ASA

Annie Searle & Associates LLC

Research Note

Mobile Payment Trends

By Andrew H. R. Hansen

Abstract – With the constantly changing technological landscape, identifying enduring trends can be difficult. Near field communication and credit card reading applications are two emerging trends in the mobile payment industry. Each of these products and services utilizes different technologies that allow currency to be transferred. These new technologies introduce new security risks. Consumers and business owners should prepare for these potential changes, and invest the necessary resources to ensure the appropriate solutions are selected.

ASA

Annie Searle & Associates LLC

Introduction

There can be no doubt that the rapid technological advances of the previous decade have fundamentally altered the way businesses and consumers interact. But with the constantly changing landscape, it is often difficult to determine which emerging trends will be embraced and incorporated into daily life, and which will be discarded after a brief moment in the spotlight. With the widespread adoption of smartphones, and the more recent proliferation of tablet computers, it should come as no surprise that many developing trends are associated with mobile devices. Trends in the mobile payments industry have the potential to impact society in a major way. But with these new mobile trends come new risks. As illustrated in a recent IBM study, "There was a 19 percent increase in 2011 in publicly released exploits aimed at mobile devices."[1] This research note will provide a general overview of two mobile payment trends: near field communication technology and credit card reading mobile applications, discuss security features and possible threats and conclude with recommendations for navigating these emerging technologies.

Mobile Payments

Alternative payment options in the mobile financial services industry operate under many names, including: mobile payments,

mobile money, mobile banking and mobile wallet. Regardless of which term is preferred, the basic objective behind the mobile payments movement is to streamline the payment process by replacing a wallet full of credit cards with a mobile device. At the influential South by Southwest Interactive Conference and Festival last month, mobile payments were a popular topic. Commenting on the trend, one writer said, "The future of buying stuff seems like it's going to be cashless, credit card-less and tied to whatever mobile device you happen to be carrying around."[2] Although the technology for mobile payments has existed for some time, 2011 saw a number of major organizations enter into the industry.[3]

Near Field Communication

Many of these new mobile payment providers share a similar technology called near field communication. Near field communication (NFC) is a "short-range wireless technology that enables the communication between devices over distances of less than 10 cm."[4] As alluded to earlier, this technology is not exactly new or cutting edge. In fact, it is a variation of radio-frequency identification (RFID), a technology that has been utilized in a large variety of products for decades. Similar to RFID, near field communication "can quickly swap information between devices when they're touched together."[5] By

producing NFC enabled smartphones, advocates promise there will be no more fussing with a wallet full of credit cards. Instead, "you simply wave your phone at a point-of-sale reader."[6]

NFC technology has been deployed in hundreds of trials, pilots and tests around the world.[7] Yet consumer adoption has been timid, a characteristic attributed to the fact that the number of establishments that accept mobile payments has been limited.[8] In 2010, "only about 10% of total POS (point-of-sale) terminal shipments included some form of contactless technology."[9] However, it is projected that "85% of terminals shipped worldwide will be contactless-enabled in 2016, driven by increased proliferation of contactless cards and, especially, rapid adoption of NFC-enabled phones."[10]

The following is a high level description of three prominent organizations that are utilizing NFC technology in their products:

Google Wallet: Google's mobile payment option. Currently only available with the Nexus S 4G on Sprint, and is accepted at over 140,000 MasterCard PayPass locations across the United States.[11] In time, Google hopes to support all major credit cards.[12] The service is expected to be offered on at least 10 additional phones on Sprint this year.[13]

Isis: A joint venture between Verizon Wireless, AT&T and T-Mobile, expects to launch in limited locations mid-2012.[14] Chase, Capital One

and Barclaycard have all entered agreements to make their debit and credit cards available on Isis.[15]

Apple: Speculated to be a feature of the iPhone 5, with the iWallet, users "can see their entire credit card profiles, view statements and messages form their banks, and even adjust preferences or add additional cards.[16] They can also keep track of their payments and statements within the iTunes billing system.[17]

PayPal: Reportedly partnering with Swedish companies Accumulate and Point, users can download a PayPal in-store iOS or Android app, and when they visit a participating store receive a sticker which allows them to pay via NFC.[18] In addition, they have developed an iPhone app that allows users to transfer money directly from one phone to the other, by bumping the two phones together.[19]

Security

Because NFC mobile payment "reuses the logical and physical security mechanisms used for contactless cards" while offering "additional security layers," it appears that sufficient protection is in place to enable secure transactions.[20] According to security firm Gemalto,[21] the following three key features reinforce Mobile NFC security:

1) The NFC SIM cards storing a consumer's payment credentials and the payment applications are certified according to security standards defined by financial services authorities and are comparable to CHIP-N-PIN security.

2) Consumers can choose to authenticate transactions by entering a PIN code on the payment application. Consumers can also request the PIN to be entered for all payments, even for small amounts – providing the end-user with complete control of protection features.

3) Secure over-the-air technology for remote management enables immediate remote blocking of the payment application.

Even with these additional security layers, one possible risk, specifically associated with Google Wallet, is the lack of encryption for all the data associated with the card.[22] Researchers with Via Forensics report "While Google Wallet does a decent job securing your full credit card's numbers, the amount of data that Google Wallet stores unencrypted on the device is significant. Many consumers would not find it acceptable if people knew their credit card balance or limits."[23] From the perspective of privacy, it may be valuable to consider how personal consumer information will be monitored and tracked by the NFC enabled devices. Mobile payment services will likely "be used to closely monitor your activity as a consumer… allow(ing) a far closer and more intensive monitoring of this activity."[24] Depending on your tolerance for information security, the unencrypted credit card balance/limits and the use of personal information might not be

alarming. Being aware of these risks and making educated mitigation decisions is the critical factor.

Card Readers

The second mobile payment industry trend we will discuss is point-of-sale mobile card readers. This technology combines a simple card reading device and mobile application that allows for the processing of credit card payments. As seen in the images, card readers developed by Square, Intuit and PayPal all offer a similar set of products and services.

25

26

27

After a user signs up for the necessary account with any of these organizations, they will be mailed a free card reader. Connecting the card reader through the earphone plug of an Android or iOS powered smartphone or tablet and downloading the necessary mobile app will transform the mobile device into a credit card processor. Charges processed by the card reader can be directly transferred into the merchant's bank account, with the service provider collecting a small transaction fee. Some of the benefits described by Intuit[28] include:

- Getting paid instantly
- Process any major credit card
- No need to purchase additional equipment
- Get authorization in seconds – no need to write down payment information or call into your back office
- E-mail or text message clients electronic receipts directly from your phone

In addition, some services like Square's Register, allows merchants to keep track of sales and offer detailed analytics that are synced and stored in the cloud.[29]

Security

Because no credit card information is stored on the phone,[30] these services are secure – or as secure as any other credit card payment method.[31] However, Square has been subject to criticism based upon potential hacking vulnerability. As explained by hackers at a 2011 Black Hat convention, plug-in adapters like those offered by Square (and the other brands previously mentioned), work by converting credit card magstripe data into audio, which is then interpreted by the application and translated back into credit card numbers.[32] With the appropriate software, arbitrary credit card numbers could be fed into the device and fraudulent credit card charges of any amount could be entered.[33] In addition to racking up fraudulent charges, there is also concern that

these devices could easily operate as "skimmers." A skimmer is a "device that gathers credit card information during an otherwise legitimate transaction."[34] For example, at a restaurant a server might take a customer credit card out of sight to process their payment, the credit card could be swiped and its information saved, without the customer ever knowing.[35]

An important distinction to make is that the security criticism these products receive is largely aimed at what ill-intentioned people can do with the technology, not necessarily the products and services themselves. Square (and others) claim that because they monitor the entire transaction process, they have the ability to detect and "stop fraud via live monitoring programs that analyze transactions as they're happening."[36] In response to the skimming criticism, Square co-founder Jack Dorsey said to call Square insecure is "not a fair or accurate claim and it overlooks all the protections already built into your credit card."[37] He went on to say, "Any technology – an encrypted card reader, phone camera, or plain old pen and paper – can be used to 'skim' or copy numbers from a credit card… The bank that issues your credit card recognizes this and does not hold you responsible for fraudulent charges."[38] This response might be sufficient for some, but it appears pressure from powerful investment partners like Visa, were

finally enough for Square to alter its system to encrypt credit card data on the fly. In very recent news, it appears that Square has started to ship card readers that use encryption.[39] For those using unencrypted plug-in adapters from any brand, moving to the more secure product is worth the effort.

Conclusion

It is expected that NFC technology will become a multi-billion dollar industry[40] whose reach will not only impact mobile payments, but will also affect the travel industry, the way we purchase tickets, comparison shopping, advertising, and possibly several others.[41] Similarly, companies like Square are now processing millions of dollars a day.[42] This research note was intended to be considered from the perspective of both the consumer and the business owner. Whether you are a technologically savvy consumer trying to maximize available technological advances, or a business owner hoping to find new ways to satisfy customer needs, the coming years will likely bring a change to the way money is exchanged.

There are many circumstances where mobile credit card readers like those mentioned previously could easily and instantly impact the business of a small retailer. But from a risk mitigation perspective, there might be some wisdom in allowing the technology and the major

players in the NFC mobile payment industry to become more fully established, before investing in their products or services. It is often tempting to respond to major trends by getting on the bandwagon as soon as possible. But manifesting patience and conducting thorough research will ensure the products and services selected will not only be the appropriate solutions, but that they will also be the solutions that endure.

ASA

Annie Searle & Associates LLC

References

[1] "Cyber-Criminals Change Tactics as Network Security Improves." *CIOInsight.* 3 Mar. 2012. Web. 6 April 2012. <http://www.cioinsight.com/c/a/Latest-News/IBM-Security-Improving-but-CyberCriminals-Are-Adapting-757749/>

[2] Gallaga, Omar L. "Big Moves in Mobile Payments Could Impact Your Wallet – If you Still Have one." *Statesman.com.* Web. 1 April 2012. 4 April 2012. <http://www.statesman.com/life/big-moves-in-mobile-payments-could-impact-your-2276305.html>

[3] "Mobile Payments." *Mobile Payments.* n. dat. 4 April 2012. <http://mashable.com/follow/topics/mobile-payments>

[4] "NFC Definition." *Gemalto.com.* n. dat. Web. 4 April 2012. <http://www.gemalto.com/nfc/definition.html>

[5] Gardiner, Bryan. "What is Near-Field Communication." *Gizmodo.com.* 6 Dec. 2010. Web. 5 April 2012. <http://gizmodo.com/5707321/what-is-near+field-communication>

[6] "Mobile Payments and NFC Technology Poised to Revolutionize Retail and Marketing." *NFC Handsets.* n. dat. Web. 4 April 2012. <http://nfchandsets.com/>

[7] "NFC Trials, Pilots, Tests and Live Services Around the World." *Near Field Communications World.* n. dat. Web. 4 April 2012. <http://www.nfcworld.com/list-of-nfc-trials-pilots-tests-and-commercial-services-around-the-world/>

[8] Morales, S. "The Emergence of the Mobile Wallet." *Glyph Interface.* 22 Feb. 2012. Web. 4 April 2012. <http://www.cjandp.com/blog/2012/02/the-emergence-of-the-mobile-wallet/>

[9] Clark, Sarah. "ABI: 85% of POS Terminals to Support Contactless Payments in 2012." *Near Field Communications World.* 11 Aug. 2012. Web. 5 April 2012. <http://www.nfcworld.com/2011/08/11/39038/abi-85-percent-of-pos-terminals-to-support-contactless-payments-in-2016/>

[10] Clark, n. pag.

[11] "Google Wallet: FAQ." *Google.com.* n. dat. Web. 5 April 2012. <http://www.google.com/wallet/faq.html>

[12] "Google Wallet," n. pag.

[13] Melanson, Donald. "Google Wallet Android App Updated, Headed to 'at least' ten More Sprint Phones This Year." *Engadget.com.* 1 Mar. 2012. Web. 5 April 2012. <http://www.engadget.com/2012/03/01/google-wallet-android-app-updated-headed-to-at-least-ten-more/>

[14] Graziano, Dan. "Google Wallet Competitor ISIS Finally Announces Launch Details." *BGR.com.* 27 Feb. 2012. Web. 5 April 2012. <http://www.bgr.com/2012/02/27/google-wallet-competitor-isis-finally-announces-launch-details/>

[15] Graziano, n. pag.

[16] Smith, Dave. "Apple iPhone 5 Release Rumors: 3 New Patents That May Become Features." *Ibtimes.com*. 16 Mar. 2012. Web. 7 Mar. 2012. <http://www.ibtimes.com/articles/315376/20120316/apple-iphone-5-release-rumors-patents-features.htm>

[17] Smith, n. pag.

[18] Rao, Leena. "PayPal Tests In-Store NFC Payments App With Swedish Retailers, Similar Mobile 'Experiments' to Roll out Soon." *Techcrunch.com.* 20 Dec. 2011. Web. 5 April 2012. <http://techcrunch.com/2011/12/20/paypal-tests-in-store-nfc-payments-app-with-swedish-retailers-similar-mobile-experiments-to-roll-out-soon/>

[19] "Google Checkout vs PayPal vs Amazon Payments: What's the Best eCommerce Option?" *DigitalFamily.com.* n. dat. Web. 5 April 2012. <http://www.digitalfamily.com/dreamweaver/ecommerce/Google-v-PayPal.html>

[20] "8 Myths About Mobile NFC – Myth 2." *Gemalto.* n. dat. Web. 5 April 2012. <http://www.gemalto.com/nfc/myths.html>

[21] "8 Myths," n. pag.

[22] Mills, Elinor. "Google Wallet Stores too Much Unencrypted Data in a Rooted Device – Report." *Cnet News.* 12 Dec. 2011. Web. 5 April 2012. <http://news.cnet.com/8301-27080_3-57341844-245/google-wallet-stores-too-much-unencrypted-data-in-a-rooted-device-report/>

[23] Mills, n. pag.

[24] Tristram, Penny. "To Beep or not to Beep – The Pros and Cons of Google Wallet." *My Social Agency.* 28 Sept. 2011. Web. April 5 2012. <http://www.mysocialagency.com/social-media/to-beep-or-not-to-beep-the-pros-and-cons-of-google-wallet>

[25] Image taken from: http://www.techclump.com/wp-content/uploads/2011/05/full_1293811604Screenshot2010-   12-31at10.47.56AM.png

[26] Image taken from: http://articles.businessinsider.com/2011-02-18/tech/29975173_1_android-apps-readers-comparison-chart

[27] Image taken from: http://smallbiztrends.com/2012/03/paypal-here.html

[28] "Intuit GoPayment Mobile Credit Card Processing." *Intuit.* n. dat. Web. 5 April 2012. <http://payments.intuit.com/products/basic-payment-solutions/mobile-credit-card-processing.jsp>

[29] "Square Register for iPad Offers Full Point-of-Sale System for Merchants." 5 Mar. 2012. Web. 5 April 2012. <http://www.appleinsider.com/articles/12/03/05/square_register_for_ipad_offers_full_point_of_sale_system_for_merchants.html>

[30] "Intuit GoPayment," n. pag.

[31] Gobry, Pascal-Emmanuel. "Verifone is Full of Crap – Square is Totally Secure." *Business Insider.* 10 Mar. 2011. Web. 5 April 2012. <http://articles.businessinsider.com/2011-03-10/tech/30064017_1_card-credit-verifone>

[32] Schwartz, Matthew J. "iPad Credit Card Reader Hacked as Skimmer." *InformationWeek Security.* 5 Aug. 2011. Web. 5 April 2012. <http://www.informationweek.com/news/security/vulnerabilities/231300283>

[33] Schwartz, n. pag.

[34] Hornshaw, Phil. "Researchers Reveal two Security Gaps in Square Mobile Credit Card Reader." *Appolicious.* 8 Aug. 2011. Web. 5 April 2012. <http://www.appolicious.com/tech/articles/9019-researchers-reveal-two-security-gaps-in-square-mobile-credit-card-reader>

[35] Hornshaw, n. pag.

[36] "Security is our Priority." *Square.com.* n. dat. Web. 5 April 2012. <https://squareup.com/security>

[37] Crum, Chris. "Square Security Defended by CEO Jack Dorsey." *WebProNews.* 10 Mar. 2011. Web. 5 April 2012. <http://www.webpronews.com/square-security-defended-by-ceo-jack-dorsey-2011-03>

[38] Crum, n. pag.

[39] Crum, Chris. "Square Card Readers Now Reportedly Encrypted." *WebProNews.*27 Mar. 2012. Web. 7 April 2012.<http://www.webpronews.com/bing-video-2012-03>

[40] Smith, n. pag.

[41] Robertson, Travis. "Eight Industries That Will Benefit From NFC Technology." *X.Commerce.com.* 19 April 2011. Web. 5 April 2012. <https://www.x.com/devzone/articles/eight-industries-will-benefit-nfc-technology>

[42] Schonfeld, Erick. "Processing $11 Million a Day, Jack Dorsey Says: "We don't Want to Make Square all About Taxi Cabs." *Techcrunch.com.* 13 Nov. 2011. Web. 5 April 2012. <http://techcrunch.com/2011/11/13/jack-dorsey-square-11-million-day/>