EMV, NFC, AAPL and MCX: Understanding the Electronic Payments Alphabet

This year has brought a surge in interest around electronic payments—both from retailers and consumers. With Apple's rollout of Apple Pay earlier this fall, these technologies were suddenly launched into the public spotlight, prompting fascination around their ease of use and casting speculation around their perceived security. But Apple Pay is hardly alone. There are a number of new and evolving electronics payment technologies being employed, and understanding their unique advantages and intended uses can arm retailers with increased security of their point-of-sale (POS) systems, reduce instances of credit card fraud and, ultimately, lower costs. With that in mind, here's an explanation of what's coming:

EMV (Europay/MasterCard/Visa): EMV is the new worldwide standard for processing *face-to-face* card transactions, and its stated purpose is to reduce instances of fraud. The technology involves a "smart" card with an embedded computer chip, which is read by special terminals. Unlike traditional magstripe cards—which are swiped at terminals—the new chip card is inserted into a terminal for a few seconds while the transaction occurs. The card itself uses dynamic data, which means it's exceptionally difficult to counterfeit.

For those retailers adopting or updating EMV systems, keep in mind that October 1, 2015 is the "liability shift" date for credit card fraud. On that date, the liability for any card fraud will shift from the card issuer to the party that has the least EMV-compliant systems in place. In other words, if the card issuer has issued chip-based cards, but a merchant hasn't yet updated their system with terminals to accept those cards,then the merchant will be liable for the fraud at their store.

NFC (Near-Field Communications): NFC is a method of sending data using very short electronic signals from a device to a terminal. It works when a device with an NFC antenna is held near a contactless card reader. Mobile payment apps (e.g., Google Wallet) use smartphones with NFC capabilities to allow purchases at a contactless terminal. However, acceptance across the industry has been weak, partly because most retailers still do not have NFC-capable terminals, and because many customers do not want to provide information on themselves and their shopping habits. However, with more retailers upgrading their terminals for EMV, they're also including the contactless (NFC) capability within their terminals.

AAPL (Apple Pay): Earlier this fall, Apple introduced its latest smartphones. They have NFC capability, as well as the ability to purchase using Apple Pay. To set-up Apple Pay on an iPhone, the user "loads" up to eight cards, simply by either taking a picture of the card or entering the card data. To pay, the user holds their iPhone near a contactless terminal very briefly with their finger on the secure Touch ID. Then, using its EMV chip, a unique Device Account Number and dynamic security code are generated and transmitted for payment. Aside from consumers' ease of use, Apple also claims its technology is more secure, as it includes a number of features to mitigate fraud. Another difference with this NFC approach is that the transfer of customer information is minimized.

MCX (Merchant Customer Exchange): MCX is a mobile payments venture owned by over 50 major U.S. retailers, and CurrentC is their mobile wallet app that's currently under development. The pilot program began this year, with a rollout scheduled for 2015. MCX's major goals are twofold: Reduce the fees paid to card networks and incentivize customers to make more purchases by offering discounts for products and services. To set it up, the consumer provides personal and banking information, and then downloads both the CurrentC app and each individual retailer's app. At the point of sale, they simply enter their QR code from

their smartphone. Originally, CurrentC would not accept Visa, MasterCard, Discover or American Express cards to avoid payment of interchange fees. Instead, the customer's bank account will be debited. Very recently, however, MCX announced it will support NFC for payments and will also allow credit cards to use its service when it launches, which is a large shift from its original goal of reducing card processing fees. It also stated in early November that its rule preventing member retailers from accepting other mobile payment will expire in months—not years.

Although the QR code scanning technology may be secure, it still will be collecting and maintaining customers' personal, banking and shopping-related information, which could lead to hesitation from consumers. Before it's released, we expect the company to provide more clarity around these questions, such as how much personal data will be collected, and how the customer will be protected from any fraudulent charges to their bank account.

Faced with these emerging technologies, where should retailers focus their attention? For brick-and-mortar retailers, adopting EMV capable terminals with contactless capabilities is an important place to start. Doing so will help lower card fraud, possibly reduce Payment Card Industry (PCI) compliance requirements, and allow the acceptance of NFC payments from customers that want to pay with smartphones—as that technology may very well catch on. Meanwhile, internet retailers should start investigating stronger payment security methods than just security code and address verification. EMV will likely be pushing more card fraud to the internet, as it already has in other countries.

Understanding the Electronic Payments Alphabet – Part Two: The Impending EMV Deadline

Last month, in part one of my series on electronic payment technologies, I briefly discussed Europay, MasterCard and Visa (EMV), the new method for issuing and accepting *face-to-face* card transactions that aims to reduce credit card fraud. While the technology and its many benefits should be top of mind for businesses, perhaps even more important is the approaching deadline that U.S. retailers face regarding their payment systems.

Beginning October 1, 2015, when any credit card fraud takes place, the liability for fraud will fall on the least EMV-compliant party (be it the merchant or card issuer). Therefore, to avoid a potentially significant increase in their liability, face-to-face retailers will need to have payment terminals and systems in place that are capable of reading and processing EMV card transactions.

Why the new standard for liability? Essentially, the EMV process is considered the new gold standard of payment technology. Not only does it involve cards with a more secure computer chip, it also utilizes more robustly protected terminals and processing systems. Unlike magstripe cards, the new chip card contains data that are updated at check-out, when the card is inserted into an EMV terminal. With this secure system in place, the process will be more difficult to interrupt, and the card will be more difficult to counterfeit.

Along with reduced instances of card fraud, fewer data breaches for brick and mortar merchants and an increased sense of security for customers, the technology brings other benefits. For merchants with EMV terminals capable of accepting *both* contact and contactless payments, if 75 percent of their card transactions originate from EMV terminals, they will be exempt from PCI DSS validation requirements each year (though they must still be PCI-compliant). Additionally, virtually all new EMV platforms provide retailers with the ability to accept contactless payments, which allow customers to pay via smartphone with Apple Pay and other

similar payment methods. This is attractive to customers and allows retailers to stay ahead of this increasingly popular payment method.

The transition period begins this October and ends when all terminals and cards will be EMV-only—likely several years from now. During this period, terminals will accept both magstripe and chip cards, and cards will be issued with both magstripes and chips, which is referred to as "backwards compatibility." And even though retailers with EMV terminals that accept magstripe-only cards can still be victims of fraud, they will not be liable for the costs of fraud because of their EMV compliance. That being the case, we recommend retailers update their terminals sooner rather than later.

Still, even as magstripe cards are completely phased out, we don't expect fraudsters to give up; in the near term, they'll likely continue to use fraudulent magstripe cards at storefronts, while in the long-term, they may shift more of their nefarious activity to the internet—a trend we've already seen in other countries. With that in mind, as your business considers its transition to EMV technology, be sure to also closely monitor charge-backs and reversals, check customer IDs at the point-of-sale and bolster e-commerce payment platforms with stronger controls, such as MasterCard's SecureCode program andVerified by Visa.

Understanding the Electronic Payments Alphabet – Part Three: Mobile Technology and Devices

Earlier this year, we discussed Europay MasterCard Visa (EMV), the new method for issuing and accepting face-to-face card transactions that aims to reduce card fraud. In the third and final part of this electronic payment technology series, let's shift the focus to Near Field Communications (NFC, or "Tap to Pay").

Before we dive in, remember that the October 1 payment system deadline for U.S. retailers is approaching fast. After that date, when any credit card fraud takes place, the liability for fraud will fall on the least EMV-compliant party (be it the merchant or card issuer). To avoid this significant exposure, face-to-face retailers need to have payment terminals and systems in place that are capable of reading and processing EMV card transactions.

Retailers should know that nearly all of these new terminals also include the ability to read electronic (NFC) signals, which are transmitted short distances from smartphones. Essentially, using this option requires the customer to have NFC-capable smartphones and the retailers' terminals to have its NFC capability activated.

For background, NFC payment technology has been available for a few years now, most notably via devices using Google Wallet and other apps. However, few retailers implemented NFC-capable terminals from the outset. Then, along came EMV and the iPhone 6 with its NFC capability (Apple Pay). Between Apple's advertising, other smartphone manufacturers getting involved and retailers upgrading their terminals, the growth of mobile payments has accelerated rapidly.
As more retailers implement this NFC payment technology, and as momentum continues to build around its use by consumers, its future looks promising. Smartphones with NFC technology provide customers with an exceptionally secure payment method, and in the case of Apply Pay and Samsung Pay, they minimize the transfer of customer data to third parties. For retailers that invest in EMV/NFC terminals, there's also the added convenience, efficiency and security of these payment alternatives for customers, which they will surely recognize and appreciate.

With all this in mind, here are brief overviews of the various NFC technologies that retailers should note as they invest and implement these new systems:

Apple iPhone – Apple Pay:
With Apple Pay, an iPhone 6 user can load information from several debit or credit cards directly onto their phone. To pay, they hold their iPhone near a contactless terminal. Then, a unique Device Account Number and security code are transmitted for payment, but not the card number. Aside from ease of use, Apple claims its technology is very secure, while minimizing the transfer of customer data. Other security features include:

- Once entered into the iPhone, the only card data available is the card type and the last 4 digits of the card number. Card data is not maintained on the iPhone or Apple servers.
- The purchase will require the user's fingerprint, or they can enter a PIN number.
- The phone only stores data from the ten most recent transactions.
-

Android phones – Samsung Pay with MST:
Samsung Pay is a new product similar to Apple Pay, and available in the new Samsung Galaxy S6. In addition to NFC, Samsung Pay has added technology called Magnetic Secure Transmission (MST). This allows payments to be made from an S6 at a terminal *with no* NFC capabilities. The card data is instead read by the terminal's magstripe reader, which allows the S6 owner to make a purchase at any card terminal—whether or not it's NFC-capable. Although a convenient option for customers, it could be less valuable in the future if most terminals become NFC-capable.

Android phones – Google Wallet:
Most other Android phones will also have NFC purchasing capability, coming preloaded with Google Wallet software. However, Google Wallet users will not have biometric security as do iPhone 6 and Samsung Galaxy S6 users, and although the retailers will not be collecting customer data, Google likely will.

Windows phones:
Microsoft has said they will have an NFC function on their Windows 10 phones, released later this year.

Merchant Customer Exchange (MCX): MCX is a payments venture owned by major retailers. CurrentC is their mobile wallet app under development with rollout scheduled later this year. MCX's main goals are to reduce fees they pay to card networks and incentivize customers to make more purchases by offering them discounts electronically. To set up the app, the consumer must provide personal and banking information, and then download the CurrentC app and each retailer's corresponding app. During the purchase, instead of using NFC technology, they scan a QR code – similar to scanning a boarding pass before getting on a plane. Although QR code scanning technology may be secure, CurrentC will be collecting customers' personal, banking and shopping information, possibly leading to hesitation from consumers.

Dennis Hoyt is President of Hoyt Treasury Services, LLC, a BDO Alliance firm that provides treasury consulting services to companies in the retail, restaurant, grocery and e-commerce sectors, among other industries. He can be reached at DHoyt@HoytTreasury.com, or at 616-656-7770.