EMV, Tokenization, and the Changing Payment Space

Version 1.0
Updated: September 2, 2015

Securosis, L.L.C. 515 E. Carefree Highway Suite #766 Phoenix, AZ 85085 **T** 602-412-3051
info@securosis.com www.securosis.com

Author’s Note

The content in this report was *developed independently of any licensees*. It is based on material originally posted on the Securosis blog, but has been enhanced, reviewed, and professionally edited.

Special thanks to Chris Pepper for editing and content support.

This report may be licensed from Securosis by third parties.

Securosis is the world’s leading independent security research and advisory firm, offering unparalleled insight and unique value to meet the challenges of managing security and compliance in a Web 2.5 world, while defending against APTs, script kiddies and everything in between while showing maximum ROI. Actually, we’re kidding; in fact we usually ridicule statements like that. We’re just a group of security folks that are totally obsessed with improving the practice of information security.

Copyright

EMV Table of Contents

Executive Summary

October 2015 is the deadline for merchants to adopt EMV compliant credit card terminals in exchange for a liability waiver for fraud in card present transactions. EMVCo's message is clear: Install the new terminals or bear the cost of card fraud. The problem is the migration to EMV-compliant card-swipe terminals does not come with a clear value proposition despite this promise. Merchants are being asked to incur significant costs and operational disruption to solve a *banking* problem rather than a *merchant* problem. As such there has been much opposition to this migration request by the card brands.

It's only when you look beyond the terminal migration, and examine the long term implications, does the value proposition become clear. During our research, as we dug into less advertised systemic advances in the full EMV specification for terminals and tokenization, did we realize this migration is more about meeting future customer needs than a short-term fraud or liability problem. The migration is intended to bring payment into the future, and includes a wealth of advantages for merchants, which are delivered with minimal to no operational disruption, including:

- Better customer experience through mobile payments
- Better tracking and analytics
- Better fraud detection through reference tokens
- Can implement P2PE with no loss of functionality
- Reduced breach potential through systematic removal of PAN data
- Reduction of PCI scope and cost

These are in addition to the trumpeted reduction in liability — both promised by EMVCo and additional protection gained through use of Point-to-Point Encryption (P2PE). We will detail these points in this research paper, and provide our unique perspective on the migration. We understand that every merchant will face varying conversion costs at every link in the chain — from point of swipe equipment, to business process adjustments, to point of sale and back office systems — but the advantages are considerable.

Introduction

EMV Compliant Terminals

October 1st, 2015, is the deadline for merchants to upgrade “Point of Sale” and “Point of Swipe” terminals to recommended EMV-compliant systems. To quote Wikipedia, “EMV (Europay MasterCard Visa), is a technical standard for smart payment cards and for both payment terminals and automated teller machines which can accept them.” These new terminals can validate an EMV compatible chip in a customer’s credit card, or validate a secure element in a mobile device when scanned by a terminal. The press is calling this transition the EMV Liability Shift because merchants who do not adopt the new standard for payment terminals have been told that they, rather than banks, will be responsible for fraudulent transactions.

But why should you care? Maybe your job does not involve payments, or perhaps your company doesn’t have payment terminals, or you might work for a merchant who only processes “card not present” transactions. But the fact is that mobile payments and their supporting infrastructure will be a key security battleground in the coming years, and even if you don’t process payments at all, will effect you.

Explaining the EMV shift and payment security is difficult — there is a great deal of confusion about what the shift means, what security it really delivers, and its real benefits for merchants. Part of the problem is the fact that the card brands have chosen to focus all their marketing on a single oversimplified value statement: the liability shift for card present transactions through non-EMV-compliant terminals. But digging into the specifications and working through the rollout process reveals a much larger change underway, with much broader ramifications. Unfortunately the press has failed to realize these implications, so the conversation has focused on liability, and lost sight of what else is going on. So we produced this research paper to explain the additional changes underlying the EMV shift, its full impact on merchant security and operations, and where the shift will take the payment ecosystem.

To collect background for this report we spoke with merchants (both large and mid-sized), merchant banks, issuing banks, payment terminal manufacturers, payment processors, payment gateway providers, card manufacturers, payment security specialists, and third-party payment security providers. Each stakeholder has a very different view of the payment world and how it should work. We remain focused on helping end users get their (security) jobs done, but we need to start with background to help you understand how the pieces all fit together — and just as importantly, the business issues driving the changes.

Payment Players and New Requirements

To set the stage, what exactly are merchants being asked to adopt? The EMV migration, or the EMV liability shift, or the EMV chip card mandate — pick your favorite marketing term — addresses US merchants who use payment terminals designed to work only with magnetic stripe cards. Merchants are being asked to replace old magstripe only terminals with more advanced, and more expensive, EMV-compatible chip terminals. EMVCo's requirement to avoid inheriting liability is to deploy terminals capable of validating payment cards with embedded EMV-compliant ‘smart’ chips by October 1, 2015.

EMVCo created three main rules to drive adoption:

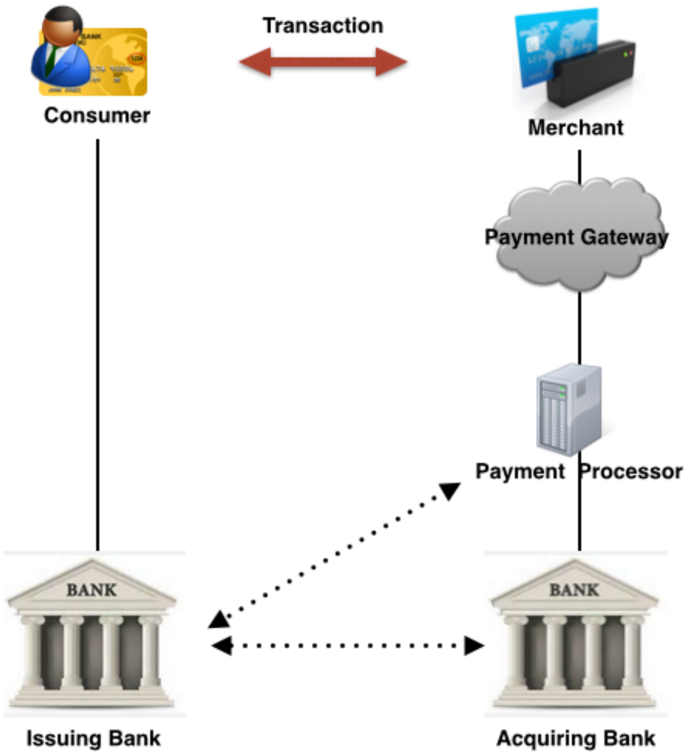
1. If an EMV ‘chipped’ card is used to conduct a fraudulent transaction with an EMV-compliant terminal, the merchant will not be liable — just like today.
2. If a magnetic stripe card is used for a fraudulent transaction with a new EMV-compliant terminal, again the merchant will not be liable — also just like today.
3. But if a magnetic stripe card is used in a fraudulent transaction with an old-style magstripe only terminal, the *merchant* — instead of the issuing bank — will be liable for the fraud.

That’s the gist of it: merchants who use old magstripe terminals pay for any fraud committed with new chipped cards. There are a few exceptions, for example the October date only applies to in-store terminals, and won’t apply to kiosks and automated systems like gas pumps until 2017.

So what’s the fuss all about? Why has this gotten so much press? And why has there been so much pushback against adoption from merchants? Europe has been using these terminals for over a decade, and it seems like a straightforward calculation: projected fraud losses from card-present magstripe cards over some number of years vs. the cost of new terminals (and software and supporting systems).

But of course it’s not quite that simple. Yes, cost and complexity are increased for merchants — as well as costs for issuing banks when they send customers new ‘chipped’ credit cards. But it is not actually clear that merchants will be free of liability. I will go into the reasons later, but for now I will just say that EMV does not fully secure the Primary Account Number, or PAN (normally called simply the "credit card number") in and of itself. You'd think with all the media hype around breaches and the threat of Federal oversight that security across the board would be tightened up, but this migration does not protect merchants from data breaches. EMVCo says merchants won't be liable when counterfeit cards are used if they fully adopt EMV compliant terminals, but unless other new features are embraced, the full security benefit cannot be realized.

But before we go into detail some background is in order. People within the payment industry know all the players and acronyms, but most security professionals and IT practitioners — even those who work for merchants — are less conversant with the payment ecosystem and how data flows. Further, it is not appropriate to focus purely on chips in cards because security comes into play many other places in the payment ecosystem. Finally, it is impossible to understand the liability shift without understanding where liability shifts *from*. Security and liability go hand in hand, so it's time to explain the payment ecosystem and discuss other areas where security comes into play.



When a customer uses their credit card, the merchant depends on several other parties to process the transaction. There may be several different banks and service providers helping to route the request and send money to the right places. Additionally, the merchant never contacts *the customer's bank* — known as the *issuing bank* directly. When a customer swipes their card the merchant likely relies on a *payment gateway* to route the transaction. The gateway might not even link directly to the merchant's bank — instead it may enlist a *payment processor* for that. A processor or the acquiring bank then collects funds from the customer's bank and provides transaction approval. The major players in more detail:

- **Issuing Bank:** An issuer — the bank that issues the cards — and typically maintains customer accounts. There are thousands of issuers worldwide. But from there is gets confusing, as many issuers delegate credit card management to another bank, who may in turn manage affinity brands (such as for charities) for card branding. Large banks typically have multiple arrangements with third parties, credit unions, small regional banks, who leverage the issuing bank for credit card services. Just to complicate things, many ‘issuers’ outsource *actual* issuance to other firms. These third parties are all certified by the card brands to perform card printing and personalization services for the issuing bank. Smart card issuance has historically been outsourced because EMV was new and complicated, and the hardware and software needed for card production and issuance is expensive.

- **Payment Gateway:** This is basically a leased service which links a merchant to a merchant bank for payment processing. Their value is in maintaining networks and orchestrating processes and communication. A gateway checks with the merchant bank to reject stolen or over-drafted cards. They often leverage fraud detection software or services to validate transactions.

- **Payment Processor:** A processor is used by a merchant to handle credit card transactions. It may be an acquiring bank or a service provider which deposits funds into merchant accounts. Processors help collect funds from issuers. Firms like PayJunction serve as both gateway and processor, and there are hundreds of Internet-only gateways/processors.

- **Acquiring Bank:** The acquirer provides capital to merchants by floating payments, then reconciling customer payments and accepting deposits on the backend. Many process credit and debit payments directly; others outsource to their own payment processor. They also accept credit card transactions from issuing banks. Acquirers exchange funds with issuing banks on behalf of merchants. Basically they handle transaction authorization, routing, and settling. The acquirer is the merchant’s partner, and assumes the risk of merchant insolvency and non-payment.

- **Merchant Bank:** The merchant’s bank is synonymous with am acquiring bank. A merchant account is a contract (actually a line of credit) between a merchant and their acquiring bank.

- **Card Brand:** Visa, MasterCard, Europay, Amex, and similar firms. Sometimes called an ‘association’ as each helps certify the ecosystem of 3rd party providers.

- **EMVCo:** The consortium of Visa, MasterCard and Europay.

In addition to the players, there are a few terms I will use throughout this paper:

- **PAN:** Primary Account Number, essentially a credit card number.

- **CCV:** A security code or card validation code printed on credit cards to help detect fraud. Sometimes called CSC, CVN, or CVV2.

- **PCI-DSS:** Payment Card Industry Data Security Standard. A set of contractual security requirements on merchants who process credit card transactions. Larger merchants, who process millions of transactions, must have their compliance externally audited.

EMV Migration Issues

Cost and Complexity

Moving to EMV-compliant terminals is not typically a straight equipment swap. While some semi-integrated and standalone terminals mean only an equipment swap, the normal use case means you can't just plug them in, turn them on, and expect everything to work. Changes are needed to the supporting software for point-of-sale systems (cash registers). You will likely need to provision keys to devices; if you manage keys internally you will also need to make sure everything is safely stored in an HSM. Changes are often required to back-office software to sync up with POS changes. IT staff typically need to be trained on the new equipment. Merchants who use payment processors, or gateways that manage their terminals, face less disruption as the 3rd party provider handles a lot of the work. Regardless, it is still a lot of work for merchants and their providers; rollouts can take months.

Much of the pushback we heard was from merchants about the cost, time, and complexity of this conversion. Merchants see pretty much the same payment system they have today with one significant advantage: cards can be validated at swipe. But merchants have historically not been liable for counterfeit cards, and so see little reason to embrace this cumbersome change.

Other Issues

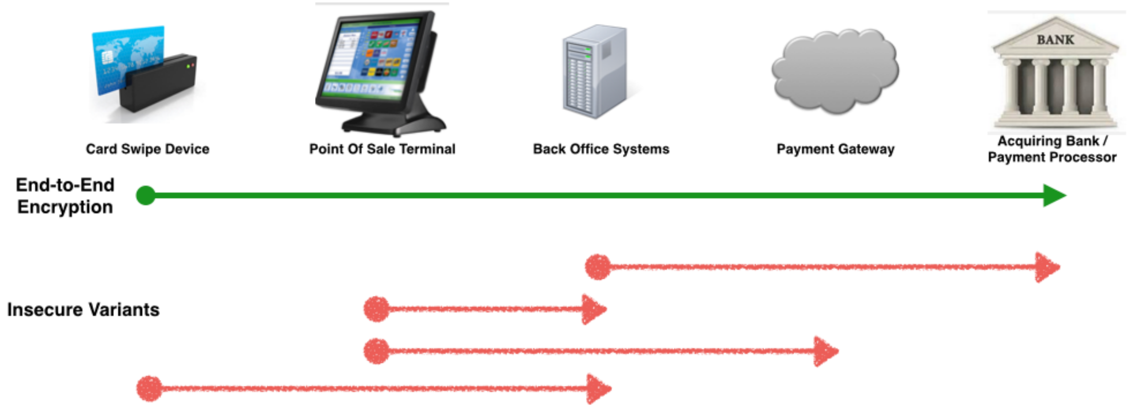
PINs vs. Signatures

Another issue we heard was the lack of requirement for “Chip and PIN”: after swiping a chipped card a user must punch in a secret PIN. This verifies that the user using the card owns it. But US banks generally do not use PINs, even for chipped cards like the ones I carry. Instead in the US signatures are typically required for purchases over a certain dollar amount, which has proven to be a poor security control. PINs could be required with smart cards in the future, but the issuers have not published any plans to do so. PINs are less important with mobile payments because it's easy to secure a phone, tie it to a specific user, and the mobile devices already have PIN codes or biometrics a mobile wallet can leverage.

Point to Point Encryption

The EMV terminal specification does ***not*** mandate the use of point-to-point encryption (P2PE), much less full end-to-end encryption. PAN data is still transferred in the clear, along with any other data passed, if payment tokens are not being used. For years the security community has been asking merchants to encrypt the data from card swipe terminals to ensure it is not sniffed from the merchant network or elsewhere when the PAN is passed upstream for payment processing. To be clear, P2PE is an inherent capability of the terminals, but not a requirement for the EMV terminal migration. Most merchants who adopt EMV terminals will continue to pass PAN in the clear.

Firms which implemented encryption often fail to encrypt from card swipe all the way to merchant bank. As shown in the diagram below, merchants might not encrypt from the card swipe, but merely from the point of sale device to a back-office server — or worse, from the back-office server to a payment gateway. Full end-to-end encryption, as originally envisioned, creates a very secure ecosystem where it is difficult for attackers to access PAN data. It also breaks older merchant business processing systems, so many chose to water down encryption and transfer data less securely.



But of course it is a bit more complicated. Many merchants use PAN data from terminals for fraud and risk analytics. Others use the data to seed back-office customer analytics for competitive advantage. Still others do not want to be tied to a specific payment provider — which is what happens with keys provided by the payment processor or acquiring bank — encrypted terminals can only speak with the recipient which holds their keys.

On the opposite side of the spectrum, many payment gateways don't want to-point encryption either. They want transaction data for their own purposes, such as to resell fraud analytics back to merchants or payment processors. P2PE would shut them out, limiting them to carrying bits from one place to another. There are a variety of different reasons the various players have not embraced P2PE, despite its profound security advantages.

No Support

But the old argument that “nobody wants EMV” is behind us — most consumers are tired of replacing their cards every few months. There is support from card producers, acquirers and gateways. Merchants cite the lack of EMV cards issued to customers, but that is a red herring, and firms like AmEx have rolled them out, and most other card brands are in process as well. Banks are not eager to eat the cost of chipped cards, especially if the terminals needed to leverage chips are absent from merchant sites, but they *are* eager to reduce fraud and avoid federal oversight. So the card brands are acting on behalf of the industry to drive things forward. But slowly, and without clearly articulating their plans.

No Credit Cards

During our conversations each stakeholder had a set of goals they’d like to see, and a beef with some other party in the payment ecosystem. The card brands strongly support any changes that will make it easier for customers to use credit cards and grease the skids of commerce, and are annoyed at merchants for standing in the way of technical progress. Merchants are generally angry at the per-transaction fees they pay — especially in light of the minimal service they receive — and want to be rid of the whole security and compliance mess because it’s not part of their core business. These two factors are why most merchants wanted a direct Merchant-Customer Exchange (MCX) based system to do away with credit cards and allow merchants direct access to customer bank accounts. Acquirers were angry that they have been forced to shoulder much of the fraud burden, and want to maintain customer relationships rather than abdicating them to merchants. And so on.

Security is Not The Focus

During our conversations security was one of the last items anyone brought up, almost as an afterthought, if at all. Nobody is talking about point-to-point encryption as part of the EMV transition, so despite the huge win for PAN security, in practice encryption will not be leveraged by many merchants. Second, PINs are not required to validate cardholders — merely recommended in limited circumstances. The press made a big deal about the lack of PIN codes for smart card user validation, but few in the industry were talking about it other than as a reference as to why security was not that important. But perhaps the biggest ‘tell’ is the EMV terminal transition will not address one of the fastest-growing types of fraud: Card Not Present transactions. In fact, if card cloning is no longer possible, it will likely drive more CNP fraud. From our research, it does not appear that security is driving the EMV shift. Not even close.

Why Move?

The key question is: Why should merchants move to EMV terminals?

This will be a bit of a spoiler for our conclusion, but the upcoming sections telegraph where this is all heading, so we will spell out the vision that Visa largely outlined back in 2011.

The vast majority of card holders have smartphones *today,* which can function as fully capable "smart cards", and many customers happily use them to replace plastic cards. We see this overseas, especially in countries that are — as one professional put it — "under-banked and over-cellular-ed" as it makes payments a reality in places where you could not safely conduct commerce before. Some African nations, for example, process around 50% of payments via mobile devices. Starbucks has demonstrated conclusively that consumers *will* use mobile phones for payment, and also do other things like order through apps. Customers don't want better *cards* — they want better experiences, and the card brands seem to get this.

Security can be better — not just with chip validation and P2PE, but also because of tokenization and 2FA which we will discuss below — so security is *one* reason for merchants to move. The liability waiver is an added benefit as well. But these are both secondary. The move from passive magnetic stripe cards to smart cards is a big jump, but from plastic cards to smartphones will be the payment industry's equivalent of the shift from horses to automobiles.

We could say this is all about mobile payments, but that would be gross oversimplification. It is about what mobile devices — powerful pocket computers — can and will do to improve the entire sales experience. New technology enables complex affinity and discount plans, enhances the consumer experience, provides geolocation, supports payment tokens, and offers an opportunity to bring the underlying system into the modern age — with modern security. If you are a merchant looking to justify an EMV investment, look no further than Starbucks and how they leverage apps for competitive advantage. Their story is about millions of users and the stickiness of a mobile app to promote their business.

The Liability Shift

So far we have discussed the EMV requirement, introduced the players in the payment landscape, and considered merchant migration issues. It is time to get into the meat of this research paper. Now we can discuss the liability shift in detail, and cover the conversations going on behind the scenes. .

What Is the Liability Shift?

As we mentioned earlier, the card brands have stated that in October of 2015 liability for some fraudulent transactions will shift to non-EMV-compliant merchants. If an EMV ‘chipped’ card is used at a terminal which is not EMV-capable for a transaction which is determined to be counterfeit or fraudulent, liability will reside with the merchant who is not fully EMV-compliant. In practical terms this means merchants who do not process 75% or more of their transactions through EMV-enabled equipment will face liability for fraud losses.

But things are seldom simple in this ecosystem, and different stakeholders we interviewed all had different takes on what this really means, or if this quoted 75% threshold is even true.

Who Is to Blame?

Card brands offer a very succinct message: Adopt EMV or accept liability. This is a black-and-white proposition, but actual liability is not often as clear. The message is primarily targeted at merchants, but the acquirers and gateways need to be fully compliant first, otherwise liability cannot flow downstream past them. The majority of upstream participants are EMV ready, but not all, and it will take a while for the laggards to complete their own transitions. At least two firms we interviewed suggested this is as much of the liability shift to anyone who is not an issuing bank, so losses will be distributed more evenly through the system. Regardless, the card brands and issuing banks will blame anyone who is not EMV-compliant, and as time passes that will be more likely to land on merchants.

Do Merchants Currently Face Liability?

That may sound odd, but it’s a real question which came in during interviews. Many of the contracts between merchants and merchant banks are old, with much of their language drafted decades ago. Their focus and concerns pre-date modern threats, and some agreements do not explicitly define responsibility for fraud losses, or discuss certain types of fraud at all. Many merchants have benefitted from the ambiguity of these agreements, and not been pinched by fraud losses — instead issuers or acquirers shouldered the expense. There are a couple cases of merchants dragging their feet because they are not contractually obligated to accept the risk. Most new contracts are written to push liability away from the service providers and onto merchants — liability waivers from card brands not withstanding. There is considerable ambiguity regarding merchant liability.

How Do Merchants Assess Risk?

It sounds straightforward for merchants to calculate the cost-benefit ratio of moving to EMV. Fraud rates are fairly well known and data on fraud losses is published often. It should be simple to calculate the cost of fraud over the medium term vs. the cost of migration to new hardware and software. But this is seldom the case. Published statistics tend to paint broad strokes across the entire industry. Mid-sized merchants don't often know their fraud rates or where fraud is committed. Sometimes their systems detect it and provide first-hand information, but in other cases they hear from outsiders and lack sufficient detail to intelligently identify proportions of losses. Some processors and merchant banks share data but that is hardly universal. A significant proportion of merchants do not understand these risks to their business well, and are unable to formulate a rational plan. These merchants fear being duped into action.

Without P2PE, Will I Be Liable Regardless?

The EMV terminal specification does ***not*** mandate point-to-point encryption. If — as in the Target breach — malware infects PoS systems and gathers PAN data, will courts view merchants as liable regardless of their contracts? At least one merchant pointed out that if they are unlucky enough to find themselves in court defending their decision to not encrypt PAN after a breach, they will have a difficult time explaining their choice to a judge. We maintain that P2PE for merchants is a critical piece of security, and strongly advise encrypting data from point of swipe to *at least* the payment gateway provider to reduce liability.

PCI <> EMV

The EMV specification and the PCI-DSS are different documents with different scopes. That said, we expect merchants who adopt EMV-compliant terminals to reduce compliance costs in the long term. Visa has stated that effective October 2015, Level 1 and Level 2 merchants who process at least 75% of transactions through EMV-enabled POS terminals (which support both contact and contactless cards) will be exempt from PCI compliance *assessment* that year. They will still be officially required to comply with PCI-DSS, but can skip one costly annual *assessment*. MasterCard offers a similar program. This exemption is distinct from the liability shift, but an attractive offer for merchants.

Systemic Tokenization

We expect EMVCo's proposed tokenization system to radically change payment security. This section focuses on use of tokens in EMV-compliant payment systems — both merchant on premise options currently in use and the proposed system for EMV-compliant terminals. This is critical because the EMV tokenization specification's security model is to stop passing PAN around as much as possible, to limit its exposure.

You do not need to be an expert on tokenization to benefit fully from this discussion, but you should at least know what a token is and that it can fill in for a real credit card number without requiring significant changes to payment processing systems. Those of you who need to implement or manage payment systems should be familiar with two other documents. The EMV Payment Tokenization Specification, version 1.0, released March 2014, provides a detailed technical explanation of how tokenization works in EMV-compliant systems; you also need to understand the Payment Account Reference addendum, released May 2015.

If you want additional background we have written extensively about tokenization at Securosis. It is one of our core coverage areas because it's relatively new for data security, poorly understood by the IT and security communities, and genuinely promising. If you're not yet up to speed and want a little background before we dig in we offer *free* research papers, including Understanding and Selecting Tokenization as a general primer, Tokenization Guidance to help firms understand how tokenization reduces PCI scope, Tokenization vs. Encryption: Options for Compliance to help firms understand how these technologies fit into a compliance program, and Cracking the Confusion: Encryption and Tokenization for Data Centers, Servers, and Applications to help build these technologies into systems.

Merchant Side Tokenization

Tokenization has proven its worth to merchants by reducing the scope of PCI-DSS (Payment Card Industry — Data Security Standard) audits. Merchants, and in some cases payment processors, use tokens instead of credit card numbers. This means merchants do not need to store the PAN or any associated magstripe data, and a token is only a reference to a transaction or card number, so they don't need to worry the token might be lost of stolen. A token is sufficient for a merchant to handle dispute resolution, refunds, and repayments, but it's not a *real* credit card number, so it cannot be used to initiate new payment requests. This is great for security because the data an attacker needs to commit fraud is elsewhere, and the merchant's exposure is reduced.

We are focused on tokenization because the EMV specification relies heavily on tokens for payment processing. These tokens come from issuing banks via a Token Service Provider (TSP) who tracks tokens *globally*, rather than from a merchant. That is good security, but a significant departure from the way things work today. Many merchants complain because without a PAN or some way to uniquely identify users, many event processing and analytics systems break. This has created significant resistance to EMV adoption, but this barrier is about to be broken. With Draft Specification Bulletin No. 167 of May 2015, EMVCo introduced the Payment Account Reference. This unique identification token solves many of the transparency issues that merchants had with losing access to the PAN.

The Payment Account Reference and Global Tokenization

Merchants, payment gateways, and acquirers want — and in some cases need — to link customers to a payment instrument presented during a transaction. This helps with fraud detection, risk analytics, customer loyalty programs, and various other business operations. But if a PAN is sensitive and lost as part of most payment fraud, how can we enable those use cases while limiting risk? Tokenization.

EMVCo's Payment Account Reference (PAR) is essentially a token to reference a specific bank account. It is basically a random value representing a customer account at an issuing bank, which cannot be reverse-engineered back to a real account number. In addition to the PAN, the EMV Payment Tokenization Specification specifies token replacement for each PAN to reduce the use and storage of credit card numbers throughout the payment ecosystem. This is what Apple Pay does today, and further reduces fraud by limiting the availability of credit card numbers for attackers to access. But rather than do this on a merchant-by-merchant basis, *it is global and built into the system*. The combination of these two tokens enables unambiguous determination of a customer's account and payment card, so everyone in the payment ecosystem can leverage current anti-fraud and analytics systems

Consider PARs in detail:

- A PAR is a Payment Account Reference, or a *pointer* to what people outside the banking industry call a bank account. A PAR is technically a token with a one-to-one mapping to a bank account, intended to last as long as the account. You may have multiple mobile wallets, smart cards or other devices, but your PAR will be consistent across them all.

- The PAR will remain the same for each PAN; a payment account may be associated with multiple PANs, but only one PAR. For example, many households share a single PAN across all cards in the family, but in cases where a home or business has a unique PAN for each card holder, the PAR is always the same. New cards — or mobile wallets — with new PAN will also retain the original PAR.

- The PAR token will be passed, along with the credit card number *or* payment token, to the merchant's bank or payment processor.

- A PAR should be present for ***all*** transactions, regardless of whether the PAN is tokenized or not.

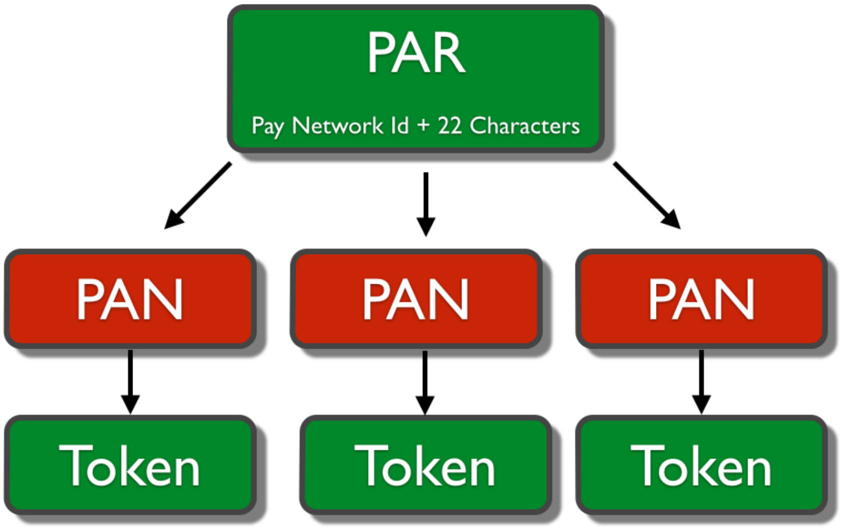
- PAR tokens are generated by a Token Service Provider, on request from *the issuing bank*.

- A PAR will enable merchants and acquirers to consistently link transactions *globally,* and to confirm that a Primary Account Number (PAN, basically a credit card number) is indeed associated with that account.

- For the geeks out there, a PAR cannot be reverse-engineered into a bank account number or a credit card number, and cannot be used to find either of those values without special knowledge. Token Service Providers will use Format Preserving Encryption, tokens created from random numbers, or — to provide global consistency — code books or one-time pads.

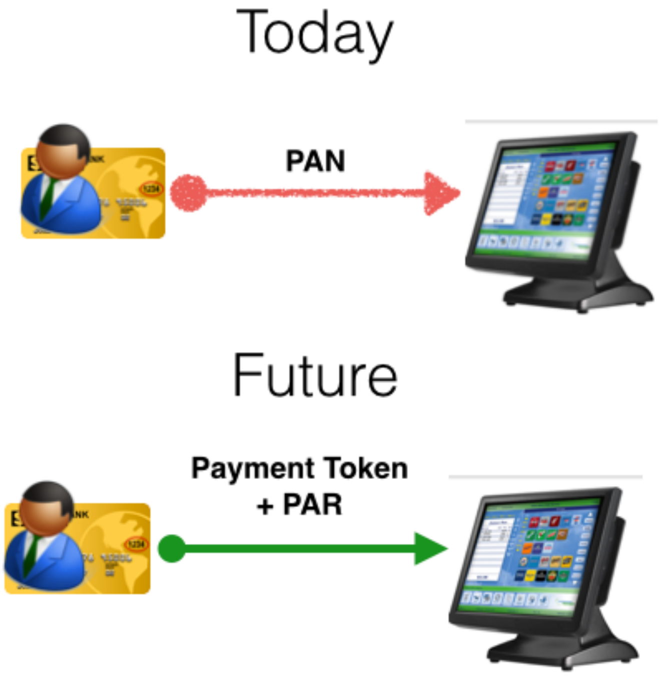
- The specification envisions a tokenized value of the PAN being used, but this is not currently mandatory, so the spec currently permits legacy usage of the original credit card number as a PAR.

The relationship between the PAR, the Primary Account Number (PAN), and the payment token looks like this:



What Is the Impact?

The PAR is designed to remove the majority of merchant objections to tokenization and loss of the PAN, and with a payment token, to provide better value to merchants than the PAN alone. Today, EMV compliant terminals *still* pass PAN data because many firms rely upon it. But in the future it means that the EMV terminals will be able remove PAN from the transaction, without loss of functionality, and provide greater security without P2PE, like this:



"In theory there is no difference between theory and practice. In practice there is." —Yogi Berra

An EMV card, or a mobile wallet, enables a terminal to validate the authenticity of a payment object presented by a customer. That is old news, but it gets much more interesting with the PAR. The PAR technical specification defines an open standard for exchanging authorization data between stakeholders, along with processes for provisioning and payment transactions. This essentially means Visa, MasterCard, and Europay — in concert with the issuing banks — are now identity providers for merchants, payment networks, and acquirers.

Unlike identity tokens from companies such as Facebook, Google, and Twitter — who allow other sites to leverage their user identities and management capabilities as a service — the PAR is intended solely for use within the payment ecosystem. And unlike services that leverage SAML or OAuth tokens, the PAR is *not* an identity token as such, and not interchangeable. The PAR technical specification emphatically states that a PAR is *not* a consumer identifier, based on the argument that most households have a single PAN value issued for all credit cards in a given household, but in practice it will be used that way. A PAR token offers the same granularity as a home phone number or a PAN today, and both merchants and acquirers can glean enough intelligence from transaction context to determine which card user is behind a transaction if needed. Privacy buffs will have a problem with this, but it is no worse than what has been going on for decades.

A PAR is *not* to be provided to consumers, and should only be shared among firms which process payments. Undoubtedly attackers will go after PARs first, as well tokenized PAN values, to test the logic implemented by payment processors and issuing banks. A PAR should not be able to initiate payment transactions but attackers will inevitably test merchant, acquirer, and payment services vendors to see how well they obey the rules.

A PAR should support point-to-point encryption without the loss of data elements merchants want for anti-fraud, consumer tracking, affiliate programs, and other programs. In practice we believe PAR will kill off end-to-end encryption altogether. Some merchants dislike tying themselves to a single payment processor or acquiring bank because an encryption key works only for a single destination, but the PAR removes most of the other impediments. With a PAR to unambiguously identify customers, merchants can manage most current analytics, even with P2PE, from swipe through payment gateway to merchant bank.

We have explained for years that payment data security requires several supporting technologies: Chip and PIN for user and device authentication, P2PE for data transmission, and tokenization or FPE for record storage. The forward-looking PAR specification accommodates all three with minimal impact on business operations. As this approach is rolled out it will disrupt existing card security programs and PCI certifications, and should force attackers to change their tactics. This is a major win for merchants, banks, and customers.

Mobile Payments

We conclude this research paper on the EMV migration and changes in the payment industry, with mobile payments. Mobile payments were not part of our initial scope, but during our conversations it became clear that they are a key part of the transition. Mobile devices are breaking long-held assumptions about payment security, so we have some tips to help merchants and issuing banks deal with the changing threat landscape.

Some of you will wonder why we are talking about mobile device payments when EMV migration discussion has largely centered on chipped payment cards supplant magstripe cards. The answer is that it's not a question of whether users will have smart cards *or* smartphones in the coming years — many will have both, at least in the short term. American Express has already rolled out chipped cards to customers, and Visa has stated that they expect 525 million chipped cards to be in circulation at the end of 2015. But while chipped cards form a nice bridge to the future, a recurring theme during conversations with industry insiders was that they see the industry inexorably headed toward mobile devices. The transition is being driven by a combination of advantages including reduced deployment costs, better consumer experience, and increased security both at endpoint devices and within the payment system. Let's dig into specifics:

- **Cost:** Issuers have told us chipped cards cost them $5-12 per card issued. Multiplied by hundreds of millions of cards, the switch will cost acquirers a huge amount of money. A mobile wallet app is cheaper and easier to use than a physical card with a chip, and can be upgraded. And customers can select and purchase the type of device they prefer.

- **User Experience:** Historically, the advantage of credit cards over cash was ease of use. Consumers are essentially provided a small loan for their purchase, avoiding impediments from cash shortfalls or visceral unwillingness to hand over hard-earned cash. This is why credit cards are called *financial lubricant*. Mobile devices offer a similar advantage over credit cards. One device can hold *all* your cards, and you don't even need to fumble with a wallet to use one. When EMVCo tested smart cards, which function slightly differently than magstripe cards, one in four customers had trouble on first use. Whether they inserted the card into the reader wrong, or removed it before reader and chip had completed negotiation, the transaction failed. Holding a phone *near* a terminal is easier and more intuitive, and less error-prone — especially with familiar feedback *on the customer's phone*.

- **Endpoint Protection:** The key security advantage of smart cards is that they are very difficult to counterfeit. Payment terminals can cryptographically verify that the chip in the card is valid and in the possession of the account owner, and actively protect secret data from attackers. But modern mobile phones have either a “Secure Element” (a secure bit of hardware like the chip in a smart card) or “Host Card Emulation” (a software — or *virtual* — secure element). But a mobile device can also validate its state, provide geolocation information, ask the user for additional verification such as a PIN or thumbprint for high-value transactions, and perform additional checks as appropriate for the transaction/device/user. And features can be tailored to the requirements of the mobile wallet provider.

- **Systemic Security:** Under ideal conditions the PAN itself is never transmitted. Instead the credit card number printed on the face of the card is only known to the consumer and the issuing bank — everybody else only uses a token. The degree to which *smart cards* support tokenization is unclear from the specification (*i.e.:* it’s not clear smart cards always use tokens instead of PAN), and it is also unclear if they can support the PAR given the chipped cards were designed prior to the PAR specification. But we know mobile wallets *can* supply both a payment token and a customer account token (PAR), and completely remove the PAN from the consumer-to-merchant transaction. This is a huge security advance, and should reduce merchants’ PCI compliance burden.

The claims of EMVCo that the EMV migration will increase security only make sense with mobile device endpoints. If you reread the EMVCo tokenization specification and the PAR token proposal with mobile — as opposed to physical cards — in mind, many lingering questions are resolved. For example, why are all the use cases in the specification documents for mobile devices, and none for smart cards? Why is EMVCo not advocating use of PIN codes? One possible explanation is that mobile devices do not require banks to incur the cost of issuing PINs, or re-issuing them when customers forget, because authentication can be safely delegated to mobile devices. And why is there no discussion of Card Not Present fraud — which costs more than forged Card Present transactions? The answer is mobile. This use case can be addressed with Two-Factor Authentication (2FA). A consumer can validate an online transaction to their bank via 2FA on their registered mobile device.

Viewed from this perspective, the goal becomes clear. That said, new issues are bound to crop up when moving from bank-issued cards to mobile wallets on consumer-owned devices. In an effort to help merchants and other players in the ecosystem, we want to warn those embracing mobile apps and wallets of new risks and avenues for fraud. The underlying infrastructure may be secure, but adoption of mobile payments will shift some liability back onto merchants and issuing banks. We will outline some of attacks on mobile payment ecosystem which many banks and mobile app providers have not yet considered.

Account Proofing

When provisioning a payment instrument a to mobile device, it is essential to validate both the user and the payment instrument. If a hacker has access to someones account — or even just the account Id, they can associate their mobile device with a customer credit card. A failure in the issuing bank's customer Identification and Verification (ID&V) process can allow hackers to link their devices to user cards and make payments. The threat was highlighted this year in what the press called the "Apple Pay Hack". Fraud rates for Apple Pay were roughly 6% of transactions in early 2015 (highly dependent on the specifics of issuing bank processes), compared to approximately 0.1% of card swipe transactions. The problem was not actually inside Apple Pay, but that banks allowed attackers to link stolen credit cards to arbitrary mobile devices. The vetting process becomes far more critical in a mobile payment market. Merchants who attempt to tie credit cards, debit cards, or other payment instruments to their mobile apps will suffer the same problem unless they secure their adjudication process.

Account Limits and Behavioral Monitoring

Merchants have historically been lax with customer data — including account numbers, customer emails, password data, and related items. So when merchants begin to tie mobile applications to debit cards, gift cards, and other monetary instruments for mobile payments, they need to be aware that their apps will become targets. Attackers will use information they have already stolen to attack customer accounts, and leverage payment information to siphon funds out of customer bank accounts. This was highlighted by false reports claiming Starbucks' mobile app had been hacked. The real issue was that customer accounts could be accessed by attackers guessing credentials, and then leveraged for fraudulent purchases. The problem was exacerbated by Starbucks' auto-replenishment feature, which continued to pull funds from the customer bank account, giving hackers access to additional funds. The user authentication and validation process remains important, but additional controls are needed to limit damage and detect misuse. Account limits can help reduce total damage, risk-based reauthorization can deter stolen device use, and behavioral analytics can detect misuse before fraud can occur. The raw security capabilities are available, but mobile apps and back-end systems need to leverage them.

Replay Attacks

Tokens should not be able to initiate new financial transactions. The PAR token is intended to represent an account, and a payment token should represent a transaction. The problem is that as tokens replace PANs in many systems, old business logic assumes a token surrogate is a real credit card number. Logic flaws may allow attackers to replay transactions, and/or to use tokens for 'repayment' — to move money from one account to another. Merchants need to verify that their systems will not initiate payment based on a payment token or PAR value without additional screening. Tokens have been used to fraudulently initiate payment in the past, and this will continue in out-of-date vendor systems.

Recommendations

Migration Recommendation

At Securosis we have a track record of criticizing security recommendations from the major card brands and their Payment Card Industry Security Standards council. Right or wrong, we regarded past recommendations and requirements to be thinly-veiled attempts to shift liability to merchants while protecting card brands and issuing banks. At first impression the shift to EMV-compliant card swipe terminals similarly looks good for everyone *except* merchants.

But when you dig into the details, it's different. When we consider the *whole* picture we see the EMV migration as a major step forward — a win for both merchants and banks. The switch is being sold to merchants almost purely as a liability reduction, but we do *not* expect most merchants to find the liability shift sufficient to justify new terminals, software updates, and training. Fortunately EMV-compliant terminals can also improve consumer experience, and *create commerce opportunities* where previously none existed, both resulting in greater sales volume. The security advantages of tokenization, and a likely reduction in PCI audit costs are purely additive benefits. These factors, in addition to the liability shift, provides ample motivation for most merchants to migrate.

About the Analyst

Adrian Lane, Analyst/CTO

Adrian Lane is a Senior Security Strategist with 25 years of industry experience. He brings over a decade of C-level executive expertise to the Securosis team. Mr. Lane specializes in database architecture and data security. With extensive experience as a member of the vendor community (including positions at Ingres and Oracle), in addition to time as an IT customer in the CIO role, Adrian brings a business-oriented perspective to security implementations. Prior to joining Securosis, Adrian was CTO at database security firm IPLocks, Vice President of Engineering at Touchpoint, and CTO of the secure payment and digital rights management firm Transactor/Brodia. Adrian also blogs for Dark Reading and is a regular contributor to Information Security Magazine. Mr. Lane is a Computer Science graduate of the University of California at Berkeley with post-graduate work in operating systems at Stanford University.

About Securosis

Securosis, LLC is an independent research and analysis firm dedicated to thought leadership, objectivity, and transparency. Our analysts have all held executive level positions and are dedicated to providing high-value, pragmatic advisory services. Our services include:

- **The Securosis Nexus**: The Securosis Nexus is an online environment to help you get your job done better and faster. It provides pragmatic research on security topics that tells you exactly what you need to know, backed with industry-leading expert advice to answer your questions. The Nexus was designed to be fast and easy to use, and to get you the information you need as quickly as possible. Access it at <https://nexus.securosis.com/>.

- **Primary research publishing**: We currently release the vast majority of our research for free through our blog, and archive it in our Research Library. Most of these research documents can be sponsored for distribution on an annual basis. All published materials and presentations meet our strict objectivity requirements and conform to our Totally Transparent Research policy.

- **Research products and strategic advisory services for end users**: Securosis will be introducing a line of research products and inquiry-based subscription services designed to assist end user organizations in accelerating project and program success. Additional advisory projects are also available, including product selection assistance, technology and architecture strategy, education, security management evaluations, and risk assessment.

- **Retainer services for vendors**: Although we will accept briefings from anyone, some vendors opt for a tighter, ongoing relationship. We offer a number of flexible retainer packages. Services available as part of a retainer package include market and product analysis and strategy, technology guidance, product evaluation, and merger and acquisition assessment. Even with paid clients, we maintain our strict objectivity and confidentiality requirements. More information on our retainer services (PDF) is available.

- **External speaking and editorial**: Securosis analysts frequently speak at industry events, give online presentations, and write and/or speak for a variety of publications and media.

- **Other expert services**: Securosis analysts are available for other services as well, including Strategic Advisory Days, Strategy Consulting engagements, and Investor Services. These tend to be customized to meet a client's particular requirements.

Our clients range from stealth startups to some of the best known technology vendors and end users. Clients include large financial institutions, institutional investors, mid-sized enterprises, and major security vendors.

Additionally, Securosis partners with security testing labs to provide unique product evaluations that combine in-depth technical analysis with high-level product, architecture, and market analysis. For more information about Securosis, visit our website: <http://securosis.com/>.