

# **Better Security Through Mobile – “The One-Two Punch”**

## **Industry Best Practices**

---

PRESENTED BY  
THE PROCESSOR COUNCIL  
OF THE ELECTRONIC TRANSACTIONS  
ASSOCIATION



## Introduction

*The objective of this whitepaper is to illustrate how, if best practices are followed, mobile payment transactions can be more secure than plastic card transactions.* As such, this paper provides background and discussion points along three general areas, including:

- (i) Overview of Plastic Card Payment Transactions related to Transmission Technology, Credentials Storage, and Authentication Technology;
- (ii) Overview of Mobile Payment Transactions related to Transmission Technology, Credential Storage, and Authentication Technology; and,
- (iii) Comparison of specific Mobile Payment Transaction Models compared to Plastic Card Payment Transactions related to Transmission Technology, Credential Storage, and Authentication Technology.

<i>Key Terms</i>	
<b>Transmission Technology</b>	Technology specification used to communicate cardholder information to the merchant point of sale
<b>Credential Storage</b>	Location of cardholder payment information
<b>Authentication</b>	Mechanisms in place to authorize payments

## Plastic Card Payment Transactions

Plastic card payment transactions are prevalent throughout the world and almost universally accepted by major retailers in the United States. With recent high profile data breaches at certain retailers, some have suggested that plastic card transactions are inherently insecure. This is not true, however, as the entire ecosystem surrounding plastic card transactions has evolved to provide participants with protections in minimizing losses from fraudulent transactions. The ecosystem is designed to distribute risk across the traditional five-party system that involves the consumer, merchant, acquirers/processors, card networks, and issuers. This evolution has occurred in the context of plastic card usage trends, tools utilized throughout the industry, and rules mandated by the card networks. For example, acquirers and

processors have tools to help detect fraudulent transactions (e.g., tokenization and encryption, transaction velocity checks, average ticket size, etc.). The card networks have introduced additional security features for plastic cards such as AVS and CVV2, as well as complex rules related to authorizations and chargebacks their systems must follow. Issuers have developed robust tools to monitor consumer payment activity such as neural networks (e.g., TRIAD). Physical merchants can tokenize card data after it is captured at the point-of-sale and eCommerce merchants have implemented sophisticated fraud detection tools and processes. Plastic payment transactions provide consumers with a certain level of convenience and security. The security and convenience inherent to plastic cards results from the transmission technology, credential storage capabilities, and authentication procedures rooted in the ecosystem. Even so, with the increasing sophistication of criminals and fraudsters in the market, it has become apparent that plastic cards alone and the rules surrounding them might have shortcomings that could be addressed by mobile technology.

**Transmission Technology** - Plastic cards communicate with the POS through a magnetic stripe or smart chip embedded into the physical plastic. Magnetic stripe technology was first developed in the 1970's and *provides a non-encrypted mechanism for communicating basic cardholder information to the merchant's credit card reader*. Smart chip technology was developed later to provide a means for communicating encrypted cardholder information at the point-of-sale, though it does not provide a pure encrypted transmission. EMV cards can be authorized in a contact, contactless or key entered transaction. In a contact or contactless authorization a cryptogram alongside the clear text PAN is sent in the transaction. In cases where the merchant key enters the cardholder's payment information where the contact and contactless redemption forms fail, the PAN is sent for authorization in the clear with no cryptogram. End-to-End Encryption (E2EE) can be paired with EMV to provide encryption of the PAN, providing a more secure transaction in preventing PAN interception for use in eCommerce. Alternatives to E2EE include the use of device-specific PANs (so that, as an example, plastic card PANs cannot be used from a phone) and channel-specific PANs (so that, as an example, plastic card PANs cannot be used for eCommerce transactions).

**Credential Storage** - *Magnetic stripe and chip cards rely on the payment credentials to be stored physically on the card itself.* Magnetic stripe technology is a less sophisticated form of data storage compared to the capabilities of mobile technology, and consumer payment card information is not encrypted within the magnetic stripe. Unencrypted cards can allow for fraudsters to skim and reproduce cardholder information. Although smart chip technology does not encrypt the PAN, it does make skimming card information and card replication fraud more difficult. For example, EMV would not have prevented the current data breach at Target stores, though EMV would have made subsequent fraudulent transactions more difficult by nearly eliminating any card replication and subsequent fraud at physical brick-and-mortar stores. However, the stolen PANs from the Target breach could still have been used in fraudulent eCommerce transactions. Enabling E2EE and EMV, would significantly mitigate and potentially eliminate the eCommerce fraud and card replication fraud in any similar future scenario like the Target breach.

**Authentication** – In general, consumers authorize a card payment transaction utilizing either a signature or PIN (there are exceptions to this for certain types of merchants whereby they waive the signature requirement for smaller ticket sizes). Authorization mechanisms like PIN passcodes provide for an additional authentication layer to exist on card issuer servers. PIN (only via PIN debit transactions) entry allows for a real-time security layer at the POS by blocking transactions that do not confirm the verifiable PIN. *Signature verification (for both credit and signature debit transactions) does not have a real-time authentication layer*, and primarily supports issuers in reviewing fraud claims after fraud has occurred. Authentication layers can generally be categorized as ‘What-You-Know’ and ‘What-You-Have.’ In the case of a plastic card transaction, ‘What-You-Know’ authentication layer would be the consumer signature or PIN; the ‘What-You-Have’ authentication layer would simply be information obtained from the cardholder’s plastic card.

*Table 1: Plastic Card Transaction Authentication Options*

<i>What You Have</i>	<i>What You Know</i>
Plastic Card	Signature PIN

The cardholder experience is seamless with plastic card transactions. However, there is minimal authentication. The capabilities of mobile payments bring increased security capabilities that not only can decrease fraud for all participants in the payments ecosystem, but also still provide a seamless cardholder experience.

### **Mobile Wallet Payment Transactions**

Mobile payment technology is developing rapidly as a number of innovative payment models have emerged. Merchants have recently begun to accept mobile payment transactions, but the ubiquity of mobile payment acceptance is developing slowly. Like plastic cards, the security and convenience inherent to mobile payment transactions is a result of the transmission technology, credential storage capabilities, and authentication procedures rooted in the device and wallet software.

**Transmission Technology** - Mobile wallets transmit cardholder information to the merchant POS through radio frequencies, barcode scanners, or the Cloud. Future mobile wallet implementations may leverage additional transmission technologies such as Wi-Fi, ultra-sonic audio, and magnetic secure transmission. Near Field Communication (NFC) and Bluetooth low energy are the two proximity-based radio frequencies currently in market that wallet providers may utilize. NFC is a radio communication specification that communicates with a contactless reader installed at the POS. Bluetooth low energy is another proximity-based radio communication technology that allows information to be exchanged between a consumer and a merchant. Bluetooth technology has a larger range, communicating information up to 30 feet, where NFC frequencies are generally limited to only a few inches of range.

Barcodes represent another proximity-based information transmission mechanism that mobile wallets may use to communicate cardholder information to a merchant POS. Barcode technology allows merchants and mobile wallets to communicate in one of two ways: In one case, the merchant POS can act as the barcode reader while the mobile device provides a barcode representing a cardholder’s payment credentials (which can be tokenized); conversely, the merchant can also generate a barcode representing the transaction detail, and the consumer’s mobile device can read the transaction detail utilizing the camera installed on the consumer’s smartphone. In the former case, the transaction is initiated through the merchant’s POS similar to a traditional card-based transaction. In the latter case, the transaction is initiated through the consumer’s mobile device to the merchant through the cloud, utilizing internet infrastructure similar to an e-commerce transaction.

**Credential Storage** - Mobile wallets can store consumer payment credentials on the mobile device or digitally in the cloud. Wallets that utilize barcode technology store payment credentials in the cloud. Today, cloud storage is protected by the requirements of PCI-DSS, protecting data at rest and in transit, and vendors that have this model must adhere to these requirements, guidelines, and certifications.

Wallets that communicate payment credentials via radio frequencies like NFC and Bluetooth can store payment credentials on the mobile device or in the cloud; NFC wallets in market have used both methods for storing payment credentials. For example, the Isis wallet stores payment credentials securely on the mobile device in a tamper-proof secured hardware module equivalent to that required in PCI PA-DSS acceptance on the terminals that store secured information similar to keys in the traditional payment ecosystem. The latest version of Google Wallet stores payment credentials on Google’s servers. Bluetooth low energy wallets have only utilized cloud-based credential storage to date (PayPal Beacon).

NFC wallets that store actual (as opposed to tokenized or encrypted) payment credentials on the mobile device must utilize the mobile device’s secure element. The secure element is a secure environment within a physical smart chip hardware on the device where information can be encrypted and stored.

Although the general standard for NFC wallets is to store payment credentials securely on the mobile device (e.g., ISIS example noted above), there are some forms of wallets that store payment credentials in the cloud using Host Card Emulation (HCE) technology. Host Card Emulation is a virtual representation of a physical smart chip using software. Host Card Emulation is quickly becoming a major topic in mobile payments, particularly since MasterCard and Visa added support for the technology. Visa is using HCE to support Visa PayWave contactless payments from smartphones, while MasterCard plans to publish an HCE specification developed with Capital One and Banco Sabadell. Since HCE allows mobile apps to bypass the phone's secure element to make Near Field Communication payments, the technology is seen as a way to allow non-carriers to build mobile payment programs and thus opens the door for cloud-based credential storage for NFC-enabled smartphones.

Many mobile wallets also use tokenization as a security feature when communicating cardholder information to the merchant. Tokenization masks cardholder information by providing a proxy set of characters to mask the cardholder's true card information. The primary difference with the existing tokenization and encryption services offered today for plastic card transactions, and those offered via mobile, is that the plastic card must be swiped and at that moment the actual card number passes to a third-party before tokenization and/or encryption of the card data takes place (though there are exceptions today with certain online wallets such as V.me). However, with most mobile wallet implementations, tokenization occurs at the wallet level and merchants can accept card payments without obtaining the cardholder's actual 16-digit payment information. Again, there are exceptions to this, as there are many different flavors of tokenization and encryption services in the market. This process limits merchant's exposure to data theft and subsequent fraud, as actual payment card information is never physically in possession of the merchant. If a merchant was to have a data breach, fraudsters would only gain access to one-time payment tokens that are no longer proxies for cardholder information. Though it is too early to tell how the recent Visa and MasterCard's announcement of tokenization standards for mobile and on-line transactions will interplay with existing

## Electronic Transactions Association - Processor Council

### Better Security Through Mobile – “The One-Two Punch” – Industry Best Practices

tokenization and encryption products and services in the market, it certainly provides further evidence that players in the industry are focusing a lot of attention on security of mobile.

**Authentication Methods** - Mobile wallet software can utilize *multiple* innovative authentication layers to provide robust security for cardholders, each of which can be more secure than a traditional plastic card with an unencrypted magnetic stripe. These layers help confirm that the cardholder has supplied proper credentials to authorize each payment. The most common authorization layer is a password requirement. Passwords are most commonly in the form of PIN entry, but other methods exist such as a fingerprint scan (e.g., Apple iTunes payment). In other cases, a merchant can confirm the consumer’s identity visually. Wallet software can communicate with the merchant via geolocation or Bluetooth and provide a picture of the actual cardholder for visual authentication. Many of the authentication measures developed by wallet providers are applied in multiple layers, meaning that multiple safeguards can be put in place to mitigate the risks of unauthorized access. These multiple layers provide new measures to confirm the cardholder is authorized by confirming both ‘what you have’ and ‘what you know’ through advanced means.

Table 2: Wallet Technology Examples

Transmission Technology	Credential Storage	Example Authentication Methods		Example Wallet Providers
		What You Have	What You Know	
NFC	Secure Element	Phone	Consumer Passcode	Isis, Google Wallet 1.0
NFC	Cloud	Phone	Consumer Passcode	Google Wallet 2.0
Bluetooth low energy	Cloud	Phone	Merchant Photo Authentication	PayPal Beacon
Barcode <i>Merchant reads card information</i>	Cloud	Phone	Consumer Passcode	LevelUp, Starbucks
Barcode <i>Wallet reads trans. Information</i>	Cloud	Phone	Consumer Passcode	Paydiant

Mobile wallet implementations may also use “who you are” authentication methods by integrating biometric capture mechanisms into payment authentication. These authentication

methods do not exist in the traditional plastic card ecosystem and are new ways to secure payment transactions enabled by Mobile solutions.

### Mobile Wallet Payment Transaction Models

Payments transactions that originate from the mobile device can occur through a number of models and can utilize a variety of the previously discussed transmission technologies, credential storage techniques, and authorization methods to facilitate a secure transaction between the consumer and the merchant point of sale.

**Mobile Model (1): NFC with Secure Element Flow at POS with Physical Entry** - One of the more popular mobile wallet models today utilizes Near Field Communication (NFC), as found in wallet products such as ISIS and the first generation Google Wallet.

**Transmission Technology** – The payment card information is received via radio transmission by the merchant at the POS. Later versions of this wallet model (Google Wallet 2.0) have emerged to circumvent the physical secure element in favor of a virtual secure element; this is known as Host Card Emulation (HCE).

**Credential Storage** - Consumer payment credentials are stored in the Secure Element embedded in the mobile device that the consumer carries (the phone). As compared to plastic cards, where the payment credentials are stored on the magnetic stripe and is unencrypted, NFC with Secure Element at the POS with physical entry *keeps the payment credentials encrypted*, thus making skimming, data theft, and subsequent fraud more difficult.

# Electronic Transactions Association - Processor Council

## Better Security Through Mobile – “The One-Two Punch” – Industry Best Practices

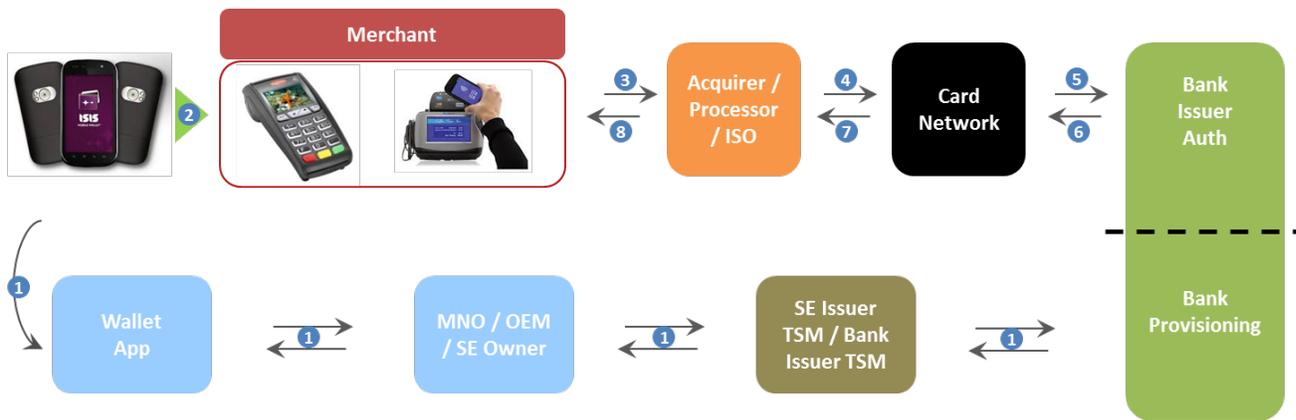
**Authentication** - Unlike the majority of plastic card transactions which have minimal authentication measures (e.g., signature), transactions using NFC with Secure Element at POS with Physical Entry have *multiple authentication options*, including:

Table 3: NFC with Secure Element Flow at POS with Physical Entry Authentication Options

What You Have	What You Know
Phone	Password for the device/phone
E-Mail verification	Password for the mobile wallet
SMS verification	
Phone number validation	
Geolocation of device	
Biometrics	
Device fingerprinting	
Verification of device black-listing	

Common, Emerging, and Other authentication option.

Figure 1: NFC with Secure Element Flow at POS with Physical Entry



Mobile Wallet Examples:



1. Consumer Initiates Loads Wallet with Payment Credential
2. Consumer presents wallet at POS
3. Merchant POS (Terminal, Integrated POS, Gateway, Merchant Host) sends transaction to Acquirer
4. Acquirer sends transaction to Card Network
5. Card Network sends transaction to Issuer
6. Issuer returns authorization or decline to Card Network
7. Card Network returns auth/decline to Acquirer
8. Acquirer returns auth/decline to merchant to complete consumer purchase

**Mobile Model (2): Cloud Flow at POS with Physical Interaction** – Another popular wallet model requires that the consumer present information to the merchant from a cloud-based wallet. Popular wallets with cloud flow at the POS with physical entry include Square Wallet and LevelUp.

**Transmission Technology** – This consumer/merchant *transaction point can occur directly at the POS via barcode scanners (typically categorized as physical entry) or through the cloud (cloud interaction)*. These wallets provide encrypted account information to the merchant via barcode. These wallet providers act as the merchant of record. As a result of this model, the actual payment originates from the wallet server in the cloud, and is therefore is qualified as a card-not-present transaction.

**Credential Storage** - The payment credentials are stored in the cloud and the security is governed by PCI-DSS compliance, protecting data in transit and at rest. As compared to plastic cards, where payment credentials are stored on the magnetic stripe and not encrypted, cloud flow at the POS with physical entry *keeps the payment credentials encrypted*, thus making skimming or other theft of credentials more difficult. Initial loading and validation of credentials into storage are the major area of concern, but methods for securing this “issuance” of the credential have been proposed by industry groups such as The Clearing House Secure Cloud and Visa Tokenization.

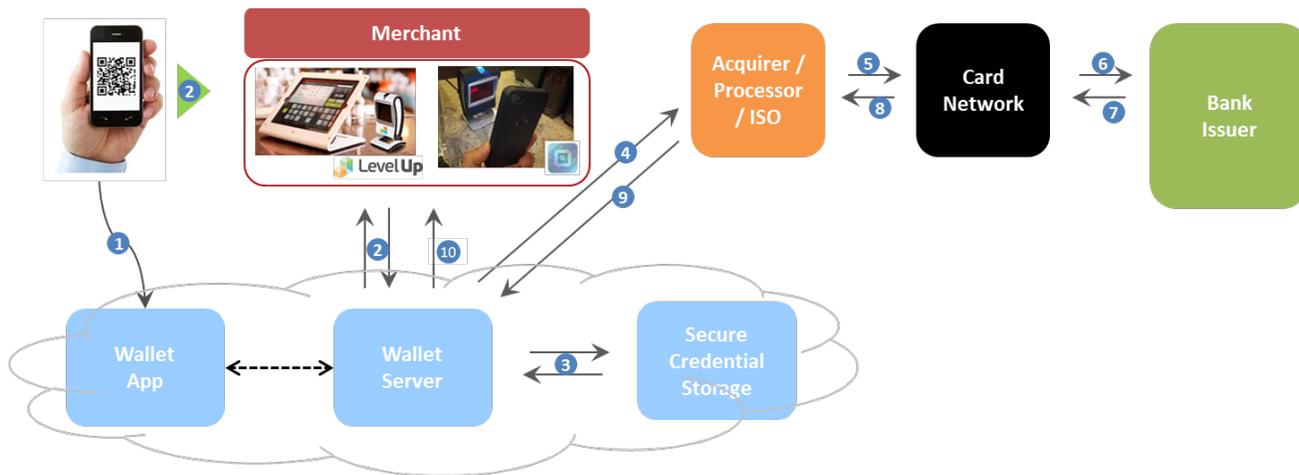
**Authentication** - Unlike the majority of plastic card transactions which have fixed authentication measures (e.g., signature), transactions using Cloud Flow at POS with Physical Entry have *multiple authentication options*, including:

Table 4: Cloud Flow at POS with Physical Interaction Authentication Options

What You Have	What You Know
Phone	Password for the device/phone
E-Mail verification	Password for the mobile wallet
SMS verification	
Phone number validation	
Geolocation of device	
SIM Card validation	
Biometrics	
Device fingerprinting	
Verification of device black-listing	

Common, Emerging, and Other authentication option

Figure 2: Cloud Flow at POS with Physical Entry



1. Consumer Loads Wallet with Payment Credential
2. Consumer presents wallet at POS
3. Wallet correlates consumer to underlying Payment Card
4. Wallet provider takes over as Merchant of Record and sends transaction to acquirer
5. Acquirer sends transaction to Card Network
6. Card Network sends transaction to Issuer
7. Issuer returns authorization or decline to Card Network
8. Card Network returns auth/decline to Acquirer
9. Acquirer returns auth/decline to wallet provider acting as Merchant of Record
10. Wallet provider returns auth/decline to merchant to complete consumer purchase

Examples:



**Mobile Model (3): Cloud Flow at POS with Cloud Interaction** – The other cloud-based wallet model involves a completely cloud-oriented interaction model between the wallet and the merchant, even though the customer is present in the store. Wallet providers such as Paydiant and PayPal Beacon utilize this model.

**Transmission Technology** – Wallets that utilize this model employ multiple technologies available on the mobile device to confirm the consumer’s proximity to the POS and willingness to make a purchase. These technologies can include Bluetooth, barcodes, geo-location and/or a combination of these and other technologies. This communication takes place wholly in the cloud and the flow of information most resembles a traditional e-commerce transaction - though the wallet holder has been confirmed by the merchant to be in the store. This consumer/merchant *transaction point occurs through the cloud*. These wallets provide encrypted account information to the merchant via the cloud. In this scenario, the wallet provider acts as the merchant of record.

**Credential Storage** - The payment credentials are stored in the cloud and the security is governed by PCI-DSS compliance, protecting data in transit and at rest. As compared to plastic cards, where the payment credentials are stored on the unencrypted magnetic stripe, Cloud Flow at the POS with Cloud Interaction *keeps the payment credentials encrypted*, thus making data theft more difficult. Initial loading and validation of credentials into storage are the major area of concern, but methods for securing this “issuance” of the credential have been proposed by industry groups such as The Clearing House Secure Cloud and Visa Tokenization.

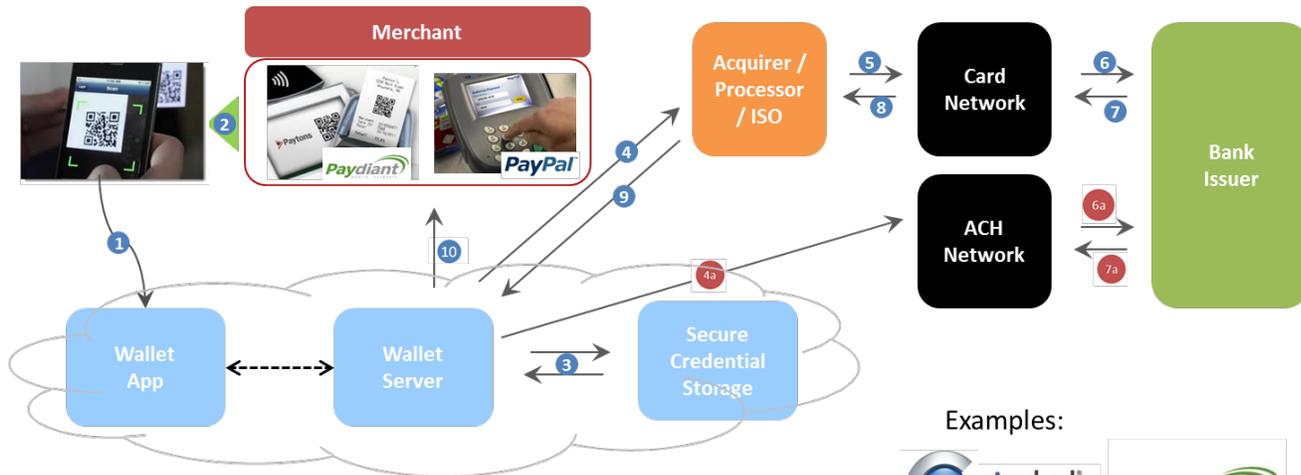
**Authentication** - Unlike the majority of plastic card transactions which have fixed authentication measures (e.g., signature), transactions under the Cloud Flow at POS with Cloud Interaction have *multiple authentication options*, including:

Table 5: Cloud Flow at POS with Cloud Interaction Authentication Options

What You Have	What You Know
Phone	Password for the device/phone
E-Mail verification	Password for the mobile wallet
SMS verification	
Phone number validation	
Geolocation of device	
SIM Card validation	
Biometrics	
Device fingerprinting	
Verification of device black-listing	

*Common, Emerging, and Other authentication option*

Figure 3: Cloud Flow at POS with Cloud Interaction



1. Consumer Loads Wallet with Payment Credential
  2. Consumer scans QR code generated by merchant POS
  3. Wallet correlates consumer to underlying Payment Card
  4. Wallet provider submits transaction on behalf of merchant and sends transaction to acquirer
  5. Acquirer sends transaction to Card Network
  6. Card Network sends transaction to Issuer
  7. Issuer returns authorization or decline to Card Network
  8. Card Network returns auth/decline to Acquirer
  9. Acquirer returns auth/decline to wallet provider who submitted transaction on behalf of Merchant
  10. Wallet provider returns auth/decline to merchant via software link to complete consumer purchase
- Note: Steps 4a, 6a, 7a are applicable to PayPal and ACH transactions*

Examples:



In both physical and cloud-based entry models, mobile wallet transactions at the POS and physical/cloud interaction confirm that the cardholder is present, with added security measures and verification layers such as user passcodes, geo-location, and other advanced tools. These measures provide similar assurances of a card-present transaction, with the added security layers that the mobile device is uniquely capable of, thereby providing more protection than plastic cards at the POS.

**Mobile Model (4): Cloud Flow for Online Card Not Present** – This transaction model resembles a legacy eCommerce transaction. In this scenario, the wallet is on a different consumer device (e.g., the laptop as opposed to the phone). There are several mobile / digital wallet examples in the market today including solutions by iTunes, Amazon.com, V.me by Visa, PayPass by MasterCard, and PayPal.

**Transmission Technology** – Wallets that utilize this model are not located in the proximity of the POS (though they could be if the consumer is shopping from a device within the physical store). The communication takes place wholly in the cloud whereby the wallet provides encrypted account information to the merchant via the cloud. In contrast to a legacy eCommerce transaction, the wallet provider acts as the merchant of record. Since these are eCommerce transactions, the Card Networks qualify them as card-not-present transactions.

**Credential Storage** - The payment credentials are stored in the cloud and the security is governed by PCI-DSS compliance, protecting data in transit and at rest. As compared to plastic cards, where the payment credentials are stored on an unencrypted magnetic stripe, Cloud Flow for Online Card Not Present *keeps the payment credentials encrypted*, thus making skimming, data theft, and subsequent fraud more difficult. Initial loading and validation of credentials into storage are the major area of concern, but methods for securing this “issuance” of the credential have been proposed by industry groups such as The Clearing House Secure Cloud and Visa Tokenization.

**Authentication** - Unlike the majority of plastic card transactions which have fixed authentication measures (e.g., signature), transactions under the Cloud Flow for Online Card Not Present have *multiple authentication options*, including:

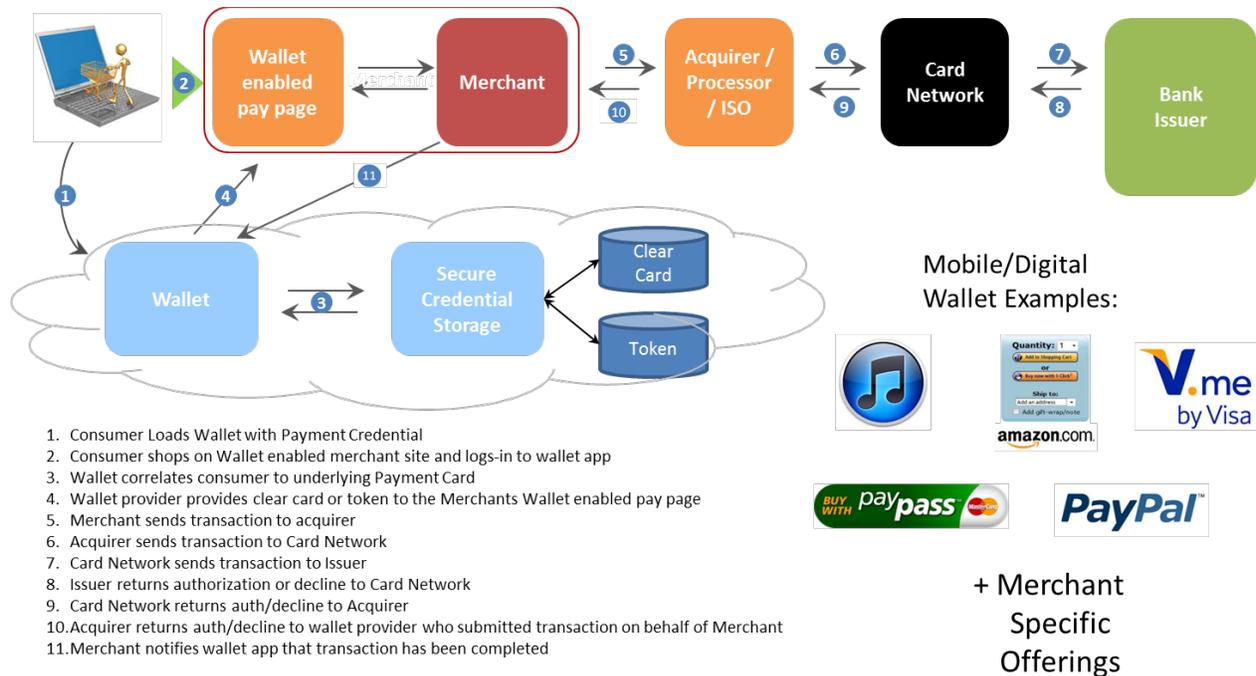
Table 6: Cloud Flow for Online Card Not Present Authentication Options

What You Have	What You Know
Phone	Password for the device/phone
E-Mail verification	Password for the mobile wallet
SMS verification	
Phone number validation	
IP verification	
Geolocation of device	
SIM Card validation	
Biometrics	
Device fingerprinting	
Verification of device black-listing	

*Common, Emerging, and Other authentication option*

Additionally, mobile adds more security to these types of transactions compared to traditional eCommerce due to authentication options such as SMS, Device Fingerprinting, Geolocation, Biometrics, SIM Card Verification, and Black Listing.

Figure 4: Cloud Flow for Online Card Not Present



Today’s authentication and fraud tools for online transactions provide a more robust level of security compared to plastic card transactions at the POS.

### Summary: Plastic vs. Mobile

The mobile transaction lifecycle has similarities and differences when compared to plastic card transactions. From an infrastructure standpoint, transactions that occur via the mobile device largely rely on the same network rails that exist in plastic card transactions. The primary difference between the two transaction types lies within the transmission technology, credential storage, and the authentication procedures that occur at the POS. Magnetic stripe cards provide the lowest levels of security at the POS as unencrypted credentials are embedded physically onto the plastic card. EMV cards that utilize smart chips provide a level of security above plastic cards yet are not to the level of mobile wallets as payment credentials are encrypted and most implementations require a PIN passcode to authorize each transaction, unlike EMV. Although EMV cards have reliably lowered fraud rates in contact transactions at physical brick-and-mortar stores, as evident by the results reported from multiple countries

having transitioned to the technology specification (e.g., Canada, U.K., and Brazil) for the majority of its card-based transactions, the upcoming US roll-out is not completely similar. For example, the Visa and American Express implementation of EMV in the US will be Chip and Choice (e.g., PIN or Signature). Thus, if a cardholder uses a PIN today for a transaction with Debit, then the cardholder will use a PIN under EMV Debit. If a cardholder uses Signature on a transaction today with Credit, then the cardholder would use a Signature with EMV Credit (no PIN here). The US industry does not gain PIN authentication for most cases of EMV under the current structure unless the Issuers all opt to provide only the PIN option to their cardholders. EMV protects against replication, but does not solve for eCommerce or lost/stolen card fraud (without PIN and only Signature-based transactions). Mobile wallet technology provides encryption technology, PIN/password entry and numerous other aforementioned security technologies to protect payment credentials.

Mobile can provide more security than traditional magnetic stripe cards and EMV as mobile combines the technologies that can lead to a powerful security solution of EMV, tokenization, and E2EE. Mobile also adds to new layers of authentication that are not easily managed or addressed in a physical-card ecosystem.

The most distinct difference in transaction security lays in the authentication features available in mobile wallets. Mobile wallets that leverage cutting edge authentication features can heighten the degree in which payments can be attributed to the authorized consumer. *It is evident that magnetic stripe cards can have less secure credential storage capabilities and limited authentication measures compared to mobile wallets as depicted below.*

## Electronic Transactions Association - Processor Council

### Better Security Through Mobile – “The One-Two Punch” – Industry Best Practices

Table 7: Transaction Elements Cards and Wallets

	Payment Type	Transmission Technology	Credential Storage	Authentication Options	
				What You Have	What You Know
Plastic Card	Mag-Stripe Card at POS	Magnetic strip	- Not encrypted - On device	Plastic Card	- Signature - PIN
	Mag-Stripe Card Online	Cloud	- Encrypted - In the cloud	Not required	- Card Number - AVS, CVV2 Number
	EMV Card	Smart Chip	- Encrypted (though it is a cryptogram with PAN text) - On device	Plastic Card	- Signature - PIN
Mobile	Mobile - NFC Wallet	Radio Frequency	- Encrypted - In the cloud	- Phone/device - Biometrics - Geolocation - Visual ID confirmation	- Passcode for device - Passcode for mobile wallet
	Mobile Barcode Wallet	Dynamic Barcode	- Encrypted - In the cloud	- Phone/device - Biometrics - Geolocation - Visual ID confirmation	- Passcode for device - Passcode for mobile wallet

*Green=Advanced or Better; Red=Less Advanced or Basic*

## Security Best Practices

Smartphones are uniquely capable of confirming that the consumer is making an authentic transaction by being able to verify ‘what you have’ and ‘what you know’ information beyond the means that are available in plastic cards. When ‘What-You-Have’ and ‘What-You-Know’ verification methods are applied in layers it becomes very difficult for fraudsters to steal credentials and conduct fraudulent transactions. For example, if a fraudster was to obtain a plastic card, they would have the basic credentials necessary to authorize a transaction. On the other hand, if a smartphone were illicitly obtained, a fraudster would need to overcome multiple verification layers at the POS to authorize the payment. In the case of some emerging technologies like biometrics, compromising authentication becomes increasingly difficult.

Additionally, studies of time recognition by the cardholder of when a phone is lost vs. a plastic card indicate a cardholder will generally notice his/her phone as missing within minutes compared to a plastic card which may be days or weeks. The ability to deactivate the payment vehicle within such a short time span will materially decrease the ability for fraudsters time to utilize the payment vehicle and will thus decrease the dollar amount of fraud.

Though mobile wallet models are still developing, service providers have begun to coalesce around certain best practices in offering advanced security. ***A security best practice is for a mobile transaction to require that the user provide at three of the options for authentication – for example at least two ‘What-You-Have’ verification layers and at least one ‘What-You-Know’ verification layer, or alternatively, at least one “What-You-Have’ and at least two ‘What-You-Know’ verification layers. In essence, a “one-two punch”.*** This is attributable to the fact that information about ‘What-You-Know’ and ‘What-You-Have’ are typically not physically stored together and therefore harder to illicitly collect.

Table 8: The “One-Two Punch” Authentication Best Practices

What You Have	What You Know
Phone	Password for the device/phone
E-Mail verification	Password for the mobile wallet
SMS verification	
Phone number validation	
IP verification	
Geolocation of device	
SIM Card validation	
Biometrics	
Device fingerprinting	
Verification of device black-listing	

## Conclusion

Mobile wallets that enable cardholder payments at the POS provide security features that can mitigate fraud risks in excess of plastic cards. Mobile wallets do so by utilizing communication technology, credential storage techniques, and authentication procedures that are more advanced than those that exist on today’s plastic payment cards, including EMV, when used at the POS. Mobile can provide more security than traditional plastic cards and EMV as mobile combines the technologies that can lead to a powerful security solution of EMV, tokenization, and E2EE. Even if EMV is not included in Cloud-based payments, tokenization and E2EE in combination with PCI-DSS best practices can be a more secure solution than magnetic stripe-based plastic cards.

The risks involved in certain plastic card transactions might not exist in many mobile wallet transaction models today because the wallet is physically present and can be validated at the merchant location (or, the cardholder is physically present). Additionally, mobile wallets utilize the cloud and technology uniquely inherent to smartphones to communicate with merchants in more advanced and sophisticated ways than traditional plastic card or e-commerce transactions, and often can provide more robust authentication to those available in plastic magnetic-stripe cards.

***In order to capitalize on the sophisticated technological capabilities of mobile devices, and ensure security for consumers and other parties across the payments ecosystem, requiring multiple authentication measures is a best practice for the industry.***

### Glossary of Terms

Term	Definition
<b>Acceptance</b>	A generic term for the acceptance of payment types including card schemes, mobile, check, prepaid or other alternative payments.
<b>Advertising</b>	The activity of attracting public attention to a product or business, as by paid announcements in the print, broadcast, or electronic media.
<b>Application</b>	A broad term used to describe specially designed software used for a specific task on networked devices.
<b>Application Provider</b>	The entity that provides the technology platform for common short code service applications.
<b>ARPU (Average Revenue Per User)</b>	The revenue generated by a single customer or unit, typically on a monthly basis. ARPU = total revenue / number of subscribers.
<b>Audio Jack Card Reader</b>	A mobile phone credit card reader when plugged in to your mobile phone’s audio jack lets you accept credit and debit cards in real-time on your mobile device.
<b>Authentication</b>	A security mechanism for verifying: 1) the identity of an individual or other entity; and 2) the level of authority of that person or entity (i.e., the ability of that person or entity to perform specific tasks or activities).
<b>Barcode</b>	An optical machine-readable representation of data relating to the object to which it is attached.
<b>Bluetooth</b>	Wireless protocol using short-range communications technology to facilitate transmission of data over short distances.
<b>Bluetooth Card Reader</b>	Lightweight reader that enables controlled access to mobile devices using Bluetooth technology.
<b>Cardholder Data</b>	At a minimum, cardholder data consists of the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date, and / or service code.
<b>Chip</b>	A small piece of semiconducting material (usually silicon) on which an integrated circuit is embedded (i.e., a computer chip embedded in the smartcard).
<b>Closed-Loop Card / Application</b>	A system that has up to three parties instead of four where the issuer is also the acquirer and the network.
<b>Cloud Computing</b>	Refers to the “floating” nature of the actual physical location of the server you may be attaching to over the Internet that is hosted “on the cloud”. The virtual server you access may be in LA one day and in Hong Kong the next in a cloud model. The server is instantiated anywhere there is space and processing power sometimes. So in that way, assets you connect to actually seem to float over the face of the earth, like a cloud.
<b>Cloud-Based Payments</b>	Payment technology that stores payment credentials in the cloud (not locally on a device) so that users can make purchases.

## Electronic Transactions Association - Processor Council

### Better Security Through Mobile – “The One-Two Punch” – Industry Best Practices

Term	Definition
<b>Contactless</b>	A family of proximity-based wireless technologies with that enable payment transactions via chips embedded in payment cards, tags, key fobs and mobile phones.
<b>Conversion</b>	The desired change in behavior of a user from one use, function, or purpose to another.
<b>Conversion Rate</b>	The number of visitors performing the desired action, whether the action is buying a product, filling out a form, or some other goal of the web page divided by the total number of visitors.
<b>Coupon</b>	A ticket or document that can be exchanged for a financial discount or rebate when purchasing a product.
<b>CPA</b>	Online advertising payment model where the advertiser pays for each specified action (a purchase, a form submission, etc.) linked to the advertisement.
<b>CPM (Cost Per Thousand Impressions)</b>	term used in online advertising and marketing related to web traffic. It refers to the cost of internet marketing campaigns where advertisers pay for every time their ad is displayed, usually in the form of a banner ad on a website or e-mail.
<b>Cramming</b>	A form of fraud in which small charges are added to a bill by a third party without the subscriber’s consent or disclosure. These may be disguised as a tax or some other common fee, and may be several dollars or even just a few cents. The crammer’s intent is that the subscriber will overlook and ultimately pay these small charges.
<b>CRM (Customer Relationship Management)</b>	All aspects of interaction a company has with its customer, whether it is sales or service-related.
<b>Developer</b>	An individual who writes computer programs to meet specific requirements. The term often implies involvement with, or responsibility for, requirements capture and testing.
<b>Digital Good</b>	A broad term to describe any good that is stored, delivered, and used in electronic format.
<b>Digital Wallet</b>	A method of storing various forms of personal data (i.e., bank accounts, credit cards, driver’s license, other forms of ID) on a mobile or other electronic device to enable electronic commerce transactions quickly and securely.
<b>Direct Carrier Billing</b>	Also known as “direct operator billing” is the ability to purchase goods and services and have them charged directly to a user’s mobile bill or account.
<b>Display Ads</b>	A type of advertising that typically contains text (i.e., copy), logos images, etc. Online, the advertising appears on web pages in many forms, including web banners.

## Electronic Transactions Association - Processor Council

### Better Security Through Mobile – “The One-Two Punch” – Industry Best Practices

Term	Definition
<b>Dongle</b>	In the mobile and payments space, used interchangeably as a magstripe reader when plugged in to the mobile device; in the technology space, it is a small piece of hardware that plugs into an electrical connector on a computer and serves as an electronic “key” for a piece of software; the program will run only when the dongle is plugged in.
<b>E2EE</b>	End-to-end encryption (E2EE) is a digital communications paradigm of uninterrupted protection of data traveling between two communicating parties. It involves the originating party encrypting data to be readable only by the intended recipient, and the receiving party decrypting it, with no involvement in said encryption by third parties. The intention of end-to-end encryption is to prevent intermediaries, such as Internet providers or application service providers, from being able to discover or tamper with the content of communications. End-to-end encryption generally includes protections of both confidentiality and integrity.
<b>EMV (Europay, MasterCard and Visa)</b>	A global standard for inter-operation of integrated circuit cards (IC cards or “chip cards”) and IC card capable point of sale (POS) terminals and automated teller machines (ATMs), for authenticating credit and debit card transactions.
<b>Encoding</b>	A code that pairs each character from a given repertoire with something else — such as a bit pattern, sequence of natural numbers, octets, or electrical pulses — in order to facilitate the transmission of data (generally numbers or text) through telecommunication networks or for data storage.
<b>Encryption</b>	The process of encoding messages (in the payments industry, encryption typically refers to the use of an industry standard (vetted) encryption algorithm such as 3DES, AES, etc.) which is reversible encoding to all who have the secret key to do so.
<b>End User</b>	Another term for wireless subscriber or consumer, end users are people and / or entities that utilize short codes for communication with applications.
<b>Face To Face</b>	Payments or transactions made in person, instead of by intermediary like MOTO or e-commerce. Payments in store are made “face to face.”
<b>Factoring</b>	When a merchant processes sales through his or her merchant account on behalf of another merchant.
<b>Feature Phone</b>	A simple cellular phone that is generally used to make calls and send text messages (SMS). A feature phone lacks the advanced capabilities such as e-mail, GPS, calendaring, and Internet browsing often found on “smartphones”.
<b>Gateway / Payment Gateway</b>	A payment gateway is a combination of hardware and software that provides merchants with the ability to perform authorizations from a website over the Internet. It’s the link between a merchant website and the processor.
<b>Geo Fence</b>	A virtual perimeter for a real-world geographic area.

## Electronic Transactions Association - Processor Council

### Better Security Through Mobile – “The One-Two Punch” – Industry Best Practices

Term	Definition
<b>Geolocation</b>	The identification of the real-world geographic location of an object, such as a radar, mobile phone or an Internet-connected computer terminal.
<b>In-App Billing</b>	Billing for content or services purchased from within a native mobile application.
<b>Loyalty Program</b>	Structured marketing efforts that reward, and therefore encourage, repeat buying behavior — behavior which is potentially beneficial to the firm.
<b>Marketing</b>	The activity and processes for creating, communicating, delivering, and exchanging offerings that have value for customers, clients, partners, and society at large.
<b>Merchant</b>	A person or company engaged in the purchase and sale of digital, virtual, or solid goods for profit.
<b>Merchant Aggregation</b>	Multiple merchants and their transactions are lumped together in one master merchant account.
<b>Merchant App</b>	Allows merchants to accept payments via a customer’s mobile device.
<b>Micropayment</b>	A transaction involving a very small sum of money in exchange for goods.
<b>MO</b>	A mobile-originated message, meaning an SMS or text message sent from a mobile phone. These messages are sent by a mobile subscriber by creating and sending the message from within their mobile phone.
<b>Mobile Acceptance / Mobile Payment Acceptance</b>	A smartphone payment application that enables a merchant to accept and process card payments.
<b>Mobile Banking</b>	The act of performing balance checks, account transactions, payments, credit applications and other banking transactions through a mobile device.
<b>Mobile Check-In</b>	The ability for consumers to “check-in” at a business using their smartphone, allowing them to keep the people in their social network constantly apprised of their whereabouts.
<b>Mobile Commerce / mCommerce</b>	This is the overarching term encompassing mobile payments, mobile loyalty, mobile marketing, mobile gifting, mobile purchasing, mobile payment acceptance, mobile e-commerce & other related activities performed around commerce by a consumer at a merchant store or while they are “on-the-go”.
<b>Mobile Coupon / Offer</b>	A discount offer sent to your mobile device, redeemable at the merchant cash register directly from the phone.

## Electronic Transactions Association - Processor Council

### Better Security Through Mobile – “The One-Two Punch” – Industry Best Practices

Term	Definition
<b>Mobile Gift</b>	Typically leveraged in reference to mobile gift cards, but can also reference the act of gifting a product via a mobile device. This action will leverage social, personal and other contact networks of the consumer to facilitate digital communication and delivery of a purchased product to another consumer.
<b>Mobile Loyalty</b>	A large variety of services that can be implemented within a mobile application. This can include storing loyalty cards in a mobile application, implementing a loyalty program based on activities executed on a mobile device, coupons, offers, vouchers or promotions (all different by definition) and more. The objective of the Mobile Loyalty bucket is to include anything that will drive consumer loyalty to a brand through implementation of a program that provides some benefit back to the consumer.
<b>Mobile Marketing</b>	A form of marketing that generally uses SMS, MMS or WAP Push to deliver its promotion to mobile phones or other mobile devices. Like outdoor, print or interactive marketing, mobile marketing is simply another push tactic marketers can use to reach a target audience. Examples include banners or in-app marketing.
<b>Mobile Payment</b>	A point of sale (POS) payment made through a mobile connected device.
<b>Mobile Payment Acceptance</b>	A smartphone payment application that enables you to accept and process card payments anywhere your business takes you.
<b>Mobile Payment Apps</b>	This is a generic term that can be leveraged as payment accepting or payment making applications. This is a wide bucket that includes any application that can allow you to accept or make payments in-store, online or remotely such as through remittance.
<b>Mobile POS (mPOS)</b>	Mobile Point of Sale (POS) references the act of turning a mobile device into a payment acceptance device through the addition of software and / or hardware to process a key entered, card swiped or card dipped (EMV) transaction with appropriate related risk-based transaction fees.
<b>Mobile Store</b>	Also known as a Mobile Storefront, this is the act of replicating an in-store or online commerce experience within a mobile application. You can browse a product catalog, load your loyalty, payment and coupon data, purchase items, interact with customer support representatives, etc., through a mobile application or mobile-web enabled service.
<b>Mobile Wallet</b>	An electronic account / storage locker accessible from a mobile device that can be used to store user payment information such as existing credit and debit cards and pay merchants.
<b>Mobile Wallet Apps</b>	Enables payment services on a smartphone.
<b>Mobile Web</b>	Access to the world wide web, i.e., the use of browser-based Internet services, from a handheld mobile device, such as a smartphone.

## Electronic Transactions Association - Processor Council

### Better Security Through Mobile – “The One-Two Punch” – Industry Best Practices

Term	Definition
<b>MT</b>	A mobile-terminated message, meaning an SMS or text message terminated on (was sent to) a mobile phone. The message may have originated from another mobile phone or from a web server, PC or other fixed device.
<b>NFC (Near Field Communication)</b>	A short-range wireless RFID technology which uses magnetic field induction to enable communication between devices by close proximity. Card accounts are linked to contactless NFC chips in mobile devices.
<b>NFC Peer-to-Peer (P2P) Protocol</b>	This is an open protocol defined by ISO 18092 that is included in the complete implementation of a near field communication (NFC) device. The three protocols of NFC include reader / writer mode, card emulation and peer-to-peer. This protocol is considered “open” as it is not strictly enforced in the payments world by the card schemes like the applets of PayWave, PayPass, Zip and ExpressPay. Other services involving Bluetooth / wireless pairing, media sharing, business card sharing, etc., are used by phone manufacturers.
<b>Open-Loop Card / Application</b>	A system wherein general purpose cards that carry the American Express, Discover, MasterCard or Visa logo and can be used where ever those cards are accepted.
<b>Opt-In</b>	A way of collecting mobile and Internet users’ personal data. Within the opt-in context, user acceptance is necessary before any mobile marketing solicitation.
<b>P2P / Peer-to-Peer / Person-to-Person</b>	The practice of lending money to previously unrelated individuals or “peers” without the intermediation of traditional financial institutions (banks). It takes place on online lending platforms that are provided by peer-to-peer lending companies on their websites and is facilitated by credit checking tools of varying complexity. P2P can alternative be used to broadly describe consumer-to-consumer payments between to individuals.
<b>PAN</b>	Acronym for “primary account number” and also referred to as “account number”. Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account.
<b>Parent-Child Account Hierarchy</b>	This is the concept of having a master account and a sub account with variable levels of permission of the master account. This concept is also a basic structure of object-oriented programming, but the concept remains the same in programming or banking reference. The parent will have full permissions and the child is associated and related to the master account, but will have modified privileges of the parent account.
<b>Payment Processor</b>	A company appointed by a merchant to handle payment transactions for merchant acquiring banks or other financial service institutions.
<b>Payments</b>	The transfer of money from one party (such as a person or company) to another, usually made in exchange for the provision of goods, services or both, or to fulfill a legal obligation.

## Electronic Transactions Association - Processor Council

### Better Security Through Mobile – “The One-Two Punch” – Industry Best Practices

Term	Definition
<b>Point of Sale (POS)</b>	The time and place that a sale takes place. POS also refers to the devices used to transmit the transaction such as card readers connected to smartphone apps.
<b>Point-to-Point Encryption</b>	This is the security functionality of encrypting card data from a single point to another point. Unlike end-to-end encryption, point-to-point encryption may not fully encrypt card or other secure data throughout the entire transaction of a merchant system, but instead from a point of acceptance to a specific device layer within a merchant network.
<b>Promotions</b>	This is a marketing term leveraged when a merchant is looking to upsell a current product or solution. In some cases, this is used as a contrast to an offer, discount or coupon, where a merchant is not providing a financial incentive to buy a single good, but instead advertising a specific product at market price or in a bundled price to create additional value. Restaurants may call this a feature of the menu.
<b>PSMS (Premium Short Message Service)</b>	This offers the ability to purchase or subscribe to premium messaging programs, provided by third-party content providers through text messaging.
<b>QR Barcode / 2D Barcode</b>	A barcode is an optical machine-readable representation of data relating to the object to which it is attached. 2D barcodes are two dimensional.
<b>RDC (Remote Deposit Capture)</b>	The action of taking a picture of a check and submitting this digital copy as a process of depositing funds from one bank to another through the ACH network.
<b>RFID (Radio Frequency Identification)</b>	The use of a wireless non-contact system that uses radio-frequency electromagnetic fields to transfer data from a tag attached to an object, for the purposes of automatic identification and tracking.
<b>Secure Element</b>	An encrypted tamper-proof smart card chip enabling secure mobile payment transactions.
<b>Settlement</b>	The payment of an outstanding account, invoice, charge. In payment processing, this is the movement of funds from the issuer of the credit card to the merchant from which goods or services were purchased.
<b>Short Code</b>	A special short number used to address SMS and MMS messages from mobile or fixed phones for value-added services such as interactive voting, mobile contributions and purchasing digital content.
<b>Show ‘N Go</b>	A non-electronic transfer of information from a consumer to a merchant through a mobile device. This use case occurs when a consumer presents a static image on their mobile phone to a merchant as an act of showing proof of purchase, redemption of a coupon or other related activity that typically will involve a manual intervention on the merchant side.

## Electronic Transactions Association - Processor Council

### Better Security Through Mobile – “The One-Two Punch” – Industry Best Practices

Term	Definition
<b>Show Rooming</b>	When a customer visits a brick and mortar retail location to touch and feel a product and then goes online or to a low-service big-box retailer to purchase the product at a lower price.
<b>SIM Card</b>	Subscriber Identification Module (SIM) is a memory chip used by some cellular phones. The SIM card can store data such as user identity, location and phone number, network authorization information, personal security keys, personal contact lists and stored text messages. Security features include authentication and encryption. The SIM card can also contain other electronic chips such as a secure element module used to store highly secure information such as electronic payment credentials.
<b>Smartphone</b>	a mobile phone built on a mobile operating system, with more advanced computing capability and connectivity than a feature phone.
<b>SmartTap™</b>	Ability to make a contactless payment by tapping your mobile device (SmartTap is a registered trademark of Isis).
<b>SMS Marketing</b>	A form of mobile marketing that utilizes SMS to deliver its promotion.
<b>Social Advertising</b>	A process for influencing human behavior on a large scale, using marketing principles for the purpose of societal benefit rather than commercial benefit.
<b>Social Mobile Commerce</b>	The ability for merchants to deliver targeted offers and behavior-based promotions to customers.
<b>SSL (Secure Sockets Layer)</b>	A cryptographic protocol that provides a communication security over the Internet.
<b>Store and Forward</b>	A telecommunications technique in which information is sent to an intermediate station where it is kept and sent at a later time to the final destination or to another intermediate station. In payments processing it relates to storing sensitive payment authentication data (like magstripe data) for a period of time until it can be transmitted to a processor for authorization.
<b>Storefront</b>	Electronic or physical location where a merchant can facilitate and promote the sale of goods.
<b>Subscriber’s Mobile Bill</b>	This is a mobile consumer’s bill from their carrier.
<b>Subscription</b>	Items that are sold with a specified, recurring billing interval.
<b>Tap / Tap and Pay</b>	A technology that allows consumers to pay for purchases at a merchant location with a mobile device that is equipped with near field communication (NFC) capabilities.
<b>Tender Steering</b>	The ability for a merchant to provide incentives to customers to use a particular type of card to pay.
<b>Tokenization</b>	The process of breaking a stream of text up into words, phrases, symbols, or other meaningful elements called tokens. In payments, it is the process of exchanging sensitive payment information for a unique identifier (token) that is used in lieu of the payments information.

## Electronic Transactions Association - Processor Council

### Better Security Through Mobile – “The One-Two Punch” – Industry Best Practices

---

Term	Definition
<b>Transaction Aggregation</b>	Combining multiple transactions from a single cardholder and submitting them as one payment.
<b>Transaction Fee</b>	A fee charged for each transaction processed by the merchant.
<b>TSM (Trusted Service Manager)</b>	A neutral broker that sets up business agreements and technical connections with mobile network operators, phone manufacturers or other entities controlling the secure element on mobile phones. The TSM enables service providers to distribute and manage their contactless applications remotely by allowing access to the secure elements in NFC-enabled handsets.
<b>UI (User Interface)</b>	The way a person interacts with a computer or electronic device. It comprises the screen menus and icons, keyboard shortcuts, command language and online help, as well as physical buttons, dials and levers.
<b>Virtual Good</b>	A digital non-physical good purchased for online games or communities.
<b>Wireless Carrier / Carrier</b>	Also known as mobile operator, carriers provide the network infrastructure for the use of a wireless device.