THE ROAD TO CONTACTLESS PAYMENTS

EMV, Apple Pay and tokenization

Are you ready to handle transactions from a variety of channels?

With EMV coming to the US in 2015, all eyes are on the new security features and anti-fraud capabilities that come with the new chip-enabled cards and terminals. That security also creates a solid foundation from which to launch a variety of contactless payment services. Now that Apple Pay has joined the mobile payments sector—and looks set to bring Apple's game-changing reputation to the world of contactless mobile payments—this could be the year that transforms the US payments business.

This paper looks at the potential of EMV for fighting fraud, its role in contactless payments and why Apple Pay has entered the market at just the right time. It also looks at the alternatives to Apple's service, what all these changes mean for ATM services, and considers the long-term affect for merchants, banks and their customers.

For more information,
visit us at ncr.com or email financial@ncr.com

Figure 1: Worldwide EMV Deployment and Adoption

Region	EMV cards	Adoption Rate	EMV Terminals	Adoption Rate
Canada, Latin America and the Caribbean	471 million	54.2%	7.1 million	84.7%
Asia Pacific	942 million	17.4%	15.6 million	71.7%
Africa & the Middle East	77 million	38.9%	699,000	86.3%
Europe Zone 1	794 million	81.6%	12.2 million	99.9%
Europe Zone 2	84 million	24.4%	1.4 million	91.2%

EMV around the world

Since it was first launched in 1996, the EMV standard has seen steady but significant adoption around the world. The latest figures from EMVCo show that nearly 30 percent of all card-present transactions worldwide taking place between July 2013 and June 2014 used EMV chip technology.[1]

When it comes to EMV adoption, the notable outlier is the United States, which is still in the earliest stages of migrating to EMV chip technology. However, although the US is the biggest single market that has not yet made the transition to EMV, adoption elsewhere is not universal. Other parts of the world have not yet converted, and various deadlines are in place. Indonesia is due to complete migration for debit cards in 2015, and the deadline for Thailand is 2016. India is expected to start migrating in 2016.

The data shows that even where the overwhelming majority of POS terminals have converted, the adoption rate of EMV-enabled cards can be substantially less. This is primarily because of the liability shift, which makes merchants whose payment terminals are not able to handle EMV transactions responsible for the costs of any fraudulent transaction.

What the chart does not show is that the drive to EMV to date has mostly taken place on credit rather than debit cards. Because fraudsters have typically found credit cards a more attractive market than debit cards, issuers have tended to focus their efforts on migrating credit card programs to EMV.

This is also a contributing factor to the different adoption rates between EMV-enabled POS terminals and EMV-enabled cards: in certain markets, like Asia, credit cards account for a smaller proportion of the total cards in issue.

While all this has been going on, the professional fraudsters have gone elsewhere: mainly to e-commerce, but also to debit and pre-paid cards. Programs are now in place to convert these card types to the EMV standard as well.

EMV and fraud prevention

EMV cards contain an embedded microprocessor that stores significantly more information than traditional magnetic stripe cards and provides a degree of computational ability. When the card is used at an appropriate terminal it allows dozens of pieces of information to be exchanged between the card, the terminal and the relevant bank systems.

As a result, EMV cards can conduct enhanced card and cardholder verification methods, such as data authentication, offline PIN verification and cryptographics for safer card-present transactions. It also means that in a payments ecosystem built around the EMV standard, fraudsters are not able to create counterfeit cards,or engage in cash-out schemes at multiple ATMs, even if they have stolen the legitimate card-holder's personal data

1. The data represents all contact and contactless EMV-chip card-present transactions processed by EMVCo's members. To qualify as an EMV-chip transaction, both the card and terminal used during the payment must be enabled with an EMV chip.

EMV in the USA

Global EMV implementation perfectly illustrates the fundamental truth of fraud prevention: fraudsters will seek out the easiest targets to get maximum return for minimum effort. If one area is too tough to crack, they simply move on to a softer mark.

As one of the world's least secure card markets, the US has become that target. According to Javelin Strategy & Research, US credit-card fraud losses came to roughly $18 billion in 2013. Aite Group suggests that about a third of those losses can be attributed to counterfeit cards. Evidence suggests that domestic fraud has grown through the use of skimming devices—with the most recent high profile case defrauding thousands of bank customers throughout New Jersey, New York, Connecticut and Florida of $5 million.

Progress in the US

It is not easy to get precise data on progress about the US transition to EMV. Events are happening fast, and understandably, banks do not want to share commercially sensitive information.

The first critical date is October 1st 2015, when Visa and MasterCard will shift liability for domestic and cross-border card-present transactions to merchants that are not equipped to handle EMV transactions. In Visa's own words: "The party that is the cause of a chip transaction not being conducted (either the issuer or the merchant's acquirer or acquirer processor) will be held financially liable for any resulting card-present counterfeit fraud losses."

But only about 59 percent of US point-of-sale (POS) terminals will be EMV-enabled by the end of 2015, according to Aite Group , and barely 50 percent of US payment cards will have been upgraded according to Payments Security Task Force.

It's worth remembering however, that Visa's own data on EMV transitions in other markets shows only about 50 percent of merchants having converted at liability shift date. It took several years for conversion to reach 90 percent.

Figure 2: EMV Card-present transactions

Region	Percentage
Canada, Latin America and the Caribbean	83.33%
Asia Pacific	19.42%
Africa & the Middle East	75.90%
Europe Zone 1	96.33%
Europe Zone 2	50.47%
United States	0.03%

Chip and choice

Chip-and-PIN verification is not mandated in the US and in contrast to the majority of EMV schemes, chip and signature looks set to be the default requirement for EMV-enabled transactions.

Visa insists that chip and signature will be secure enough and downplays the need for chip and PIN, claiming that online processing during which transactions are transmitted in real time to the issuer for approval is enough to provide authentication. Cost, convenience and customer engagement are cited by many of the big banks for going down the signature route—reflecting the significant amount of work to be done in educating the public about the use of the new technology.

This does seem to be a short-sighted decision, however, as there is a danger of a false sense of security arising. Relying on a signature still exposes the card to fraudulent use and offers little protection in the case of lost or stolen cards.

The magnetic stripe will also be retained so the card can continue to be used in non EMV compliant terminals. But fraudsters have been known to deliberately damage a card's chip to force the use of this more vulnerable alternative. Interestingly, regulators in Canada are planning to follow their counterparts in certain European countries and block magnetic stripe use for domestic spending. Only when cards are used south of the border will the magnetic stripe be active. The other lesson from international markets is that even where EMV cards are standard, retaining the magnetic stripe means that skimming remains viable for fraudsters.

The fraud effect

Typically, once the move to EMV is complete, fraud becomes more fragmented. It becomes harder to perpetrate fraud in a card-present environment, so there is a move to card-not-present (CNP) transactions instead. In the European Union, EMV implementation caused card fraud loss ratios to drop between 2008 and 2011. But from 2012, card fraud loss ratios began to grow again due to rising CNP fraud and cross-border fraud. In the UK, losses from CNP fraud accounted for 66.8 percent of total card fraud losses in 2013, compared to 54 percent in 2008. Tokenization (see page(s) 6, 7) is intended to address this problem.

There is also a move to other types of fraud attack especially account takeover. Fraudsters gain access to customer's personal details through 'phishing' emails and then are able to execute transactions moving funds out of the account or ordering new cards to be sent to the fraudsters address.

We are also seeing more labour-intensive approaches. There has been growth in voice phishing , or vishing, where criminals contact consumers by standard telephone, often posing as fraud investigators or police officers, and acquire PINs, card details and sensitive personal information from unwitting victims. That information is then used to gain access to bank accounts, arrange for victims to transfer money or hand over their cards to a courier. With the chip currently impossible to clone and PINs required for physical transactions, this is the surest way for criminals to use chip and PIN cards at ATMs without arousing suspicion.

Figures from Financial Fraud Action UK reveal losses to vishing scams trebled in 2013 to reach at least £23.9 million.

To protect consumers, banks are moving to 'enterprise' fraud detection systems that look at customer activity across all channels: cards, internet, branch, telephone to identify fraud attacks on the account. It's also worth noting that the UK experienced a notable increase in counterfeit fraud immediately before the introduction of Chip and PIN cards in 2004, as fraudsters went on one last spree.But by 2012, face-to-face transactions accounted for just £54 million in losses—compared to £189 million previously.

This picture is repeated time and time again. Where EMV is introduced, it has achieved an overall long-term reduction in card fraud that can hide a more complex fraud picture. In the US, the same will happen even if the details are slightly different.

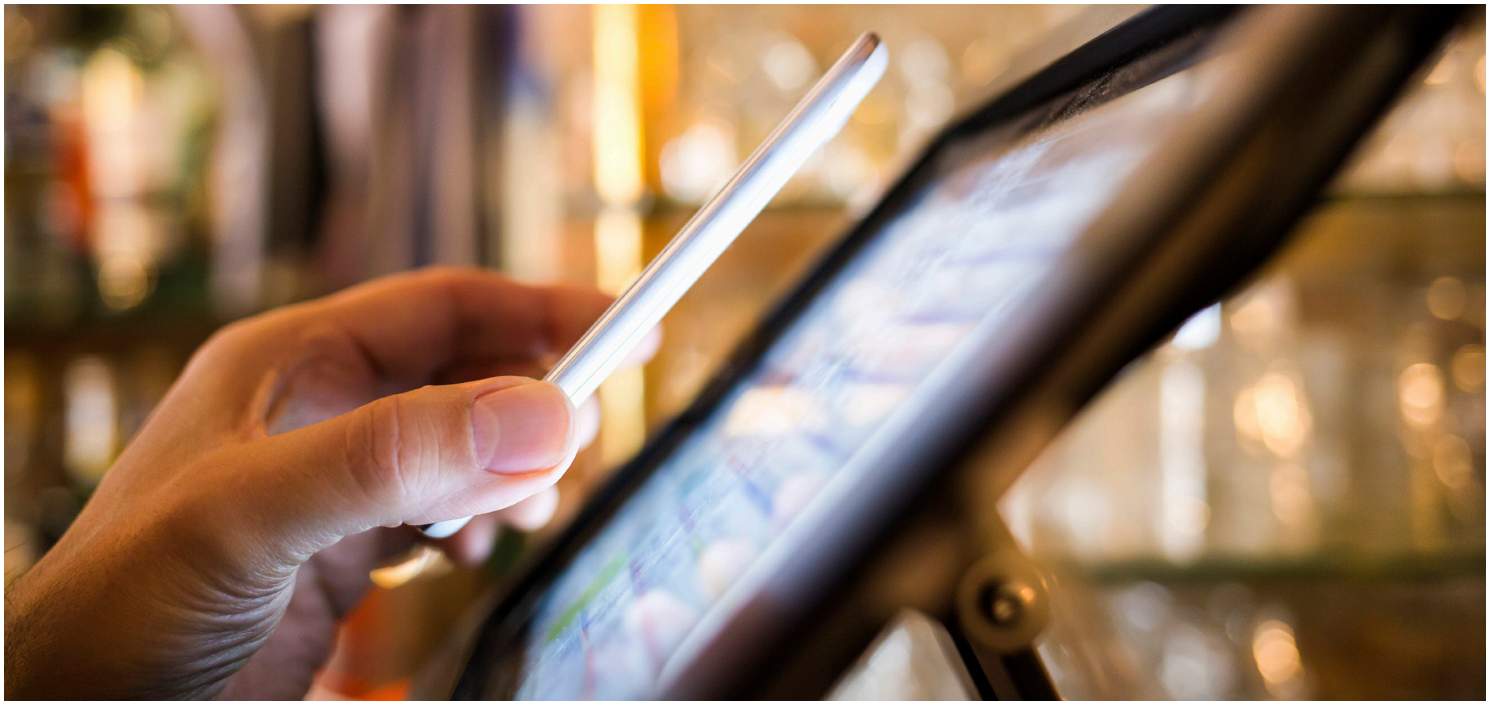
For example, both the UK and France saw cross-border fraud rise significantly in 2012, following sustained falls from 2008 to 2011 as fraudsters moved away from the harder-to-crack domestic markets.

But as most other regions have already adopted EMV, so the US is unlikely to see the same growth in cross-border fraud on this occasion. Fraudsters have demonstrated an unfortunate resilience and are continually finding new methods to gain illegitimate access to other people's funds.

EMV and ATMs

Most of the attention regarding EMV is focused on POS terminals rather than ATMs, and generally other countries have found that the ATM network was a relatively low priority during their transition to EMV.

However, the argument that fraudsters target the weakest area applies to ATMs too. With EMV used to secure in-store transactions, ATMs are the target. Since PINs are an expected and familiar part of the cash withdrawal process, there is little if any education or communication work to be done. The big change is purely technological: enhancing ATMs to read chips over magnetic stripes.



Contactless payments and tokenization

Near-field communications (NFC), the underlying technology that enables cards and terminals to 'speak' to each other when the card is brought into proximity of the terminal, has been available since the 1990s: building passes, key fobs, even public transport cards have all used NFC for years. The arrival of EMV allows the same technology to be used for secure contactless payments. At the same time, mobile technology is now at a point where contactless capability needs to no longer be confined to a card: payments using a smart phone or other device are now possible.

Contactless payments have passed the 'tipping point' in Europe, where there are currently 62 contactless payment projects live, or about to launch. The number of countries accepting contactless payments doubled between early 2013 and early 2014; the number of contactless POS terminals trebled during the same period.

Contactless capability brings non-cash payments to smaller, more routine transactions. Neither customers nor merchants want a daily newspaper to be purchased with a card that has to be inserted into a card reader and validated with a signature or PIN. But with 'tap-and-go' contactless payments, it becomes a lot more appealing. It is easier, faster and more convenient for both consumer and merchant, and it reduces cash costs. Card schemes have ensured that service charges to the merchant are proportional to the typical value of the transaction.

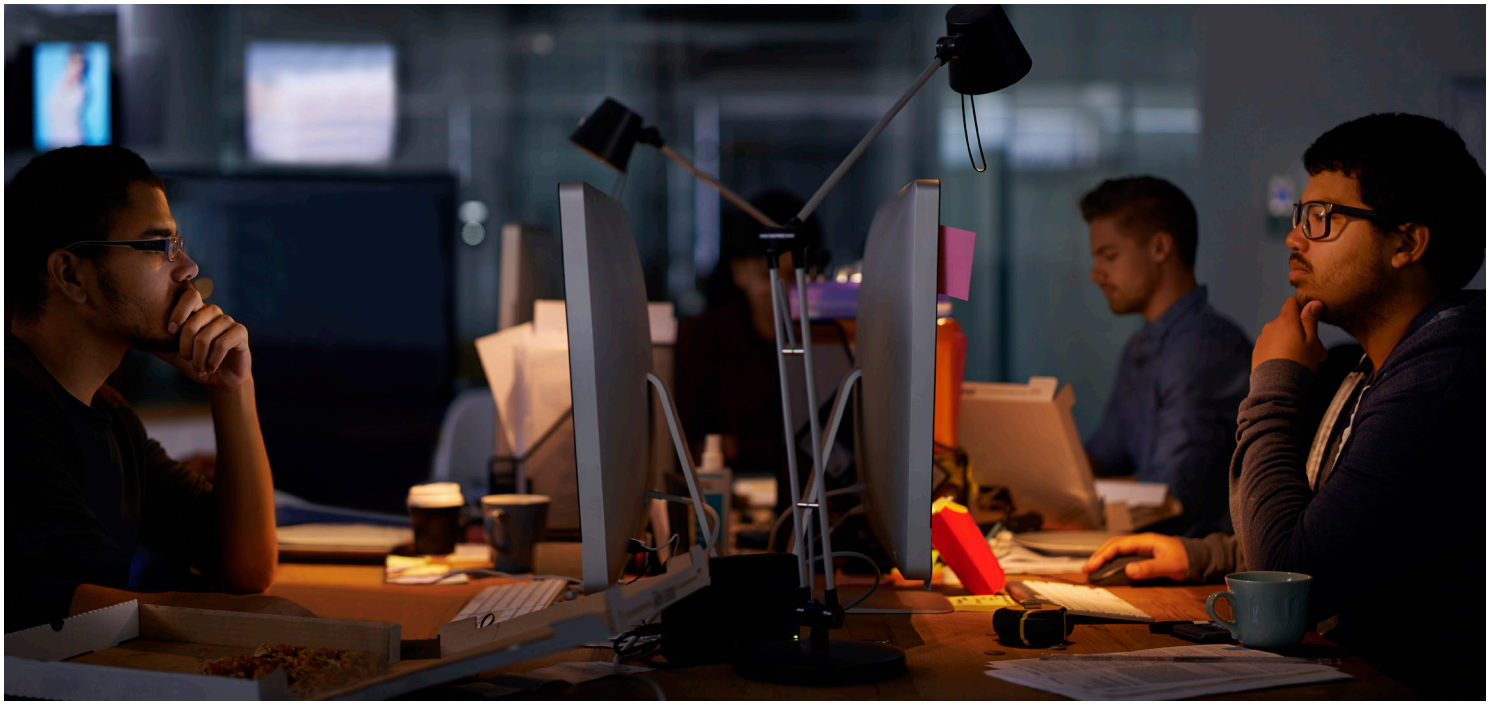
With no PIN or signature to validate the transaction, contactless could be an attractive fraud target. But this is generally managed by requiring the card holder to enter a PIN or signature on a random basis and, more importantly, by setting a maximum value for the transaction. In the UK, for example, the limit is currently £20. This transaction limit is the real control as the fraudsters' goal, as always, is to secure the maximum value from the smallest number of transactions.

The same technology—an EMV enabled card and NFC technology—can also be used to deliver contactless ATM withdrawals.

Spotlight on Poland

Visa has now enabled more than 2.1 million contactless terminals across the whole of Europe. But it is Poland that is seen as the poster child of contactless payments, and is already Visa's largest European market when it comes to contactless transaction volumes. Close to 70 percent of Visa cards in the Polish market have contactless functionality, and the technology accounts for more than 40 percent of all Visa payments in Poland.

More than 75 percent of all in-store POS terminals support contactless payments, and there are plans in place for all Polish POS terminals to support the technology by the end of 2017.



Spotlight on ANZ

Australia's third-largest bank, ANZ, is working with NCR and Visa to roll out an EMV-enabled "tap and PIN" ATM. The new ATM system will be able to read customers' cards without users having to insert them into the machine, for faster more convenient withdrawals.

The solution will also be able to work with future NFC and contactless devices—including mobile phones—for authentication, and prepares the way to pre-staging transactions. Customers will then be able to pre-program their phone or other mobile device with the value and denomination of the cash they want to withdraw.

Critically, the move to contactless eliminates the need for the card to come into contact with the ATM—and so removes the chance of fraudsters skimming card details.

Tokenization

Although EMV is a solution for some aspects of fraud, the one area it does not address is the collection of card data from a hacking attack. This has been an area of focus for fraudsters in recent years as, if successful, they can collect a very large amount of usable card records. The industry's solution to this issue is tokenization.

Tokenization is the process of substituting a card's primary account number (PAN) with a single use or limited-use pseudo-PAN.

This new tokenized PAN has enough data to allow it to be processed by the standard card systems but it can only be used with a specific outlet, or in a specific time frame, or from a specific device (such as a mobile phone) so it has limited or no value if the 'token' is compromised. In addition, the tokenized PAN means a fraudster cannot determine the real account information and has no way of generating a real, and valuable PAN.

Tokenization has the additional benefit of addressing fraud in CNP transactions, which have become a more popular target for fraudsters unable to counterfeit EMV cards or use stolen chip-and PIN cards. By the same principle, it also applies another extra layer of security to EMV-enabled contactless transactions which are not validated by a PIN or signature.

The advent of Apple Pay

Initially launched in the US in October 2014, Apple Pay is a mobile payments system that enables users to use their phone as a contactless payment device at stores that support the system. It saw one million activations in its first three days alone.

As with contactless card payments, the underlying technology is NFC, and the latest iPhone 6 and iPhone 6 Plus come with an integral NFC antennae. To make a purchase, customers place their phone on the sensor of a standard NFC terminal at the point of sale, and verify themselves by using the Touch ID fingerprint scanner on the phone.

To use Apple Pay, customers sign up with their bank, take a photo of their card, and then verify the card is theirs. They can register multiple cards with their phone and then choose which to use in each transaction.

Once a card is registered, tokenization comes in. No card data or other sensitive information is saved to the phone or Apple's servers. When a payment is made, the payment network or issuing bank provides a one-time Device Account Number (or token) that cannot be traced back to the real account by any party other than the issuing bank. Utilizing the secure element on the phone secures access to token, card or transaction data within the handset.

The merchant only sees and stores the token, so if a hacker does get hold of the data it has very limited use.

The use of biometrics for authentication and dependence on the phone's hardware for security gives Apple Pay an immediate advantage over mobile payment solutions that depend purely on software-based validation systems.

The Secure Element

A Secure Element (SE) is a generic name for protected memory on a smart card. The SE could either be embedded in the body of the phone or embedded in the network operator's SIM card.

The SE securely stores card and cardholder data and carries out cryptographic processing. During a payment transaction the SE emulates a contactless card using industry-standard protocols to help authorize a transaction.

The clear separation of phone and card also means it is inherently more secure than the card itself.

This extra layer of security on offer opens up the possibility of using mobile, contactless payment device for much higher transaction values.

Protecting contactless payments by limiting the possible transaction value has been an important barrier to more widespread adoption of contactless capabilities. That in turn restricts where the cards can be used: fast-food outlets and transport networks are obvious candidates and consequently early adopters.

HCE

Host-card emulation (HCE) is being promoted as a short-cut to mobile NFC payments, which could allow banks to launch mobile NFC products without needing to use the SIM or other secure element within a phone. Instead the mobile operating system would communicate directly using NFC in card emulation mode. Banks could therefore issue mobile NFC products without having to cooperate with mobile operators.

With Apple Pay's combination of convenience and validation, it creates real possibilities for retailers of big-ticket items to adopt contactless, phone-based payments.

If Apple Pay takes off—and the launch of a new product from Apple is often the spur that pushes a market segment from challenger status to somewhere closer to the mainstream—then mobile payments could move out of the fast-food outlets and into a much wider range of stores.

A number of big-name retailers have already embraced the technology. Equally important, Apple Pay can be used for e-commerce: the payments app can use the iPhone's passbook function to provide tokenized card data for buying online.

However, early reports[2] indicate that Apple Pay transactions suffered fairly significant problems with fraud. The problem is provisioning fraud—individuals using stolen PAN data to falsely provision an iPhone with someone else's card data. This wasn't the fault of Apple itself. Issuers can block this with better authentication means, but the harder issuers make it to sign up for new programmes the lower the take up rate. Some sources reported fraud rates as high as 6% on Apple Pay due to this weak link. However, these revelations were quickly followed by reports[3] of banks stepping up security checks to prevent this happening.

2. http://www.pymnts.com/news/2015/is-fraud-running-rampant-on-apple-pay/#.VQBRyfmsX9Z
3. http://www.technologytell.com/apple/147536/banks-take-steps-avoid-apple-pay-fraud/

Contactless alternatives

Apple Pay could be a transformative technology if enough retailers are equipped to handle contactless payments. At the launch, Apple claimed that Apple Pay could be used at 220,000 merchants in the US who support contactless payments—a number that had been flat in the three years since Google launched its own contactless Google Wallet scheme. In addition to the big six issuing banks, Apple also claimed to be working with some of the biggest names in American retail.

It appears that, in contrast to other mobile payments providers, the launch of Apple Pay is helping to create a robust ecosystem in which contactless payments can thrive. Partly this is because of the brand and the level of noise that a new development from Apple typically commands. Partly it is because tokenization has allowed Apple to overcome some of the barriers that have slowed down the adoption of other systems.

The role of the telcos

Google Wallet initially used the Secure Element to emulate a payment card. But it quickly ran into difficulties. Most of the major network operators, including Verizon and AT&T, developed their own brand of wallet—formerly Isis, now Softcard. They therefore blocked access to the SE on the SIM card by any other wallet providers, including Google.

As providers of the SE (the SIM card) the telcos were also responsible for data security, and understandably wanted a fee for managing it.

Today, Google Wallet uses host-based card emulation (HCE)—which opens up the possibility of performing mobile NFC payments without using a SIM as an SE. Although Apple Pay uses the traditional device-based SE, there are critical differences to Google Wallet and Softcard.

- Apple Pay uses tokenization so the real card data is not stored
- Apple owns and controls the SE embedded inside the device itself—so avoids challenges from mobile network operators.
- Apple Pay is much simpler because it avoids the complex process of provisioning real card details. Tokenization enables Apple to strip provisioning back to the bare minimum.

Payment networks vs. Automated Clearing House

The Apple approach has also run up against CurrentC, the mobile payment service from Merchant Customer Exchange (MCX).

Unlike Apple, which uses existing payment networks, CurrentC relies on an Automated Clearing House (ACH). The immediate attraction for retailers is that it gets rid of the Merchant Service Charge. But it also requires merchants to set up a complete infrastructure for handling these transactions.

This includes dispute resolution and chargebacks, which take a lot of time and effort.

CurrentC also relies on QR codes, so consumers have to hold their phone under a code-reading scanner, which is normally on the retailer's side of the checkout desk. This is certainly less convenient, and partially cancels out the big contactless advantage. More importantly, the retailer has to change their terminal system to read the codes. In contrast, Apple Pay uses standard EMV contactless technology, which is being rolled out anyway, and existing payments infrastructure.

Even before the full launch of MCX there is a turf war going on, with MCX insisting that merchants must choose to join the CurrentC gang or hang out with the Apple kids. Since MCX membership requires merchants to turn off their NFC capabilities, CurrentC retailers also cut out Google Wallet users and most other mobile payment solutions.

Future of contactless

By bringing together EMV, tokenization and biometrics and NFC, Apple Pay could open up a range of possibilities for mobile and contactless payments.

As roll out increases, biometric authentication will become a more regular feature of payment transactions. Where contactless payments were once seen purely as a means of replacing cash, they could now become a more secure means of replacing cards for higher value transactions.

Apple Pay can already be used for online purchases and with e-commerce apps and has the potential for wider use. The combination of tokenization and biometrics helps overcome online fraud in e-commerce—one of the areas targeted by fraudsters in an EMV-enabled environment.

The same technology can also be deployed at the ATM. Although there is less pressure on transaction time at the ATM, a banked population that is familiar with using a phone in a 'tap and pay' environment will likely demand similar capabilities when withdrawing cash. There is, however, a question around when and whether upgrading ATMs to handle contactless transactions is a worthwhile strategy. While the magnetic stripe remains in operation, there is little imperative for new-form ATMs. However, if consumers stop carrying cards in favour of their phones, then contactless ATMs become much more important.

Why NCR?

NCR Corporation (NYSE: NCR) is the global leader in consumer transaction technologies, turning everyday interactions with businesses into exceptional experiences. With its software, hardware, and portfolio of services, NCR enables more than 550 million transactions daily across retail, financial, travel, hospitality, telecom and technology, and small business. NCR solutions run the everyday transactions that make your life easier.

NCR is headquartered in Duluth, Georgia with over 30,000 employees and does business in 180 countries. NCR is a trademark of NCR Corporation in the United States and other countries. The company encourages investors to visit its web site which is updated regularly with financial and other important information about NCR.

Whatever the decision, the big challenge for ATM operators lies not so much in upgrading the machinery, but in standardizing those changes to prevent a strong, united front against skimming fraud. There would also need to be some consistency for customers around the process of a transaction. For example, how to perform pre-staging to confirm an amount and validate a withdrawal—such as by using a PIN. The industry would need to work together to create a uniform and familiar process.

Biometrics

What does seem more likely is that with fingerprint scanning becoming more widely used on a phone, it will become more readily acceptable—even desirable for other channels like the ATM. In countries such as India, Malaysia and parts of Latin America, fingerprint-scanners already feature on ATMs, either replacing PINs entirely, or providing a second layer of authentication.

There could even be a case for using biometrics on the card itself. MasterCard has already presented the idea, and EMVCo is looking at the possibility of including biometrics in its next generation of specifications.

For longer-term future gazers, fingerprints are only the start of the biometrics possibilities. Face and eye recognition are potential candidates for ATMs or online shopping, while sensors that detect and identify the unique rhythms of a user's pulse could make smart watches the authentication component that is used in mobile-initiated transactions.

Developing markets

Perhaps the area where these developments will have the most impact is in developing markets that have already embraced mobile payments in their various forms, such as MPesa in Kenya—particularly as a means of providing the unbanked with access to financial services. Biometrics in particular help overcome the security issues incurred by less literate populations.

With mobile payments already established and regulated, a strong prepaid element in place, and sophisticated handsets slowly becoming more widely available over time, contactless payments could reduce the costs incurred by cash handling still further. It will be interesting to see how different schemes that involve telecoms providers and banks to various degrees adopt and adapt contactless payments.