Mobile Security: What's the risk?

HOW TO MAINTAIN CONSUMER CONFIDENCE AND TRUST WHEN SELECTING A MOBILE PROGRAM PROVIDER

In the US alone, 72% of all new mobile phones purchased in 2012 were smartphones.

Imagine having no need to carry plastic credit cards, gift cards, paper coupons, loyalty cards or key fobs. This is, in fact, no longer imaginary but rather a reality that consumers are taking advantage of today. This fast growing landscape is being referred to as mobile commerce, wherein consumers have the ability to use their mobile handset as the form factor to complete transactions. The form factors being replaced by the mobile handset vary from plastic magnetic stripe cards to paper coupons. While it is currently being adopted on a limited basis, this technology is being rolled out quickly to more and more consumers each day.

Now imagine using your mobile handset to pay for your groceries, redeem some coupons and earn loyalty points, then realizing that the debit card balance is $300.00 short. Your account has just been compromised – what happened? With this scenario in mind, what do you think is most important to consumers as they begin to adopt mobile commerce as a regular practice? Convenience … "YES". Ease of use … "YES". Security … "Well, I haven't given it that much thought."

Mobile usage growth by consumers has reached its breakout moment. As of Q1 2013, there were 1.038 billion smartphones worldwide, almost double the number in 2011[1]. In the US alone, 72% of all new mobile phones purchased in 2012 were smartphones [2]. These statistics clearly show that phones are no longer just for talking and texting; they act as wallets, hubs for coupons, loyalty programs and gift cards, and so much more.

As this mobile momentum continues to build, consumers are increasingly sharing their confidential financial information in order to conduct mobile commerce transactions, similar to the evolution of online purchasing over the past few decades. However, unlike mobile commerce security protocols, security best practices for online transactions are mature and proven. In the world of mobile commerce, security standards have yet to be established.

1 http://www.businesswire.com/news/home/20121017005479/en/Strategy-Analytics-Worldwide-Smartphone-Population-Tops-1
2 http://www.comscore.com/Insights/Press_Releases/2013/2/comScore_Releases_the_2013_Mobile_Future_in_Focus_Report

mocapay
Mobile Commerce Made Easy

FOR MORE INFORMATION

Contact Karen Moritzky Bigelow, Director of Client Relations at Mocapay.
303-381-3909 or karen.moritzky@mocapay.com

COLLECTION AND USAGE OF CONSUMER INFORMATION

Retailers, financial institutions, social media and service providers are on task to capture the attention of consumers through mobile. The two most popular approaches are to build a mobile app that may be downloaded from an app store or build a mobile-optimized web application. Mobile-optimized web applications are becoming increasingly popular and offer rich feature functionality, similar if not the same as a downloaded mobile app. These may be accessed by any phone with a web browser and require no download. Consumers may also be driven to a mobile web application via another source: Google, Yelp!, Around Me, or other sources where their brand comes up in a search. In either case, these apps may be accessing consumer information without that consumer's knowledge. Information such as a phone number, device ID and location are easily captured from applications and HTML5 sites.

From a merchant's perspective, information gleaned in this passive manner, as well as consciously shared information, is used for a variety of purposes: acquiring new customers, increasing customer loyalty and learning more about customers buying habits in order to create more relevant and targeted promotions or campaigns. Reaching consumers directly via their preferred method of communication – mobile device – is a benefit to merchants for the following reasons:

- Ability to share more meaningful and relevant messages with consumers (new products, seasonal promotions, location information)
- Ability to send promotions that may be tracked to the individual when redeemed
- Mobile payments - capture and store payment information for the purpose of simplifying purchases
- Enhance loyalty programs by allowing consumers to enroll, earn and redeem awards via the mobile device
- Offer gift card programs with features to allow for purchasing and giving gift cards, transacting with the merchant and managing accounts

FOR MORE INFORMATION

Contact Karen Moritzky Bigelow, Director of Client Relations at Mocapay.
303-381-3909 or karen.moritzky@mocapay.com

THE IMPORTANCE OF MAINTAINING CONSUMER CONFIDENCE AND TRUST

Headlines such as "Google Wallet Security Breach Is A Warning To All Smartphone Users" only hurt the adoption of mobile technology as a whole by consumers.

While the benefits of mobile data collection are clear for the merchant, how do merchants maintain consumer confidence and trust? While consumers understand the value exchange between sharing some of their information in return for free items, discounted pricing or special promotions, they should also be afforded the confidence that their information is being safely guarded by the trusted merchant. In order to maintain consumer confidence in this relatively new ecosystem, it is the responsibility of the merchant (with the help of their technology provider) to keep consumer information safe and secure.

Certainly there are regulations and guidelines that govern how information is secured and shared (such as HIPPA, PCI, and MMA) but what is ultimately at risk? What should business owners know about technology in order to make intelligent decisions around mobilizing their brand? When evaluating the choice to share and/or use information shared via the mobile device, businesses and consumers should be aware of security and fully understand where and how information is being stored and used – especially personal information.

Information that is being shared from one device to another (mobile-to-mobile, mobile-to-host, mobile-to-POS, etc.) is especially relevant. Merchants need an awareness of the different ways information is being captured by mobile devices, as well as an understanding of what happens when consumers use their devices to transact with merchants. The bottom line is that both merchants and consumers need to be concerned about security, specifically around securing personally identifiable information (PII). When information is not secured, trust in the system diminishes. Headlines such as *"Google Wallet Security Breach Is A Warning To All Smartphone Users"* [3] only hurt the adoption of mobile technology as a whole by consumers.

3 http://www.businesscomputingworld.co.uk/google-wallet-security-breach-is-a-warning-to-all-smartphone-users/

FOR MORE INFORMATION

Contact Karen Moritzky Bigelow, Director of Client Relations at Mocapay.
303-381-3909 or karen.moritzky@mocapay.com

SHARED INFORMATION: WHAT'S THE RISK?

In light of mobile payments, let's narrow the scope of this topic to transactions that occur between consumers and merchants. Within this example, there is a wide variety of transactions that can take place – everything from a payment transaction to simply accepting and redeeming an offer. In most instances, personally identifiable information (PII) is captured and used in order to make these transactions possible. The question is, once that information is shared, what happens to it? Since each technology uses information in different ways, the answer depends on the technology being used. In any case, the information is most likely being leveraged for marketing purposes, where the consumer may opt in or out at any point. The information may also be used to conduct a transaction. Transactions may vary from a payment transaction (credit or debit), gift card, loyalty, coupon, online ordering, or other. In almost every case, the information is being stored – presumably securely—by the party to which the consumer has entrusted their information.

In the emerging world of mobile payments, PII security is especially important to merchants as they consider mobilizing their brand. While understanding the risks and executing a secure, trustworthy solution may seem daunting, some basic education about data and how it is managed with relation to mobile devices will help merchants in the technology decision-making process.

UNDERSTANDING HOW DATA IS HANDLED IN RELATIONSHIP TO MOBILE DEVICES

When considering mobile commerce and payments applications, there are two basic ways data is handled:

1) The mobile application or mobile-optimized website stores data on the actual handset
2) The app may be capturing data and storing the information in the cloud for future use.

FOR MORE INFORMATION

Contact Karen Moritzky Bigelow, Director of Client Relations at Mocapay.
303-381-3909 or karen.moritzky@mocapay.com

UNDERSTANDING HOW DATA IS HANDLED IN RELATIONSHIP TO MOBILE DEVICES

Although the functionality of these applications is similar, the way the consumer interacts with and accesses them is very different. In general, a mobile application is downloaded from an app store and can either use the handset's operating system to function or use the phone's browser. With applications that use the browser to operate, much of the functionality may be managed in the cloud. This not only simplifies how the consumer gains access to the application (via the browser), but also allows developers to update applications so consumers have immediate access to new functionality and improvements without manually updating their mobile applications.

When consumers make use of applications, the consumer first downloads the application and is guided through a series of authentication steps. These steps are in place to verify that the individual registering is actually who they say they are and to collect information from the handset that qualifies it as a "trusted" device. In most banking applications, for example, data is stored on the bank's platform and the phone or device must be authorized as an access device to inquire upon that data or conduct financial transactions accessing their bank accounts. Most banking applications do not store information on the handset since there is no reason to duplicate the information from their systems to the handset, not to mention the risks that practice could potentially introduce. When information, such as PII, is stored on a host platform, this is referred to as 'stored in the cloud'.

Alternatively, the entire application may be stored in the cloud and accessed via a browser. This is typically how mobile-optimized websites work. In either instance (mobile application or mobile-optimized web), there is an option to store the sensitive PII in the cloud or on the mobile handset.

FOR MORE INFORMATION

Contact Karen Moritzky Bigelow, Director of Client Relations at Mocapay.
303-381-3909 or karen.moritzky@mocapay.com

UNDERSTANDING HOW DATA IS HANDLED IN RELATIONSHIP TO MOBILE DEVICES

When payment applications store actual credentials on the mobile handset, the process by which the credentials get onto the handset is sometimes referred to as account provisioning. In order to provision an account to a handset, a Trusted Service Manager (TSM) is used. The TSM performs authentication steps prior to accessing the account credentials from the processor. The processor, for example, may be the credit card company who is holding the credentials and delivers them to the mobile handset.

When the credentials are being transferred by the TSM from the processor to the mobile phone, multiple security processes (such as encryption) are utilized to ensure the PII is not compromised. In the case of sensitive financial information, such as credit card credentials, the PII is encrypted and stored on a hardware module within the phone called a secure element. The secure element is a tamper resistant device that stores encrypted payment card information and can access it when the consumer wants to make a payment using their mobile phone. In almost all cases, these payments are "touch and go" payments, which takes advantage of NFC (near field communications) technology. The information is passed to the POS in a contactless manner via an electronic signal versus a card swipe, in which the plastic card's magnetic strip is read by the POS.

Provisioning may be a somewhat cumbersome process and if a phone is lost, stolen or exchanged since the credentials stay on the phone. While they do remain encrypted, it's important to know that any information that is encrypted can also be decrypted. Additionally, the secure element is typically locked down by either the network or the phone manufacturer and can only hold one set of credentials. The entity that controls the secure element controls what can be placed onto the secure element. This payment type may only be available on specific handsets and on specific networks.

FOR MORE INFORMATION

Contact Karen Moritzky Bigelow, Director of Client Relations at Mocapay.
303-381-3909 or karen.moritzky@mocapay.com

Apps that store sensitive consumer credentials in the cloud have many advantages.

Some mobile applications and mobile-optimized websites store consumer credentials in the cloud. Applications that store sensitive consumer credentials in the cloud have many advantages.

- **Flexibility:** Enables users to register and provision accounts to their app and update PII from a computer, their handset, speaking with a live operator, or by using an automated voice response service (VRU).

- **Encryption:** The options available to secure PII on a host platform (cloud) are tried and true. Encryption is the first layer of protection making use of an HSM (Hardware Security Module) to store and control encryption keys. Data is stored in an encrypted manner and may be moved safely from one source (handset) to another (host) safely.

- **Tokens:** Cloud application service providers may also make use of tokens to protect sensitive information. In many cases, tokenization and encryption are used in tandem. When using tokens, the PII is not only encrypted, but it does not move from application to application or database to database. Instead the token is used as a reference point and in order to process transactions. This way, encrypted PII is centrally stored and controlled.

UNDERSTANDING HOW DATA IS USED

Another point to consider is whether the app is interacting with another device, such as a point of sale (POS) system or an eCommerce website. If so, what information is being exchanged? Are actual credentials being delivered from the mobile handset to the POS or is there another piece of information being used to represent the consumer's sensitive information?

FOR MORE INFORMATION

Contact Karen Moritzky Bigelow, Director of Client Relations at Mocapay.
303-381-3909 or karen.moritzky@mocapay.com

UNDERSTANDING HOW DATA IS USED

With tokens, consumer information is at no time exposed in the clear.

This information, the consumers' credentials, may be represented using substitute or proxy information that interacts with another device, such as a POS system. The proxy information may be an encrypted version of the original data or it may be a token that stands in for the credentials. In the case of encrypted data, a key must be exchanged in order to decrypt the data before the transaction is processed. In the case of a token, a database stores the credentials and the token so sensitive personal data is not passed directly over the air. In either case, the distinct advantage for the consumer is that their actual information is at no time exposed in the clear (unencrypted or not tokenized).

When transacting using encrypted or tokenized data, some solutions simply use the handset to replace a plastic card as a form factor with a token. This option takes advantage of the "rails" that the merchant and payment providers have already established to process any type of transaction (credit, debit, gift, loyalty, or other). The consumer credentials are securely stored, in an encrypted fashion, on the host server and are referenced by a token. This allows merchants to use their existing payment, gift, and loyalty provider while adopting mobile as an additional channel add- solution. Mocapay is an example of a provider that utilizes this system.

The token system provides merchants with the ability to select the types of transactions they would like to mobile-enable and also to control marketing and messaging that reaches the consumer via the merchant-branded application. Other solutions, like Paypal, may use the handset to process the transaction and interface directly with their proprietary payment authority. Tokens may also take many forms. Mocapay uses a patented, single-use, perishable token to stand in for payment credentials, while other solutions, like Square, actually use a picture of the customers face to authenticate the transaction.

When mobile applications interact or transact with other third party systems, security is critical. If PII from the mobile device – either delivered to the handset from the cloud or managed locally on the device – is used to complete a transaction on a POS system or an ecommerce website, users should be concerned about exposing their PII in the clear.

FOR MORE INFORMATION

Contact Karen Moritzky Bigelow, Director of Client Relations at Mocapay.
303-381-3909 or karen.moritzky@mocapay.com

THE RISK AND REWARD OF MOBLIZING EXISTING TENDER TYPES

Mobile transactions provide consumers flexibility, convenience, and value.

Mobile transactions provide consumers flexibility, convenience, and value while offering merchants the ability to reach their customers, learn more about them, and specifically measure the effectiveness of mobile marketing programs. Generally speaking, the mobile handset is simply a different medium that replaces more traditional methods.

Examples of traditional mediums include plastic gift cards, plastic credit card or debit card, a paper coupon, or plastic or paper loyalty card. When translating these transactions to mobile, the three most common methods of handling them are:

1) Storing the consumer information on the phone and presenting it to the point of sale in the clear
2) Storing the encrypted consumer information on the phone and presenting it securely to the point of sale
3) Storing the encrypted consumer information in the cloud and presenting it securely (encrypted or tokenized) to the point of sale to process the transaction.

When actual credentials are involved as in methods one and two above, security is paramount. These credentials can include not only the consumer's name, but also their credit card number, security code (CVV), expiration date, and zip code. The utmost precaution should be taken in protecting that information. As such, there is more than just feature functionality to consider when looking for and making use of mobile commerce applications and mobile websites.

FOR MORE INFORMATION

Contact Karen Moritzky Bigelow, Director of Client Relations at Mocapay.
303-381-3909 or karen.moritzky@mocapay.com

THE RISK AND REWARD OF MOBLIZING EXISTING TENDER TYPES

There are some mobile interfaces (applications and mobile-optimized web) that use the actual credentials in order to process a transaction. The most common example of credentials being used on a mobile handset to process a transaction is with a merchant's prepaid or gift card account. In these instances, the actual account number may be displayed on the handset, or in print (from an email or website), sometimes in the form of a bar code or a QR code, and accepted by the POS in order to process the transaction. The primary risk in this scenario is that an image of the screen (or printed media) with that account number could be captured and the screen recreated in order to access the account fraudulently.

As merchants and brands begin to rapidly adopt mobile to reach customers in their preferred form of media, the race for adequate security standards within the mobile landscape is on. Similar to the days when companies were launching their first websites, they are now thinking about where to begin when it comes to mobile. Many factors come into consideration including: feature and functionality, branding, user interface (UI), social media integration, GPS, marketing, and advertising.

When building mobile technology that has the ability to capture and store PII, such as payment card, gift card, or loyalty card data, companies should take into consideration how the security of PII will be maintained. They need to weigh the advantages and disadvantages of each option and also consider how *"future proofed"* the selected solution is. In other words, will this solution still function in tomorrow's POS and ecommerce environments? In doing this, they will not only protect themselves from a potential breach, but also protect their customers, thus avoiding a potential public relations challenge and affecting customer loyalty and commitment.

FOR MORE INFORMATION

Contact Karen Moritzky Bigelow, Director of Client Relations at Mocapay.
303-381-3909 or karen.moritzky@mocapay.com