITGI Japan
Norwich University
Solvay Brussels School of Economics and Management
Strategic Technology Management Institute (STMI) of the National University of Singapore
University of Antwerp Management School
ASI System Integration
Hewlett-Packard
IBM
SOAProjects Inc.
Symantec Corp.
TruArx Inc.

Introduction: What Are Mobile Payments?

Mobile devices have changed business and everyday life in the field of communication and now possibly the way financial transactions of all types are made. Mobile devices—in particular, mobile phones—are in wide use and consumers are becoming increasingly familiar with using mobile phones for various purposes such as "secure" financial transactions via a web banking site.[1] A newer opportunity is emerging for service providers and merchants—the use of a mobile phone as a mobile wallet. Considering the success of mobile content services such as ringtones, games and other applications, it is becoming apparent that consumers are willing to utilize mobile phones for payment purposes. Mobile phones are also providing an unprecedented opportunity for expansion of financial activity in developing countries where the number of phone users can exceed the number of those having bank accounts.

Definition and Distinguishing Characteristics

Mobile payment is defined as:

> *Payment for products or services between two parties for which a mobile device, such as a mobile phone, plays a key role in the realization of the payment.*

Mobile payment is defined as: Payment for products or services between two parties for which a mobile device, such as a mobile phone, plays a key role in the realization of the payment

Mobile payments center on transactions between consumers and merchants that involve direct purchase of goods and services that can be both account-based and point-of-sale (POS).

Mobile payments can be categorized based on the technology used as either one of two types—proximity or remote. These types drive the nature of the payment service model, the value proposition for both the consumer and merchant, and the relevant technologies and infrastructure considerations required to realize the type of mobile payment. **Figure 1** provides an overview of these two payment types.

Figure 1—Types of Mobile Payments

Type	Technology Involved	Worldwide Adoption
Proximity Payment Proximity payment generally refers to contactless payments in which the payment credential is stored in the mobile device and is exchanged over the air, based on NFC technology, with a dedicated and compatible payment terminal. In other words, the mobile device acts as a contactless payment card, thus becoming a new payment form factor. Contactless payment also could be used remotely; for example, to make an online purchase by swiping the mobile device over a contactless NFC reader plugged into a personal computer (PC).	The mobile phone is used by the consumer at the storefront to pay for goods or services via a contactless reader or via text-based or personal-identification-number-based (PIN-based) methods using Near Field Communication (NFC) technology[2] involving communication between the consumer's device, the payment scheme operator, and the retail merchant at the storefront. All NFC-compatible mobile devices can send as well as receive data so NFC phones can also act as card readers. It is a technology highly aligned with the use of trusted computing media such as subscriber identity module (SIM) cards and Trusted Platform Modules (TPM).	NFC-based systems are either being used or examined in regions such as Western Europe, the United States, Canada and Japan. They are also gaining acceptance in developing countries, particularly in the form of contactless card transactions. Installations of this type are: ExpressPay™ from American Express, Discover® Network Zip℠, MasterCard® PayPass™, and Visa® payWave™ and Speedpass™. In July 2011 PayPal™ introduced a new payment model using NFC. It is a variant on the eWallet® model in which PayPal acts as a transparent intermediary for payment person-to-person (P2P) allowing Android™ users to pay one another by tapping two NFC-enabled devices together.

[1] Mobile banking involves using mobile devices, primarily smartphones, to gain access to traditional banking and financial services, principally banking and investing. It is transaction-oriented and focuses on transactions between banks and their customers. A mobile device is used as a communication instrument rather than as a payment instrument; e.g., for accessing web banking services via a smartphone browser application.

[2] NFC is a radio standard used to transfer data over distances up to 10 centimeters (3.9 inches).

Figure 1—Types of Mobile Payments *(cont.)*		
Type	**Technology Involved**	**Worldwide Adoption**
Remote Payment Remote payment covers payments that take place either via a mobile web browser or a resident smartphone application, in which the mobile phone is used as a device to authenticate personal information stored remotely. Remote payment solutions also can be used for transactions such as face-to-face and vending machine transactions.	The mobile phone is used by the consumer in combination with the network messaging service such as Short Message Service (SMS)[3] or Unstructured Supplementary Service Data (USSD)[4] to pay for services or digital content. The messages themselves can either be used to initiate or authorize payment or in some situations act as a unit of currency or exchange. For low-value transactions such as purchases of ringtones or when mobile content authentication solutions based on the mobile subscriber identification number (MSIDN) are used, billing is via the user's phone bill. Higher-value transactions can be processed using a variety of technical approaches such as: • Credit/debit card-based payment by entering user information via a secure Wireless Application Protocol (WAP) interface • eWallet/stored-value account-based payment via a secure WAP interface. In this case, user card and bank account information are stored securely on the user's mobile device. PIN-based authentication is used in conjunction with transport over interactive voice response (IVR), WAP, SMS and USSD channels. • Secure activation of the customer by the service provider and trusted enabling of the link between the MSIDN and the card number are essential.	SMS and USSD systems are finding wide application in Africa and in parts of the Middle East where there is a high mobile device concentration, large migrant communities and low banking service penetration. These message services are being used for applications such as payments to merchants, remittances across national boundaries, and salary payments for migrant workers. A widespread application of this type of mobile payment is the use of the premium SMS rate for the purchase of ringtones, games and other goods. Until now, this kind of payment usually was used for small amounts (micropayments).

At present, stakeholders have not clearly separated roles within the mobile payment ecosystem. Financial institutions and mobile network operators (MNOs) are competing for the entity that will hold the customer account and receive the biggest portion of fees. This unclear environment has created another kind of categorization based on the entity that holds the account of the customer—bank-centric and nonbank-centric.

In the bank-centric model, the account of the customer is held by a bank. Issues involving matters such as liability, anti-money laundering, transaction monitoring for fraud detection and compliance fall under the appropriate local, national and international banking laws and regulations. When a payment is initiated, the consumer's bank must authorize the transaction. The payment networks used are the traditional ones such as Visa and MasterCard and the major differences are at the endpoints of the transaction.

In the nonbank-centric model, the account of the customer is held at nonfinancial organizations such as an MNO or a third-party payment service such as PayPal. In such a case, important regulatory, security and even profit sharing questions arise. For example, which entity will be responsible for the regulation of these services—the respective national telecommunication authority or the respective national bank?

Especially in the European Union (EU), the easing of restrictions on payment operators are leading to changes in the mobile payment landscape across Europe. Specifically, new players (mobile operators, department stores, etc.) will be allowed to be recognized as Payment Service Providers (PSPs) without having the status of a traditional credit institution

[3] SMS is a text messaging service component of phone, web or mobile communication systems, using standardized communications protocols (Global System for Mobile Communications/general packet radio service [GSM/GPRS] and code division multiple access [CDMA]) that allow the exchange of short text messages between fixed line or mobile phone devices.
[4] USSD is a protocol used by GSM mobile phones to communicate with service provider computers.

(as defined in the European directive 2000/12/CE) and to operate in direct competition with traditional financial/credit institutions, provided they comply with the requirements set out in the directive. Specifically, they can act as an Electronic Money Issuer (EMI)[5] or PSP.[6] They will be able to offer services such as cash deposits, cash withdrawals, direct debits, credit transfers, payments initiated by a card or a similar device, and credit (for a maximum 12-month period). Many competitors already own electronic money issuer licenses in Europe, from Internet giants such as PayPal and Google™, to start-ups such as Crandy, Luup or Tunz. Some telecom operators already own a banking license, e.g., Mobilkom in Austria, have a subsidiary with financial status, or have built partnerships with PSPs or banks. Until now, none of the above-mentioned initiatives seems to have worldwide adoption.

Currently, the bank-centric NFC-based payment model seems to be the most prevalent and, for that reason, will be the main focus of this paper. There are nonbank-centric payment systems being used, but the degree of adoption has not been as great. That being the case, this paper highlights the features and risk for nonbank-centric payments for illustrative purposes while focusing primarily on the issues around proximity and bank-centric NFC-based systems for the larger discussion.

The Mobile Payment Ecosystem

The mobile payment ecosystem involves the following types of stakeholders:

- Consumers
- Financial service providers (FSPs)
- Payment service providers (PSPs)
- In-service providers (merchants), including content providers
- Network service providers (NSPs)
- Device manufacturers
- Regulators
- Standardization and industry bodies
- Trusted service managers (TSMs)
- Application developers

These stakeholders can take a variety of forms—financial institutions, debit/credit card networks, clearing/settlement organizations, software solution providers, third-party payment processors, MNO/wireless operators, handset/chip manufacturers, customers and merchants. The various different stakeholders fight to take their share of the revenue in the new ecosystem with financial institutions, debit/credit card networks and MNOs competing for the role of FSP and NSP and for the associated transaction fees. Mobile contactless payment is one application among many. A global overview of the main stakeholders in the NFC ecosystem, and the role they could play in the near future, are presented in the next paragraph.

The various different stakeholders fight to take their share of the revenue in the new ecosystem with financial institutions, debit/credit card networks and MNOs competing for the role of FSP and NSP and for the associated transaction fees.

Some examples of the value propositions for these varied stakeholders are:

- **Mobile operators**—Mobile contactless payment provides a means to add value to their commercial offerings with new services that will, potentially, allow them to increase their average revenue per user (ARPU) thanks to new revenue that could come from different sources, such as transaction fees, renting space on the handset or SIM card, data traffic (mainly from over-the-air [OTA] downloads), managing service providers' applications, and providing financial services.

[5] Electronic Money Issuer: The entrant must have an electronic money issuer license, defined by directive 2000/46/CE, allowing it to manage low-value payments, based on an online stored-value account.

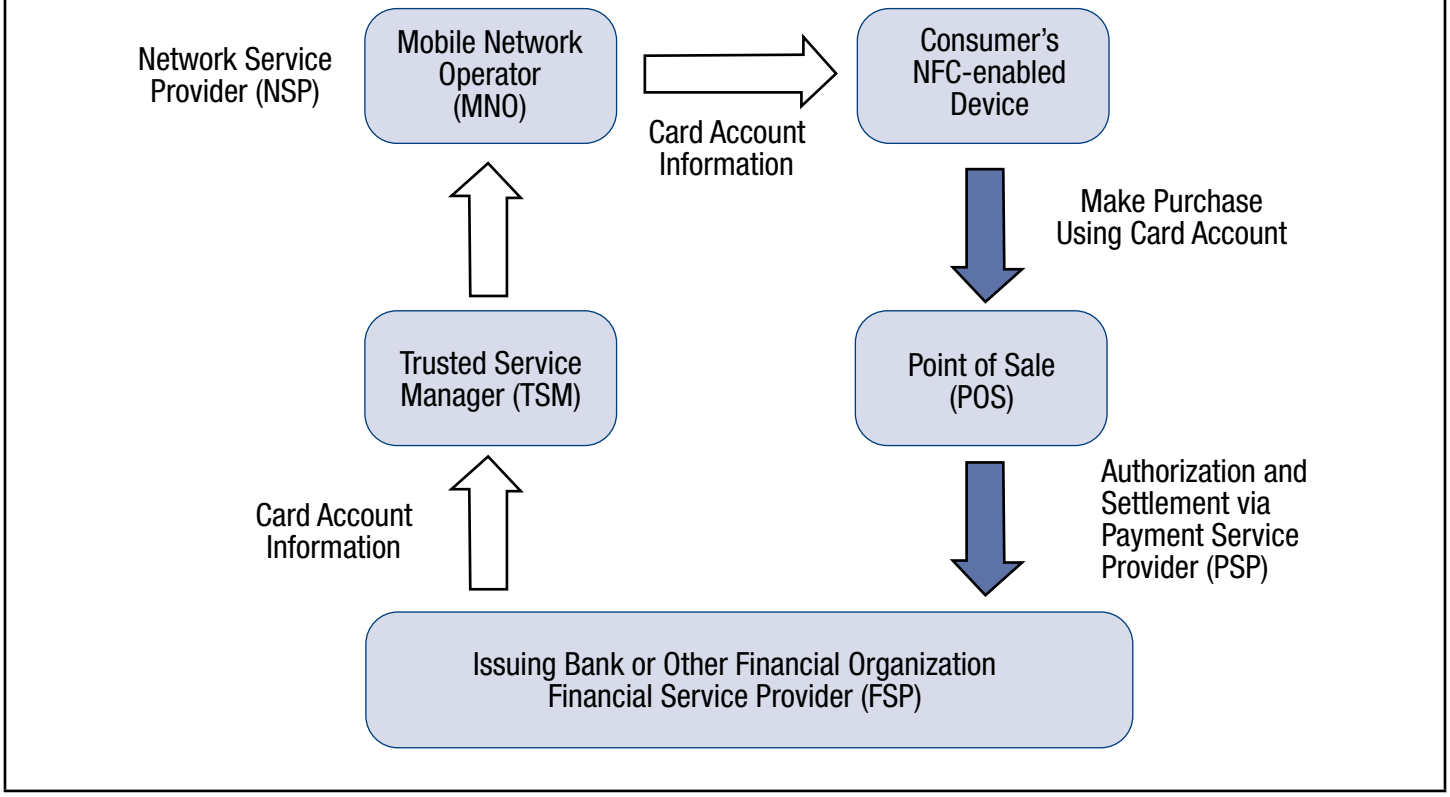
[6] Payment Service Provider: The entrant must have the status of a Payment Institution (PI), as defined in article 6 of the European directive on payment services in the internal market, adopted in April 2007.

- **Banks**—Mobile contactless payment will reduce cash handling (for micropayment) and plastic card issuing costs (for macropayment). It also provides the opportunity to offer more interactive services, linked to online banking services, such as providing credit at the point of purchase.
- **Merchants**—Contactless payment helps to speed up transaction time as well as generating more transactions, especially for micropayments, and also reduces cash handling. Mobile contactless payments also could reveal new opportunities for loyalty programs, especially with an e-coupon that could be stored in the handset and consumed at the checkout by swiping the phone.
- **Transportation operators**—Many transit system operators already offer contactless cards for use on their networks. Because the infrastructure is already deployed, the transportation sector is a preferred one to launch mobile contactless services on a large scale. Putting an e-ticket into the mobile phone helps increase customer satisfaction by making daily travel easier. And replacing tickets and contactless cards with contactless applications that can be downloaded to the handset will significantly reduce ticket issuing costs.
- **Ticket vendors**—Event organizers, museums and cinemas that sell tickets via the Internet or over a mobile network can now send tickets directly to the purchaser via their NFC-enabled handset, making the purchasing of tickets much faster and possible from any location. Additionally, purchasers can be fast-tracked into the event when they arrive, rather than waiting in lines or queues. Event organizers also can use these applications for more interactive services, such as providing additional information about the event.

While it is clear that the potential of mobile contactless payment is significant for everyone involved, there are questions concerning the business model and value sharing.

To provide some context and to further expand on points made earlier, this paper takes a look at the life cycle of a bank-centric NFC mobile payment as illustrated in **figure 2**.

Figure 2—Life Cycle of a Bank-centric NFC Mobile Payment



The diagram illustrates the various stakeholders involved in a bank-centric mobile payment. It depicts also the flow of information concerning: a) provision of the consumer's payment account information to the phone from the issuing financial institution (personalization of the device) and b) authorization of the NFC proximity mobile payment via an existing PSP provider network. The solid arrows indicate payment-related transactions, while the outlined arrows denote actions related to the personalization of the application. It is also assumed in this figure and in the NFC transaction model that the user's mobile device that hosts the NFC chip is a trusted platform, i.e., it utilizes a trusted platform module (TPM) as defined and specified by the Trusted Computing Group (TCG).

A new stakeholder which is introduced in the NFC model is the Trusted Service Manager (TSM). The TSM is a trusted third party who (potentially) could be used to manage the deployment of mobile applications. As illustrated in **figure 2**, the mobile payment life cycle including a TSM would involve the following:

- A financial institution prepares the account data and sends the payment account information to a TSM.
- The TSM delivers the consumer's payment account information over the air (OTA) through the mobile network to the secure element in the mobile phone.
- Once the payment account is in the phone, the consumer can use the phone as a virtual payment card at merchants who accept contactless credit and debit payments.
- In this case, the payments are processed over the current financial networks with credits and debits to the appropriate accounts.
- The mobile operators' network is used only during the personalization of the device. The TSM also handles the life cycle of the device so it administers the customer account data federation between its mobile phones and deactivates the NFC chip in case of theft.

Worldwide, there have been a number of deployments of mobile payments across the spectrum of proximity and remote payment and for both bank-centric and nonbank-centric transaction models. **Figure 3** provides a snapshot of the types of mobile payment services that are being provided and that are representative of the mobile payments ecosystem that is evolving.

Figure 3—Mobile Payment Services

Service Provider Type	Services—Examples
Hybrid-collaborative	• Safaricom and Vodafone (Africa) launched M-PESA—an SMS-based payment service targeting the unbanked, prepaid mobile subscribers in Kenya. • Google Checkout™ (US)—Google partnership with Sprint®, Citi®, MasterCard, and FirstData®
Mobile network operator (MNO)	• Paybox by MobilkomAustria—an SMS-based system that also has an NFC system for mobile ticketing for mobile transport • NTT DoCoMo, Inc. (Japan)—Osaifu-Keitai® mobile wallet service
Independent payment services	• Obopay™, Inc. (US)—A P2P mobile payment company enabling mobile phone users to send and receive money through their phones via a mobile web browser or SMS • PayPal Mobile™ (US)—Provides mobile PIN-based web and SMS capabilities for PayPal account payments • Western Union® —Mobile application provides P2P money transfers from the sender's bank account to the recipient's Western Union cash card • e-Transfer by Interac, Inc. (Canada)—Provides the ability to send and receive money directly from one bank account to another using online or "mobile banking" through a participating financial institution without sharing any personal or financial information

Each party views its responsibilities and liabilities differently, the ecosystem requires a road map to identify the required infrastructures and functionalities to support the transaction contexts and, most importantly, success will require collaboration and interoperability among industries that have not worked together or used a shared environment.

Some key points to note are that each party views its responsibilities and liabilities differently, the ecosystem requires a road map to identify the required infrastructures and functionalities to support the transaction contexts and, most importantly, success will require collaboration and interoperability among industries that have not worked together or used a shared environment. This last point highlights the fact that there will be both business risk and technical risk encountered as mobile payments are adopted, especially in situations where the industry may move away from the bank-centric model.

Business Benefits and Challenges

The advent of mobile payments brings a variety of benefits both from a business and consumer perspective. These include:

- **Speed and convenience for the customer.** They do not need to carry cash or credit cards.
- **Cost-effective coverage is available in rural areas where no financial institutions exist.** In fact, recent evidence from the Philippines has shown that a typical bank branch transaction costs the bank US $2.50, while a mobile payment transaction costs only US $0.50 (according to a 2007 *Asian Banker* report).
- **The capability to send money abroad via person-to-person (P2P) mobile payment services.** With an estimated 191 million migrant workers around the world, and with the business potential for international remittance of US $257 billion in 2005 (according to the UN and the World Bank, respectively), international fund transfers via mobile phone represent a significant opportunity for mobile operators.
- **The mobile wallet can consolidate many cards.** This eliminates the need for physical cards and providing one type of device for all NFC applications (transportation, buying goods, etc.).
- **Improved authentication via PIN-based service.** This provides an enhanced layer of security.
- **There is an opportunity to reach a large proportion of the earth's population without the need for a large investment in technology.** Mobile phones are more widespread than bank accounts, particularly in rural areas.
- **There is no need for cash for merchants and clients.** This reduces the risk of carrying and transferring cash, particularly in high-risk or volatile environments.
- **The amount of required stored data to meet compliance requirements is reduced.**
- **Smartphone capabilities such as geolocation and Internet connection can be used to improve the security of the transaction and improve the capabilities of detecting fraud.** Additionally, the combination of the two previously mentioned technologies can create a new type of marketing, "geomarketing," where the merchant can use geolocation and mobile payment data to build a customer profile and provide a personalized experience.
- **Better realization in case of theft of the mobile phone vs. that of a credit card.** Consumers tend to be more aware of their mobile phones than their credit cards because their phones are multifunction devices and therefore are more frequently used.
- **Mobile payments open the market for professionals and low-segment merchants without point-of-sale (POS) terminals.** It is a cheaper alternative than investing in hardware to accept electronic payments. At present this is a nascent aspect of mobile payments that may over time become a key selling point of the technology.
- **The use of smartphones counters skimming methods that account for a significant portion of card fraud.** They also provide protection against so-called pickpocketing of information from cards equipped with radio frequency identification (RFID) tags.
- **Remote wipe functionality is widely available on smartphones and tablet devices either by default or as an application.** This provides protection of user personal and financial information should the mobile device be lost or stolen.

There are some challenges and cost-value considerations for businesses when considering use of mobile payment services. These include agreement on the business model to be used for revenue sharing and customer ownership, the retooling costs to support mobile payments such as deploying an NFC capability, and the current regulatory uncertainty.

Risk and Security Concerns

Historically, fraudsters have targeted the various payment vehicles and this is likely to be the case for mobile payments; therefore, upfront analysis and countermeasures are needed to mitigate the risk of this double-edged tool. Risk from a mobile payments perspective can be categorized as either traditional or emerging. Traditional risk involves denial or theft of services and loss of revenue, brand reputation and customer base whereas emerging risk involves the use of mobile payments in money laundering and terrorist funding.

Traditional risk involves denial or theft of services and loss of revenue, brand reputation and customer base whereas emerging risk involves the use of mobile payments in money laundering and terrorist funding.

Because the most widespread current implementation is the bank-centric NFC model, the emerging risk at present is out of the scope of this paper and therefore the current discussion will focus on traditional risk issues. For a discussion of money laundering and terrorist financing issues and risk mitigation approaches, an excellent source is the document "Integrity in Mobile Financial Services: Measures for Mitigating Risk From Money Laundering and Terrorist Financing" written by the World Bank.[7]

Risk for the participants in the mobile payments ecosystem depends on the role of the entity user, network or communication provider, or payment service provider. Some entities such as MNOs may play two such roles simultaneously. **Figure 4** provides a snapshot of the types of threats and risk that may come into play across the mobile payments environment among its principal players.

Figure 4—Mobile Payment Risk

Target Type	Vulnerability	Threat	Risk	Countermeasures
User	Over the air (OTA) transmission between phone and point of sale (POS) (NFC reader)	Interception of traffic	Identity theft, information disclosure, replay attacks	Trusted platform module (TPM), secure protocols, encryption
User	Inadvertent installation of malicious software on mobile phone by user	Downloaded application intercept of authentication data	Theft of authentication parameters, information disclosure, transaction repudiation	Authentication of both user (PIN) and application (digital signature by trusted third party), TPM
User	Absence of two-factor authentication	User masquerading	Fraudulent transactions, provider liabilities	Two-factor authentication
User	Changing or replacing mobile phone	Configuration and setup complexity	Reduced adoption of the technology; "security by obscurity"	Simplified user interface, security parameters in TPM set by trusted party
User	Smartphone Internet and geolocation capabilities	Malware on mobile device; poor data protection controls at merchant/payment processor	Data disclosure and privacy infringement; profiling of user behavior	User control of geolocation features, cryptographically supported privacy, trusted platform module, vetted authorization and accounting
Service Provider	POS system accepts OTA transmissions	Malicious party floods POS system with meaningless requests	Denial of Service (DoS)	Request filtering at reader based on mobile device-reader relative geometry
Service Provider	POS devices are installed at merchant premises.	Masquerade attacks; tampering with POS	Theft of service, replay, message modification	POS vendor vetting, message authenticators, vetted authorization and accounting
Service Provider	Lack of digital rights management (DRM) on mobile device	Mobile device user illegally distributes content; e.g., ringtone, video, games	Theft of content, digital piracy, risk to provider for digital rights infringement, loss of revenue to content provider or merchant	DRM incorporated in smartphone TPM design, cryptographically supported DRM
Service Provider	Weakness of Global System for Mobile Communication (GSM) encryption for OTA transmission; SMS data in cleartext on mobile network	Message modification, replay of transactions, evasion of fraud controls	Theft of service or content, loss of revenue, illegal transfer of funds	Strong cryptographic protocols, SMS message authenticators, encryption

[7] Chatain, P.; et al.; "Integrity in Mobile Phone Financial Services—Measures for Mitigating Risks from Money Laundering and Terrorist Financing," World Bank Working Paper No. 146, World Bank, Washington D.C., USA, 2008, *http://siteresources.worldbank.org/INTAML/Resources/WP146_Web.pdf*

Strategies for Addressing Risk

Mobile payments bring new opportunities and new risk. The mobile payment transaction can be more exposed to risk because several parties are involved in performing the payment service jointly. This may worsen if important services are outsourced to potentially unregulated third parties without clear lines of accountability and oversight, or which are located abroad. This multiparty transaction environment is conducive to exploitation by fraudsters using both technological and sociological attacks if the appropriate protection mechanisms and accountability controls are not established throughout the mobile payment ecosystem. With careful planning that includes all the stakeholders, processes and technologies involved, the opportunity exists to make security an intrinsic element of all mobile payment systems.

The financial, payment and network service providers (FSPs, PSPs, NSPs) should implement the appropriate safeguards and privacy and security governance programs. The lack of clear regulation should not be used by an organization as an excuse for not being proactive. There exists risk from misuse by authorized users such as money laundering and risk of illegal use, the latter area may require support from new laws that will evolve to ensure adequate protection. Each organization involved in the chain of the transaction data should put in place strong positive controls to protect such data while in its custody.

One central concern is ensuring that the transaction being undertaken is most likely being carried out by the person authorized or registered to carry it out. Use of two-factor authentication will contribute to more effective identity protection for the consumer and higher identity assurance to the merchant. In the case of bank-centric NFC transactions, protection from transactions originating from unauthorized users or bogus mobile phones can be accomplished by the use of dynamic card verification values (CVVs). NFC chip-enabled mobile phones support dynamic CVVs as compared to the static CVVs used on magnetic stripe cards. Thus, if a bogus mobile phone is then used, it will present the wrong CVV and the transaction will not go through, thus protecting both the consumer and service provider or merchant. Similarly, the same type of assurance to the consumer should be established at the merchant side. Techniques analogous to secure sockets layer (SSL) methods should be used to ensure that only legitimate POS or service providers can interact with the mobile phones. These points are representative of a larger set of issues regarding trustworthiness of identities and credentials for both mobile payments and mobile commerce in general. Such issues and potential strategies for addressing them are discussed, for example, in the 2010 White House publication on the United States national strategy for trusted identities in cyberspace.[8]

Another important factor to consider is the data classification during the transmission and storage of the data at the various nodes. Organizations should identify the data which are considered personal and sensitive and should ensure that appropriate mechanisms are in place. Also, in the case of financial data, a very important facet (aside from encryption) is the matter of data integrity. Organizations should take this into account. In case the mobile payment data will be used for marketing services, organizations could be found liable for unfair business practices if they utilize customer data for purposes not included in the customer notices.

Equally important to consider are POS systems in the case of proximity payments. Organizations should ensure that the third parties with which they interact have robust security governance projects in place. Additionally, specific attention also should be given to the TSM, which acts as the entity that "personalizes" the TSM-compatible chip on the vendor-supplied mobile device. In such a collaborative cross-platform environment, an organization's risk control program should have a strong focus on the management of the third-party services.

ISACA's Business Model for Information Security (BMIS) and COBIT and Risk IT frameworks provide useful approaches for businesses to follow in analyzing and actualizing the people, processes, technology and organizational changes associated with the adoption of mobile payments. BMIS can be used to help the organization address the context and protection of mobile payment data within the organization. The COBIT and Risk IT frameworks can be applied by an enterprise to ensure that an effective risk control mitigation process will be established regarding the use, collection and governance of mobile payment information not only within the organization, but also for the management of the risk arising from relationships with the third parties.

[8] "National Strategy for Trusted Identities in Cyberspace—Enhancing Online Choice, Efficiency, Security and Privacy," The White House, USA, April 2010, *www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf*

Finally, just as a chain is only as strong as its weakest link, specific attention should be given at the originating point of a mobile transaction—the customer device and the user. Users should be educated to understand the corresponding risk. Mobile device manufactures should not only collaborate with the payment industry for the development of platforms that ensure a secure environment for conducting mobile transactions, but also the interoperability between different smartphone models as users tend to frequently change or update their mobile phones. The seamless provision of secure interoperable services is of critical importance for the success of mobile payments.

Additional discussion of many of these points as they relate to mobile devices may be found in the ISACA white paper (2010) *Securing Mobile Devices*.

Additionally, in this new ecosystem, the control mechanisms developed by banks over many years should be leveraged. These controls, when used in conjunction with technological countermeasures and information that can be derived from mobile transactions—such as geolocation—can raise the confidence that a transaction is not fraudulent. Regardless, transactions also should be segmented by purchase amount, location and merchant category, and risk should be managed accordingly.

Governance and Change Issues

The adoption of mobile payment systems will require changes in business models and processes as well as the underlying technology infrastructures involved. Training and new internal controls should be designed and monitored. A major driver in the adoption of mobile payment services is the business model that delivers value to all players in the ecosystem. Business models can be bank-centric, mobile operator-centric, independent service provider-centric or hybrid-collaborative. As noted previously, this publication is focused on the bank-centric aspects of the mobile ecosystem.

The adoption of mobile payment systems will require changes in business models and processes as well as the underlying technology infrastructures involved.

From a business model perspective for both business-to-business (B2B) and business-to-consumer (B2C) activities, there will need to be both provision for fair access to consumer segments among mobile payment stakeholders and adequate customer protection and privacy. Sound customer relationship management (CRM) will require adequate and timely disclosure of risk, responsibilities and liabilities associated with mobile transactions to customers; and identification of recourse for customers and establishment of grievance handling procedures for both internal and cross-platform and cross-organizational transactions.

There will be a need to modify existing networks or develop new network structures to provide the seamless interoperability that will be needed among the participants in the mobile payments ecosystem, many of which have not had direct interaction previously.

Due to the unique nature of the mobile payments, individual organization countermeasures will not be sufficient so specific attention should be given to interorganization relationships within the mobile payments ecosystem. For example, until now, payment cards had been controlled by a financial organization or institution. Now, card information is stored on chips, e.g., SIM cards, that can be moved from device to device. And customers change mobile phones, lose phones and buy from various vendors that are not controlled by banks. This situation requires that a new entity be put in place to govern the uncontrolled chip and to ensure the trusted distribution of payment card information.

A possible solution to provide mitigation of such mobile payment threats at a systems level is to deploy a TSM architecture that is collaborative across technical and business boundaries to provide the core of a secure mobile payment ecosystem.

A possible solution to provide mitigation of such mobile payment threats at a systems level is to deploy a TSM architecture that is collaborative across technical and business boundaries to provide the core of a secure mobile payment ecosystem. Such an approach is being actively evaluated by some of the national banks in discussion with network operators and merchant communities.

In a TSM-based infrastructure, the TSM would be a neutral intermediary to oversee business and operational requirements for large-scale deployment of mobile payments. Its functions would include such things as management of business rules and authentication, providing connectivity between MNOs and service providers, ensuring end-to-end security, providing application life cycle management for MNOs, handsets and customers, and end-to-end customer support. Some caveats in using this approach are that the TSM would not participate in actual NFC contactless transaction processes, i.e., transactions would be processed over existing payment channels and the TSM would facilitate secure authentication to the edge of the network prior to transmission over existing channels.

Assurance Considerations

Upon examining the mobile payment ecosystem, the roles of the stakeholders and the nature of the transactions involved, it can be seen that an optimal way to determine what assurance criteria should be applied (and in what context) is to consider two levels or degrees of assurance. The type of assurance approach to mobile payment services is a function of the roles involved. Specifically, this can be accomplished by:

- Applying banking-level compliance scrutiny to service providers handling the distribution of money as well as payment services; e.g., PayPal, Western Union, Google Checkout and lottery systems
- Applying standard audit models and standards for payment systems associated with the purchase of goods and services; e.g., MNOs, transit system authorities and retail merchants

The assurance professional should consider the following when reviewing organizations that provide mobile payment services:

- ISACA's COBIT framework can be particularly useful to service and third-party providers because it provides a sound basis for risk management, compliance and proper protection and use of mobile payment information. ISACA's *Mobile Computing Security Audit/Assurance Program* document provides a useful COBIT domain and process cross-reference that can be tailored directly to the mobile payment security and audit environment and context.
- Ensuring compliance with pertinent regulations governing both the payment industry and the telecommunication industry because this new kind of payment logically falls into both categories
- The contractual relationship of the organization with the TSM, particularly mutual assurance obligations and representations
- The trust transfer points of the mobile payment transaction process and how these are protected to ensure end-to-end trust from consumer initiation of a transaction to purchase fulfillment, payment and settlement
- Privacy protection and integrity of transaction data and the account details of the customer data
- Awareness training of organization members for the new risk and responsibilities for handling mobile payments that the new ecosystem brings

Conclusions

The mobile payments market is one that is undergoing transformation and holds a future that is promising for both consumers and providers alike in a world that is witnessing a rise in mobile services based on smartphone technology. Some key points of particular interest to security and assurance professionals, based on the current state and anticipated future for mobile payments, that can be noted are:

- **Collaborative and competitive (co-petitive) models for mobile payment services are being created**. There are recent partnerships such as the one that Google struck with Sprint, Citi, MasterCard and FirstData and the Visa announcement of its acquisition of Fundamo™, the platform behind mobile payments solutions in more than 40 countries. Such cross-business and cross-platform operations will be necessary for mobile payments to gain traction and will require adaptations of existing business, security and assurance models as well as revised or new interoperability standards
  and regulations.
- **Security and privacy as well as convenience are key drivers from a consumer perspective.**
- **Strong assurance from independent trusted third parties as well as the development of, and adherence to, best business practices within the mobile payments ecosystem will be required to encourage widespread consumer adoption.** Compelling business cases will need to be made for enterprises to retool to accommodate mobile payment technologies such as NFC.
- **Right now the future is promising and seductive, but uncertain.**

Additional Resources and Feedback
Visit *www.isaca.org/mobile_payments* for additional resources and use the feedback function to provide your comments and suggestions on this document. Your feedback is a very important element in the development of ISACA guidance for its constituents and is greatly appreciated.