Reducing the risk of payment card fraud

Leonardo Rodriguez
– Director, Strategy and Innovation AT&T Mobility & Business Solutions

**Introduction**

We live in an age of constant, disruptive, technological expansion and innovation that is changing the way we live, work, and play. There always seems to be a new device, a new service, a new product, a new app, a new loyalty program, or countless “new” ways of doing things to consider; the flood of “NEW” is endless, as is its consumption. Mandated by this rapid pace of business and powered by the accelerated evolution of technology, the new business paradigm is access ubiquity; the delivery of information anytime and anywhere for the purpose of consumption of products and services. This ocean of data continuously flows to and fro, facilitating the purchase and delivery of products and services, driving the proliferation of credit and debit card (“payment card” or “card”) transactions globally.

This paper discusses several powerful approaches designed to help businesses protect against fraud by using AT&T API and mobility data solutions as part of payment card (“payment card” or “card”) use cases.
Over the past several years, the risk of payment card fraud has grown exponentially, as has the potential for financial impact that such fraud poses to merchants, card issuers, and payment processing services providers alike. We now measure the theft of consumer payment card information in the tens of millions of accounts compromised on a seemingly regular basis, and occasionally, in the hundreds of millions as in the case of recent events affecting a number of US retail companies.

Due to limited cardholder liability laws in the United States, merchants and financial institutions generally bear the majority of the losses suffered. To mitigate the staggering potential for loss that exists, merchants, card issuers and payment processing service providers spend countless hours and hundreds of millions of dollars yearly on cyber security defense mechanisms, fraud countermeasures, customer confidence campaigns and call center solutions in order to detect, manage, mitigate and address such thefts.

As a result of the growing risk of fraud, card users are advised to review their card transactions on a daily basis due to the ease with which identity thieves can access their accounts, drain their funds and execute fraudulent transactions with stolen card information. According to the Federal Trade Commission, 17% of all Identity theft fraud reported in the United States in 2013 was credit card fraud.

Common Methods Used in Payment Card Fraud

**Skyrming**
A common method used for acquiring payment card information for the purpose of fraud is known as “Skyrming.” Skimming is the theft of card information used during an otherwise legitimate transaction, usually at a point of sale merchant location such as a store, restaurant, gasoline station, or AT machine. The thief steals card information using methods that can be as basic as photocopying a card and recording zip code and security code information from the consumer during the course of a transaction, to something as sophisticated as the installation and use of a small, concealed electronic device or “skymer” that can read the cards used by consumers at that particular location. These devices are often equipped with miniature cameras that capture the consumer’s PIN numbers and the card security code on the face or back of the card. Camera equipped skimmers are the preferred method used in ATM (Automatic Teller Machine) skimming. Subsequently, skimmed cards can then be replicated through a cloning process and then fraudulently used at automated teller machines, unattended merchant devices, or on the Internet.

**Cloning**
Cloning is the replication of payment cards through the use of forged cards enabled with read/writeable magnetic strips or programmable embedded chips (EVM) that can accept data in the machine readable format that has been stolen from legitimate cards. This method uses credit card information procured either through direct theft, skimming, or purchase of cardholder information from hackers that have compromised merchant or card issuer systems. Cloning of traditional magnetic strip equipped cards has existed for decades and recent evidence suggests that hackers are able to defraud banks issuing EVM equipped cards as well.

Committing Fraud with Stolen Card Data
The use of stolen card information is most prevalent in CNP (Card Not Present) transactions such as those conducted via the Internet or by phone because of the difficulty the merchant has in verifying that the holder is in fact the person they purport to be. Although safeguards exist to protect against fraudulent CNP transactions, most can be bypassed or rendered ineffective through the use of skimming, phishing, carding or other information gathering techniques popular with cyber criminals. This is because most safeguards rely on static information such as postal codes, static PIN numbers or security codes.

Preventing Fraud on ATM and Point of Sale Merchant Machines

**Time Sensitive PIN Generation**
To eliminate the reliance on a static PIN, zip code or card security code, a dynamic pin generation application with a scheduler function is integrated into a bank’s back end ATM access authentication application or a credit card issuer’s transaction authorization system. The PIN generation application provides an externally facing GUI that allows the consumer to create a schedule by which the access authentication service will allow access to ATM applications or credit card transactions. Instead of memorizing a PIN number or a ZIP code that is associated with a billing address, both of which can be acquired by thieves, a new PIN is generated for transactions on a scheduled basis set by the consumer.

The approach can be further enhanced by incorporating a strong multifactor authentication solution on the device, thereby further protecting access to the PIN if the consumer uses a smartphone. A variety of multifactor authentication approaches can be used, including APIs like the AT&T Global Smart Messaging Suite, the pin generation application pushes a time sensitive PIN to the consumer’s SMS capable cell phone at a designated time or via an on-demand process triggered by the consumer. Additional fraud prevention can be attained by incorporating a single use PIN into this process.

This solution can be both network and device agnostic, with the caveat that a device must support SMS at a minimum. Enhanced solutions for smartphones may be limited to certain devices but are otherwise carrier-agnostic, requiring only that SMS service be available.

Location Information Services (LIS) Triggered PIN Generation
As in the previous scenario, a dynamic pin generation application is integrated into a bank’s back-end ATM access authentication application or a credit card issuer’s transaction authorization system. An API is integrated into this system that allows it to receive LIS triggers when the consumer’s mobile device is within defined proximity of a recognized Bank branch.
Using an SMS Messaging service API, the pin generation application pushes a time sensitive or single use PIN to the consumer’s SMS capable cell phone.

As in the time sensitive PIN generation scenario, the approach can be further enhanced by incorporating a strong multifactor authentication solution on the device if the consumer uses a smartphone. The same multifactor authentication approaches previously mentioned can also be utilized. Additional enhanced LIS based authentication solutions may be developed and deployed in the future. These could include network based geo-fenced limitations to the triggering mechanism, device based International restrictions or permissions and card use to phone location verification APIs.

This solution can be carrier and device agnostic in the US and Canada but would require a smartphone and application download for international use.

**Wi-Fi Beacon Triggered PIN Generation**

By integrating Wi-Fi positioning solutions into the LIS solution architecture, the capability to include indoor positioning and “Push” notification / triggering mechanism can be realized.

This approach can provide a refined way for an LIS driven triggering solution to activate when an embedded API on the consumer’s smart device recognizes a bank branch or registered merchant location by detecting its proximity to the entity’s registered Wi-Fi beacon. This process can then push a request to the card issuer or back-end banking ATM access control system that would have a dynamic pin generation application enabled and integrated into an SMS service. The single use (or time sensitive) PIN would be sent to the user device and used for authorizing the transaction or providing access to the ATM.

This solution can be enhanced through the incorporation of the same multi-factor authentication techniques described in both previous scenarios. The solution can be carrier agnostic but may be limited to specific smartphone devices that can support location based triggering applications.

**Online Merchant and Internet Banking Providers**

Online merchants and Internet Banking providers can harden their security and fraud prevention measures by integrating the same dynamic PIN generation solutions described in this whitepaper and incorporating either SMS or email delivery services to send single use or time sensitive PINs to the consumer attempting to logon or to conduct a transaction.

This solution can be enhanced through the incorporation of the same multi-factor authentication techniques described in the previous scenarios and may be carrier agnostic and device agnostic, depending on the hardening enhancement solutions chosen.

**Conclusion**

As consumers in the United States approach the recommended deadline to migrate to EVM equipped cards by the end of 2016, identity thieves are already demonstrating their ability to compromise this technology through innovative approaches. As long as a dependency on static data such as passwords and PINs exists, be they on magnetic strips, chips or simply committed to memory, there will always be risk associated with their use and exposure.

Through the integration of dynamic code pin generation technologies, secured messaging, Identity toolkit APIs, multifactor authentication, and Location Information Services, AT&T can help enable merchants, banks and card providers with the tools and mechanisms necessary to provide enhanced multi-layer payment card fraud prevention solutions.

**Notes**


3. Does not imply a commitment, nor an offer to provide services and is subject to change.

For more information contact an AT&T Representative or visit www.att.com/api-services