Technology and Security Considerations for Mobile Contactless Payments at the Point-of-Sale in the U.S.

Summary Report of June 18-19, 2013 Mobile Payments Industry Workgroup Meeting

Susan Pandy
Federal Reserve Bank of Boston

November 8, 2013

Susan Pandy is a Director in the Payments Strategies Group at the Federal Reserve Bank of Boston.

 The authors would like to thank members of the MPIW and panelists for their thoughtful comments and review of the report.

I. Introduction

In June 2013, the Federal Reserve Banks of Boston and Atlanta convened a meeting with the Mobile Payments Industry Workgroup (MPIW) to address the technological and security considerations that are impacting the rollout of mobile contactless payments at the point-of-sale (POS) from the perspective of POS terminal providers and smart card providers.[1] For more information about the meeting panelists, see Appendix I.

This paper will highlight some of the panel discussions at the meeting. The primary objective of the meeting was to gain a better understanding of which technologies will likely prevail for mobile contactless payments in the U.S. — near field communication[2] (NFC), cloud, or QR codes — with many companies hedging their bets on all technologies. However, the panel discussions were primarily focused on NFC technology, given the experience of the panelists with NFC and the challenges to its widespread adoption. This paper covers the (a) technical complexity and cost of NFC adoption; (b) security challenges of mobile payments at POS and tools for addressing related vulnerabilities; and (c) practical considerations for the future. Some attention was also given to EMV[3] migration in the U.S. due to its impact on NFC adoption.

II. Technical Complexity and Cost of NFC Implementation

One of the challenges to U.S. adoption of mobile contactless payments is the technical complexity and cost to deploy NFC. Implementation of an NFC platform involves multiple stakeholders (banks, card networks, smart card (chip) makers, POS terminal and handset manufacturers, mobile network operators (MNOs), and trusted service managers (TSMs)), who all must coordinate the critical testing and

[1] Smart card providers, also referred to as chip manufacturers, represent expertise in security processes, software, hardware, and cryptography. Together, they offer solutions such as manufacturing of secure elements (SE), which include embedded SEs, Universal Integrated Circuit Cards (UICCs) or SIM cards, and/or microSDs, as well as corresponding trusted service management services and trusted execution environment secured software. Details about each company are located in the Appendix I.

[2] Near Field Communication (NFC): Standards-based wireless communication technology that allows data to be exchanged between devices that are a few centimeters apart. NFC-enabled mobile phones incorporate a smart chip (a secure element) that allows the phone to store payment application and consumer account information securely and use the information as a virtual payment card. NFC payment transactions between a mobile phone and a POS terminal use the standard ISO/IEC 14443 communication protocol currently adopted by EMV and U.S. contactless credit and debit cards that allows the mobile phone to emulate a physical contactless card.

[3] EMV is a global specification for credit and debit payment cards based on chip card technology that defines requirements to ensure interoperability between chip-based payment cards and terminals. EMV chip cards contain embedded microprocessors that provide strong transaction security features and other application capabilities. The EMV specification encompasses credit, debit and contactless (card and mobile) payment transactions. The primary use for these chip-based cards is to perform payment transactions that store encryption data for authentication. As part of the transaction authorization, the card uses the data to prove it is authentic, thus preventing the use of stolen or cloned cards. For more information, see http://www.emvco.com.

certification of secure elements (SEs),[4] mobile handsets, POS terminals, and payment applets[5] to provide the level of security expected from NFC-based payments.

Merchants and the POS

Merchants have been reluctant to adopt NFC because it is a complex process. Adoption requires merchants to upgrade existing POS terminals or purchase new, NFC-enabled POS terminals that have been tested and certified. Furthermore, merchants must train staff to use the new terminals as well as generate consumer awareness and adoption. They must invest time, resources and money, without any guarantee that consumers will use NFC-enabled mobile devices to make purchases. To add to the complexity, merchants are now struggling with how and when to migrate to EMV.

NFC-enabled POS terminals in the U.S. represent about 10% of the largest merchants to date. Preparing to deploy EMV may also affect this low penetration. So, even though over 20 million phones are certified for the Isis mobile wallet,[6] adoption of NFC mobile payments in the U.S. remains slow. The fact that Apple once again did not include NFC on its latest iPhone 5S also impedes adoption because 39% of smartphone owners in the U.S. have iPhones, while 52% have Android smartphones.[7]

Merchants expressed discontent about the large investments in hardware and software that they have made over the years for fraud prevention. Merchants must now make similar investments in POS terminals to prevent fraud. Before committing to future POS terminal investments for fraud prevention (i.e., EMV) and to accept new payment types (e.g., NFC, QR code), merchants want to know the shelf life of new terminals, whether they are capable of being upgraded to EMV,[8] and the extent to which existing terminals can be upgraded to retain Payment Card Industry Data Security Standard (PCI DSS)[9] compliance. POS terminal providers noted that many of the newer terminals are upgradable with software to enable NFC, cloud, or QR code payment acceptance, but most of the older terminals are not software upgradeable.

---

[4] A secure element (SE) is a tamper resistant smart card chip that facilitates the secure storage and transaction of payment and other sensitive credentials. SEs are used in multi-application environments and can be available in multiple form factors like plastic smart card, UICC (SIM), embedded SE (eSE), micro SD, etc. For more information, see http://www.smartcardalliance.org/.

[5] Each of the card networks has their own payment applet that enables the mobile device to interact with NFC-enabled terminals.

[6] According to Isis, it has over 40 "Isis-Ready" device models being sold at this time. Currently, Isis is only available on Android handsets but has plans for rolling out iOS (Apple) and Windows Mobile.

[7] comScore (2013) accessed from http://www.comscore.com/Insights/Press_Releases/2013/6/comScore_Reports_April_2013_U.S._Smartphone_Subscriber_Market_Share/.

[8] Merchants with EMV/smartcard hardware can accept EMV after a software upgrade and associated certification. Merchants without EMV/smartcard hardware can add a consumer-facing EMV/smartcard PIN pad to the existing terminal or replace the existing terminal with an EMV/smartcard- enabled terminal.

[9] See https://www.pcisecuritystandards.org/security_standards/documents.php?association=PA-DSS.

Currently, there is a significant difference in NFC adoption between Tier 1 and Tier 2-3 merchants.[10] Some Tier 1 merchants are adopting NFC[11] because they can create a viable business case and justify the investment to upgrade their terminals. NFC also enables Tier 1 merchants to invest in loyalty programs and expand the range of marketing activities they can pursue to attract consumers. One panelist suggested that as more consumers gain experience with other technologies to make contactless payments (e.g., cloud, QR code), they will eventually ask the larger Tier 1 merchants to enable NFC. For now however, the majority of Tier 1 merchants are not motivated to invest in NFC given little consumer demand.

For smaller merchants (Tier 2-3), there is not a strong business case for NFC mobile POS payments because most of their customers do not yet have NFC-enabled smartphones that could lead to further demand. Merchants also cannot afford to upgrade their terminals to accept NFC-based mobile payments and therefore, will have to wait for critical mass (i.e., more NFC-enabled devices and more customers using this technology).

In the short-term, the simplest approach for some merchants may be to offer cloud-based mobile payments because implementation is easy, the investment is minimal, and it requires nominal changes to most modern POS terminals. However, potential risks should be factored into any mobile platform decision.

A mobile payment platform that does not store consumer data on the mobile device may be more appealing to merchants if it alleviates the need for them to comply with PCI DSS (the cloud service provider would need to comply with PCI DSS) and still creates value for the consumer. Another option would be for the industry to use the unique characteristics of the mobile device to make the transaction more secure, so that merchants can avoid further costs for security on their end.

Card Issuers, Smart Card and Handset Manufacturers and Related Stakeholders

The technical complexity and cost of NFC adoption affects card issuer and/or bank decision-making as well. Issuers face a different release cycle for NFC than what they are accustomed to for physical

[10] Each payment card brand (Visa, MasterCard, etc.) has their own requirements and definitions of Payment Card Industry (PCI) compliance levels. Visa's PCI compliance level definitions categorize Tier 1 – 3 merchants as follows: Tier 1 merchants are those processing over 6 million Visa transactions annually. Tier 2 merchants process 1 to 6 million Visa transactions annually. Tier 3 merchants process 20,000 to 1 million Visa e-commerce transactions annually. For details see http://usa.visa.com/merchants/risk_management/cisp_merchants.html.

[11] Some merchants that have adopted NFC include McDonald's, Walgreens, CVS, and Cinemark Theatres, to name a few. NFC mobile payments can be accepted at merchants that accept MasterCard PayPass, Visa PayWave, American Express ExpressPay, and Discover Zip. Over 200,000 U.S. merchants accept contactless and NFC payments today, according to Gemalto.

distribution of plastic cards, which is every 1 – 2 years. Distribution of mobile SIM cards tends to be more frequent as it must address mobile device operating system changes that occur every 6 – 12 months, requiring multiple recertification steps. In effect, mass deployment is complicated because of the need to get all of the handsets enabled with certified SIMs, applications and the operating system. According to panelist Brian Russell of Giesecke & Devrient, "the sheer number of certification activities is daunting."

Testing and certification processes to support NFC are important to ensure security compliance and interoperability, but involve a lot of coordination. EMVCo first certifies all secure element (SE) and hardware processes based on the GlobalPlatform Compliance Program before the card networks provide customized certification. The SE (UICC (SIM), microSD, or eSE), mobile device, and payment applet (payment application of the various card networks that go into the SE) must all be independently certified. Each card network has a proprietary certification process for SEs. Certification for each type of SE (UICC (SIM), microSD, and eSE) is handled differently because even though the requirements may be the same, each SE type is considered a different form factor. POS terminals and the payment applications residing on the terminals require certification as well.

In addition to managing the NFC lifecycle issues, NFC chip providers must address the incremental expense associated with the SE and the Trusted Service Manager (TSM).[12] The retail cost of the SE can range from $3.00 - $5.00 per 100 kilobytes of memory.[13] To improve the NFC business model and increase opportunities for adoption, TSM costs to MNOs, card account issuers, and mobile wallet providers (who pay TSMs to provision payment credentials to the SE and provide lifecycle management of NFC applications) must be reduced.

III. Security Challenges for Mobile Payments at the POS

Using a mobile device to pay at the POS presents a complex security challenge because the handset contains multiple applications that can access the Internet. According to Jack Jania of Gemalto, "mobile technology makes it hard to determine where the edge[14] is anymore – a mobile device can serve as a

[12] Trusted Service Managers (TSMs) are responsible for provisioning credentials to secure elements in mobile phones to ensure transaction security. Depending on the size and scope of a TSM, other functions may include provisioning/account set-up; ensuring compliance with security requirements for software, hardware, handsets, chips and applications; fraud and risk management; and customer service and support. Defined in Federal Reserve Banks of Boston and Atlanta. 2011. *Mobile Payments in the United States Mapping Out the Road Ahead*, accessed from http://www.bostonfed.org/bankinfo/payment-strategies/publications/2011/mobile-payments-mapping.pdf.

[13] A kilobyte refers to computer memory. One kilobyte equals 1024 bytes as defined by Microsoft Windows and Linux. For example, Samsung has an NFC eSE with 760 Kilobyte high-density flash memory with sufficient capacity to store diverse mobile services such as credit cards, e-money, transportation payment services, coupons, etc. For more information, see http://www.samsung.com/us/news/newsRead.do?news_seq=19957&gltype=globalnews.

[14] Edge network, from the perspective of a networking security professional, and in the context of this paper, represents a shift in the approach for enterprise security from the traditional firewall method to a more granular method that stresses data protection

payment method or be used as a payment terminal (mPOS) to accept payments." Furthermore, businesses have a tendency to focus on the security of the device itself (i.e., a POS terminal or a mobile device) rather than the security of the network, which is the point of vulnerability where a fraudster can maximize his attack and attain the highest return. To that point, card readers should encrypt all data before transmission (data at rest), and while the data is being transmitted from a mobile device to a terminal to complete a transaction.

Tools for Addressing Vulnerabilities for Mobile Payments at the POS

Fortunately, there are several tools and technologies available to fortify mobile payments at the POS, including smart cards (chips), encryption and end-to-end security, tokenization, and authentication and identity management.

Smart cards are considered a very good technology for securing the edge of the network, particularly because they help to secure the exchange of data throughout the network. Smart cards secure a transaction by providing tamper-proof storage of user and account identity information and have proven to be much more reliable than the magnetic stripe card counterpart. Smart cards also protect against multiple security threats, from careless storage of user passwords to sophisticated system hacks.

Encryption is another important tool for securing the mobile payments ecosystem, however not all merchants use encryption to protect transaction data. Many small merchants use older POS systems with minimal encryption, making them more vulnerable to data breaches. Also, while many small merchants may rely on POS vendors, they often do not change the default passwords on these systems. Furthermore, small merchants are simply unaware of the importance or existence of PCI compliance standards. For those merchants familiar with PCI, the compliance costs are often too high or they may feel that their third-party processors are responsible for PCI compliance for their POS systems.

Historically, POS terminal providers focused on encrypting PINs at the POS, but not the actual card account data. Today, more POS terminal providers are focused on end-to-end security and overall database security. The experts agreed that using hardware, or point-to-point encryption, is the best way to address weaknesses in the mobile contactless payments system. Hardware-based encryption is also a critical component to overall risk prevention.

One challenge to mobile payment adoption is the assumption by some mobile industry specialists that the mobile device is not secure. They believe that the mobile handset exposes the entire network to fraud,

---

over infrastructure protection. See http://www.enterprisenetworkingplanet.com/datacenter/datacenter-blog/virtualization-muddles-the-network-edge.html.

and that every link needs to be secured to prevent the entire system from collapsing. To address this challenge, smart card manufacturers are working with companies including Intel and Symantec to develop a new security area known as the Trusted Execution Environment (TEE) that resides in the mobile device.[15] This concept is still in its nascent stage of development.

Customer authentication, whether making a payment at the physical POS, online, with a card, or using a mobile phone/app, is a critical component of security that minimizes the potential for identity theft and data compromise. For mobile POS payments, authentication can be enhanced using a number of methods including encryption and/or tokenization. The goal of any method is to protect the transaction from end-to-end.

Another way to approach the security of mobile payments is through identity management.[16] There is growing industry support to focus on consumer identity and multifactor authentication using the mobile device because it provides numerous opportunities to enhance security for mobile payments by leveraging additional authentication factors such as photos, PINs, location-based data, voice prints, biometrics and more.

When applying identity/credential management to the mobile payment paradigm, the debate tends to focus on the application of federated versus distributed credentials. Distributed credentials remain under the direct control of the owner (the consumer) whose biometric credentials (e.g., fingerprints, photos/iris template, and voice prints) reside on his mobile device, allowing the service provider to securely communicate with the mobile device. Distributed credentials release service providers from dealing with the risk and hassle of managing millions of sensitive credentials in a centralized database.

Federated credentials, or "federated identity", link a consumer's electronic identity across multiple systems, allowing the user to have a single secured and protected identifier (the identity) that is recognized across many service providers. For example, in a federated identity model, a merchant

[15] According to GlobalPlatform, a Trusted Execution Environment (TEE) is a secure area that resides in the main processor of a smartphone (or any mobile device) and ensures that sensitive data is stored, processed and protected in a trusted environment. The TEE's ability to offer safe execution of authorized security software, known as 'trusted applications,' enables it to provide end-to-end security by enforcing protection, confidentiality, integrity and data access rights. For more information, see http://www.globalplatform.org/mediaguidetee.asp.

[16] Identity management and authentication were also discussed in the context of security clearance in airports, noting examples of iris scanning combined with a smart card in the Netherlands, which failed because it was too expensive; and the U.S. Global Entry program that allows expedited clearance for pre-approved, low-risk travelers arriving in the United States. Global Entry enables participants to check-in at kiosks with a machine-readable passport or U.S. permanent resident card, scan their fingerprints for verification, and make customs declarations. France has a natural security solution that uses the fingerprint that resides on a card that the consumer carries and does not depend on a centralized database of biometrics.

website could accept a customer's identity credentials maintained at another site to create efficiencies in usability and economies for itself.[17]

IV. Practical Considerations for the Future of Mobile Payments

Fragmentation in the mobile payments ecosystem and little traction with any one mobile platform continue to drive many industry stakeholders to experiment with multiple technologies (e.g., NFC, cloud, QR code) because they do not know which solution will ultimately prevail. NFC is still struggling because its value proposition to incent consumer adoption for mobile beyond payments is unclear. Providers of NFC mobile platforms must figure out what will change consumer behavior. This will include educating consumers on how to effectively 'tap and pay,' similar to how the mouse changed consumer behavior/attitude towards clicking. As use of the mouse matured, consumers became less aware of why they clicked at all and gave it little thought. The path to NFC adoption may require taking baby steps to build consumer comfort with tapping and waving versus swiping at POS. Therefore, a key question underpinning investments in mobile payments is how to build consumer experience. The industry needs to solve how consumers will gain additional value by tapping, touching, presenting or scanning their mobile device to pay at the POS.

Starbucks is viewed by payments analysts and industry trade reports as an example of successful implementation of a closed-loop mobile payment model. Starbucks enables the customer to pay using a mobile app that generates a QR code on his mobile device to scan at the POS reader. Starbucks processes about 4.5 million mobile transactions a week. Customers receive value from the loyalty program attached to the payment functionality. Starbucks benefits by collecting valuable information about its customers' preferences and purchasing behaviors. Mobile phones are used to pay for over 10% of Starbucks' U.S. transactions, and the Starbucks (plastic) card is used to pay for over 30% of its U.S. transactions. The Starbucks loyalty program is used for 25% of transactions.[18] Following the success that Starbucks realized, other retailers such as Dunkin Donuts and CVS also rolled out closed-loop loyalty mobile payment systems using QR codes. The Merchant Customer Exchange (MCX)[19] is also planning to use QR codes for its initial mobile payments model.

---

[17] For more information on federated identity management, see http://das.ufsc.br/~lucianobarreto/artigos/Federatedidentitym.pdf.
[18] Wolfe, Daniel. (2013, June). Starbucks: Over 10% of our U.S. transactions are mobile payments. *PaymentsSource*. Retrieved from http://www.paymentssource.com/news/starbucks-over-10-percent-of-our-us-transactions-are-mobile-payments-3014457-1.html.
[19] The Merchant Customer Exchange (MCX) was created by a group of the nation's big box merchants to offer consumers a customer-focused, versatile and seamlessly integrated mobile-commerce platform. For more information, see http://www.mcx.com.

In the current environment, cloud-based mobile payments appear to be the easiest and quickest way for merchants to accept mobile payments at the POS. Investment at POS is lower than the cost to upgrade terminals for NFC and changes to the POS system are nominal. However, use of a cloud provider that stores customers' payment credentials must be factored into the cost and risk.

While NFC solves larger, complex and more critical problems (such as security), it has yet to demonstrate how it will enhance the user experience at the POS. According to some marketing experts, for NFC to stand out against competing solutions, providers have to incent consumers to pay using an NFC-enabled mobile phone at least once per day. To accomplish this, they need to transform the overall payment experience by integrating new capabilities that the mobile phone offers into the payment/purchase process.

Because adding mobile payments to the POS infrastructure requires merchants to make considerable investments, they want to know the potential for value-added services. When customers use mobile features such as store check-in, facial recognition, or location-based services that generate customer data for analysis, this enhances the merchants' ability to know their customers and improve their purchasing experiences. Line-busting, used by Chipotle, Five Guys and Jamba Juice,[20] is an example of the value in enhancing the user's experience and the transaction process by completely removing the need to pay at the physical POS.

Merchants will have to take several factors into consideration before choosing a technology platform for mobile payments, including how to implement EMV to reduce card-present fraud. Depending on whether they select chip plus PIN or chip plus signature, merchants will need to make sure their equipment is compatible. Merchants will also need to make sure that any terminal upgrades are compatible with their mobile payment strategy.

There are challenges to all of the POS technologies emerging in the mobile payment ecosystem that need to be addressed. These challenges are summarized below:

[20] Line-busting works well in high-throughput retail locations. These mobile apps allow customers to configure an order, pay for the order directly on their smartphone, select a store and available pick-up time, and then skip-the-line to pick-up their pre-ordered meals. These applications can create loyal customers, help to handle peak traffic times in the store and improve the overall customer experience.

1. For NFC, the technical complexities of the secure element (SE) and the cost of implementation need to be resolved.

2. The mobile payments industry needs to ensure that the ecosystem is secure. Encryption is a strong, hardware-based approach; however, any security solution used must consider what is best for the overall user experience.

3. A coordinated industry consumer education and awareness campaign is needed to encourage consumer adoption of mobile contactless payments in the U.S. The payments industry has done very little to educate consumers, particularly the "non-adopters" who are reluctant to use mobile because of security and fraud concerns. The industry should also look at why contactless cards failed in the U.S. and fix those issues as they relate to mobile contactless payments.

4. Providers need to help issuers and merchants understand the business case for adopting contactless mobile payments and the benefits it will provide: increased speed of checkout, convenience, enhanced security, potential for increased sales, more volume, loyalty, etc.

5. The industry would benefit from some standards or guidelines around certain areas to improve the process and level the playing field, but not inhibit innovation. Security standards that are device, technology, and solution agnostic and supported by all stakeholders must be a priority. Some MPIW members support standardizing storage of credentials by securing the device with hardware (e.g., encryption) or by securing the cloud. It was also noted that standards would benefit the transit industry given the diversity in their approaches and uncertainty for how to move forward. Standards might help transit authorities move more quickly to a mobile solution, knowing that their systems would be more interoperable based on a set of standards.

V. Conclusion

While there are technical and security issues to be resolved, the general consensus of the experts was that mobile contactless payment solutions for POS payments can be successful in the long-term, along with other types of mobile solutions. Complexities in implementation involving multiple components and participants sometimes result in misleading news reports that predict or forecast success or failure before the solution has time to evolve. For example, pilots should be viewed as positive developments that provide education and support progress. Enhanced industry collaboration could help address some of the commercial challenges and reduce the friction around some technologies that are perceived as hurdles.

Many industry stakeholders believe that there is an opportunity for enhanced authentication using the smartphone. Broadly demonstrating the security opportunities afforded by the mobile device could further advance mobile contactless payment adoption.

The MPIW should develop a roadmap to help the industry figure out how to remove risk from the mobile payment system, drawing on the security tools noted earlier, create value for consumers, and determine what standards could help achieve a more open and secure mobile payment system in the long-term.

Appendix I
Moderators and Panelists

MODERATORS

Damien Balsan, Chief Operating Officer, *Loop*

Loop, Inc. is the world's first and only mCommerce platform provider with a mobile wallet solution that works at nearly 90% of existing retail locations, today. The platform allows consumers to securely and conveniently buy and save using their smartphones, and allows merchants to easily promote actionable deals and offers to their customers' mobile, without heavy integration or cost. Loop also provides the most advanced mobile POS and Checkout solutions seamlessly integrated with its mobile wallet and promotions system. The company leverages its patent pending breakthroughs to create a platform that includes mobile peripherals, mobile apps, and cloud-based services to facilitate truly innovative next generation commerce. www.looppay.com/.

Seb Taveau, Chief Technology Officer, *Validity*

Headquartered in San Jose, California, Validity is the world leader in Natural ID authentication, providing fingerprint sensors with the highest levels of performance, security, cost-effectiveness and design flexibility. Validity's patented LiveFlex® fingerprint sensor technology enables authentication, mobile payments, and touch-based navigation for smartphones, tablets, and notebook computers. For the latest news on biometrics and authentication, read the Natural ID blog by Validity CTO, Sebastien Taveau. www.validityinc.com/.

PANELISTS

Jack Jania, Senior Vice President/Gen. Manager, Secure Transactions NORAM, *Gemalto*

Gemalto is the world leader in digital security with 2012 annual revenues of €2.2 billion and more than 10,000 employees operating out of 83 offices and 13 Research & Development centers, located in 43 countries. We are at the heart of the rapidly evolving digital society. Billions of people worldwide increasingly want the freedom to communicate, travel, shop, bank, entertain and work – anytime, everywhere – in ways that are enjoyable and safe. Gemalto delivers on their expanding needs for personal mobile services, payment security, authenticated cloud access, identity and privacy protection, eHealthcare and eGovernment efficiency, convenient ticketing and dependable machine-to-machine (M2M) applications. We develop secure embedded software and secure products which we design and personalize. Our platforms and services manage these products, the confidential data they contain and the trusted end-user services made possible. Our innovations enable our clients to offer trusted and convenient digital services to billions of individuals. Gemalto thrives with the growing number of people using its solutions to interact with the digital and wireless world. www.gemalto.com

Brian Russell, Senior Vice President/Gen. Manager, Payment Mobile Security Division, *Giesecke & Devrient*

G&D develops, produces, and markets products and solutions for payment, secure communication, and identity management. G&D maintains a leading competitive and technological position in these markets. The group's clients most notably include central banks and commercial banks, wireless communications providers, businesses, governments, and public bodies. G&D is a global technology leader in banknote production and processing. It supplies banks, mobile network operators, local public transit authorities, other companies, and original equipment manufacturers (OEMs) with end-to-end solutions comprising hardware, software, and services for mobile security applications, especially in telecommunications and electronic payments. G&D also provides highly secure travel documents, ID systems, and healthcare cards that serve not only as conventional identification documents, but also as tools for authenticating and securing online business transactions. www.gi-de.com

Rod Hometh, Vice President, Market Development, *Ingenico*

Ingenico is the worldwide leader in the secure electronic payments industry. With over 20 million payment terminals deployed across 125 countries, we are the first choice for retailers, banks and payment service providers when it comes to payment solutions. Delivering the very latest security certified and high performance electronic payment solutions as well as the widest range of value added services, Ingenico is shaping the future direction of the payment solutions market. Offering the complete global solution, Ingenico takes banks and businesses 'beyond payment' by unlocking powerful customer intelligence from each and every transaction to enable the creation and delivery of a host of unique and differentiating new services - securing brand loyalty and increasing business revenues. http://ingenico.us/

Ken Harris, General Manager, Global Payments, *NCR Corporation*

NCR Corporation is the global leader in consumer transaction technologies, turning everyday interactions with businesses into exceptional experiences. With its software, hardware, and portfolio of services, NCR enables more than 300 million transactions daily across the retail, financial, travel, hospitality, telecom and technology industries. NCR solutions run the everyday transactions that make your life easier. NCR is headquartered in Duluth, Georgia with over 26,000 employees and does business in 180 countries. NCR is a trademark of NCR Corporation in the United States and other countries. www.ncr.com

Hans Reisgies, Co-founder, Head of Product Development, *Sequent*

Sequent provides a leading Trusted Service Manager (TSM) software and services platform. Sequent's comprehensive SE-TSM Secure Element Management service supports diverse contactless security technologies while rapidly onboarding issuers and application providers. Sequent's SP-TSM software enables banks and other service providers to provision and manage their own credentials on the secure elements of mobile phones. Sequent's Wallet Enablement Platform makes it easy to add Near Field Communication (NFC) payments and other credentials into rich, branded consumer mobile apps. The Company is backed by Opus Capital, Jado Investments and SBT Venture Capital, the venture arm of Sberbank.
www.sequent.com

Erik Vlugt, Vice President, Product Marketing, *Verifone*

VeriFone Systems, Inc. is the global leader in secure electronic payment solutions. VeriFone provides expertise, solutions and services that add value to the point of sale with merchant-operated, consumer-facing and self-service payment systems for the financial, retail, hospitality, petroleum, government and healthcare vertical markets. VeriFone solutions are designed to meet the needs of merchants, processors and acquirers in developed and emerging economies worldwide. www.verifone.com