A First Data White Paper

December 2010

Why Wait for EMV to Solve Your Fraud Problems? One-Time Use Card Numbers Can Reduce Debit Fraud Now

By:
Julie Saville,
Vice President, Product Management
and
Nancy Loomis,
Director, STAR Network New Product Development

Introduction

Debit card fraud is a huge issue worldwide, with losses to financial institutions (FIs), merchants and consumers running into billions of dollars annually. According to the American Bankers Association (ABA), industry losses from debit card fraud—including POS signature, POS PIN, and ATM transactions combined—were estimated at $788 million in the U.S. alone in 2008.[1] While that amount may seem relatively low given the size of the industry, consider this: 92 percent of the participants in the 2009 ABA Deposit Account Fraud Survey reported experiencing debit card fraud. Perhaps your institution was among them.

These losses seem even more significant now in the wake of the passage of the Dodd-Frank Wall Street Reform and Consumer Protection Act. Fraud expert Tim Brady of Memento, Inc. points out in a posting on the Bank Fraud Forum blog, "As banks lose more of their ability to generate fee income, it is becoming more apparent that they need to 'rethink fraud' and its impact on the bottom line. Having an 'acceptable' fraud loss budgeted is outdated and perhaps even 'unacceptable'."[2]

Debit card technologies have a direct impact on how well we can prevent or at least limit the fraudulent use of consumers' cards. This is one reason that several large U.S.-based retailers are urging the financial industry to support deployment of chip + PIN cards and applications based on the EMV (Europay, MasterCard and VISA) standard. Given that virtually every geographic region outside the U.S. has already deployed or is currently implementing EMV "chip + PIN" cards, the U.S. market is the last bastion of use for cards based on magnetic stripe technology. Studies have shown that the EMV chip + PIN cards in a specific region or country vastly reduce domestic card present (CP) fraud, but there is a corresponding increase in fraud linked to stolen account information used outside that domestic market. For this reason, many experts predict a tidal wave of fraud will hit the U.S. market soon, especially as Canada converts the majority of its ATMs and debit cards to EMV by the end of 2010.

> ***"As banks lose more of their ability to generate fee income, it is becoming more apparent that they need to 'rethink fraud' and its impact on the bottom line."***
> **– Fraud expert Tim Brady, Memento, Inc.**

However, FIs as well as most retailers in the U.S. aren't in a position to transition from magnetic stripe to EMV chip + PIN cards in the immediate future. Javelin Strategy & Research estimates the transition cost would exceed $8 billion. What's more, other countries have shown that it takes upward of five to ten years to fully transition to EMV. There are new trends showing that even countries that have already adopted EMV chip + PIN within contact terminals are now launching trials using a contactless variation of EMV chip + PIN in order to prepare for digital wallets within mobile phones—a payment trend that is set to explode as the face value of purchases and transactions rises from US$69 billion in 2009 to US$633 billion by end-2014.[3] Additionally, many U.S. industry payment professionals now advocate skipping contact terminals entirely.

Not so coincidentally, there is a new alternative technology to EMV on the market today that can help reduce debit card fraud now. This paper introduces a streamlined solution that can help solve the fraud issues that EMV was created to solve. This approach builds upon current contactless technologies and fits into the current U.S. payments infrastructure at minimal cost to FIs and merchants, allowing them to build on a secure infrastructure that also can accommodate a possible migration to EMV chip + PIN by the international brands in the future. The point-of-sale (POS) solution, STAR CertiFlash™, is a STAR® Network innovation that combats PIN debit card fraud and identity theft in card transactions with advanced, multi-layered security features, without compromising consumer convenience and transaction speed.

Key Takeaways

As you read this paper, we hope that you will take away and consider several key points in the context of your own business processes:

- → The broad implementation of chip + PIN based on the EMV standard in every significant financial market outside the U.S. has solved some fraud problems while creating others. In particular, experts predict that we will soon see much higher levels of magnetic stripe fraud in the U.S. as a result of criminals moving to the market with the weakest security.
- → If EMV adoption in the U.S. should come to pass, it would be expensive and may require implementation over a decade or more. Nevertheless, pressure to fully deploy EMV mounts from international financial markets, large domestic retailers, and even members of the U.S. Federal Reserve Board.

- → Non-EMV smart cards are already in use today in the U.S.; specifically, contactless cards utilize chip technology. Such cards provide increased security measures based on dynamic data elements when compared to our decades-old magnetic stripe technology which uses easily compromised static data.
- → Any payment solution deployed in the U.S. absolutely must accommodate mobile payments, which are on a meteoric rise. Some experts see a direct tie between contactless EMV chip + PIN and near-field communications (NFC), the technology used by the mobile phone.
- → Now there is a streamlined debit payment solution that builds upon current contactless chip technologies in use today. The STAR CertiFlash solution utilizes one-time card number technology to solve the fraud issues that EMV was created to solve, but without imposing high capital costs on FIs and merchants. This solution fits into the current U.S. payments infrastructure at minimal cost, and also can be deployed to customers side-by-side with EMV chip + PIN contactless solutions in the future.
- → STAR CertiFlash has been designed to overcome some of the shortcomings of EMV. For example, EMV chip + PIN uses less secure offline verification of the PIN, whereas STAR CertiFlash uses real-time online PIN verification. What's more, currently deployed EMV technology requires physical contact between the card and the reader—a showstopper for mobile payments. In contrast, STAR CertiFlash uses contactless technology, which is an essential building block for mobile payments. With mobile payment transactions in the U.S. predicted to reach $56.7 billion by 2015[4] , merchants must consider how technologies that are deployed today will position them for the future

Debit Fraud in the U.S.

The problem of payments fraud has existed since the dawn of the use of credit and debit cards. However, as the use of such cards and the amount of money lost to fraud continue to grow each year, the financial industry is taking a closer look at how to combat the problem. In addition, the Durbin Amendment of the Dodd-Frank Act could soon put pressure on FIs to improve their fraud prevention technologies if they want to continue to earn healthy interchange fees for debit transactions.[5]

According to the American Bankers Association, debit card fraud cost the financial industry $788 million in 2008.

What debit card fraud costs us

While there are no precise statistics about the actual cost of payment card fraud, estimates can be extrapolated from various industry surveys and reports—and the estimated figures are staggering. Still, some experts believe they are too low as they don't include all costs associated with fraud, such as the damage to FIs' and retailers reputations, reduced productivity, and increased investments in security and fraud detection/ prevention.

According to the American Bankers Association and Tower Group, approximately 77 percent of payment fraud in the U.S. stems from credit and debit cards. The Smart Card Alliance estimates direct financial losses reached $1.7 billion in 2007, the latest year for which figures are available. The Mercator Advisory Group estimates this figure rises to $16 billion after factoring in indirect costs such as data breach forensics and lawsuits.[6]

Looking specifically at debit card fraud, the American Bankers Association estimated industry losses at $788 million in 2008. This includes all forms of POS signature, POS PIN and ATM transactions combined. First Data conducted an analysis of 56,000 reported debit fraud incidents and identified a number of additional costs associated with fraud, including:[7]

→ Reissuance costs: The cost of reissuing cards, providing consumer correspondence, reactivation campaigns, and other associated activities averages $25 per customer for each event. In 2009, more than 1 in every 4 consumers had their debit or credit cards replaced due to security issues.[8]

→ Reduced reactivation rates: Approximately 20 percent of affected consumers did not reactivate their accounts. Issuers spent an average of $200 per consumer to recoup the lost business.

→ Decreased transaction volumes: Of those consumers who had their cards replaced, 37 to 40 percent say it adversely affects their card usage.

→ Loss of customers: Customers look to their banks and credit unions to protect them from ATM fraud (often resulting from skimming at POS or ATM). Among consumers who are victimized by identity fraud, 17 percent will end up leaving their primary financial institution.

Americans feel most vulnerable about the loss or theft of their personal or financial information. Fifty-four percent of Americans said the prospect of losing this data "extremely concerned" them (based on a rating of eight or higher on a 10-point scale). Losing personal or financial information ranked similar to concern over job loss (53 percent) and not being able to provide healthcare for their family (51 percent).[9]

In summary, these figures and the overall fallout from debit fraud are too significant to ignore. As Memento's Tim Brady points out, it's time to "rethink fraud."

Significant causes of debit card fraud

In recent years, hundreds of millions of payment card accounts have been compromised through merchant and acquirer/processor data breaches. In 2008 alone, more than 285 million consumer records were compromised.[10] Many of these breaches have been linked to international crime rings, which have made a "business" out of card data theft. According to Javelin Strategy & Research, more than 33 million credit cards and 39 million debit cards were replaced in 2009 after account compromises stemming from data breaches. The replacement fees alone incurred by FIs reached $252.7 million.[11] Despite the card replacements, compromised card data has still led to many instances of payment card fraud.

For information on how to stem the losses due to cardholder data breaches, please read the First Data white paper, Where Security Fits in the Payments Processing Chain.

Another significant cause of debit card fraud involves the process of skimming, which is the illegal downloading of the information stored on the magnetic stripe of a debit or credit card, using a small device to capture the data electronically. Some ATM and POS skimming devices have become so sophisticated that they are virtually undetectable by customers and employees. The thief often captures a consumer's PIN via use of a camera in order to match it with the card's account information.

Whether stolen account data is garnered through a skimming device or a data breach, the concern is that it can be used to complete illicit transactions, either in-person (using a counterfeit card) or via phone, mail or Internet. First Data has identified ATM skimming and counterfeiting cards in non-EMV countries as two of the top fraud trends in 2010.[12]

Authentication: Signature Debit versus PIN Debit

Using a signature on a POS terminal or a printed receipt is a much weaker form of authentication than entering a multi-digit PIN. Fraud losses to FIs average about 7.5 basis points for signature debit, and 1 basis point for PIN debit, according to management consulting firm Oliver Wyman. But despite the security risk, issuers enjoy the higher income derived from signature debit transactions, and have not had much incentive to encourage PIN rather than signature transactions. In fact, many issuers actually encourage their customers to use signature debit by offering loyalty rewards based on signature debit use.

At least one bank, however, has found signature debit fraud to be so rampant in certain states that the bank has forbidden these types of transactions in those locales. In August of 2010, Bonneville Bancorp suspended signature debit transactions in three states "for the foreseeable future" until the company can evaluate how to address the fraud.[13] PIN debit, however, will continue to be accepted.

Authorization: Online versus Offline

One of the reasons the U.S. payments industry continues to use cards based on magnetic stripe technology is our robust and reliable system for authorizing payments online. The system, which is built upon always-available high speed communications, contains numerous real-time fraud detection measures that help prevent fraud by denying suspect requests for payment.

In Europe and other regions, payments are frequently authorized offline at the POS. Historically this is due to poor or unreliable communication systems that can't support real-time authorization via the payment network. In this environment, EMV chip + PIN technology is necessary to authenticate the cardholder and authorize the payment based on information stored on the chip, as described below.

The EMV standard, use cases and benefits

The EMV global interoperability standard was originally developed by Europay, MasterCard and VISA in 1999 and is now maintained by EMVCo, LLC. The standard defines how smart cards embedded with a chip interact with POS terminals and ATMs for authenticating credit and debit card transactions. Payment cards based on chip technology are more secure than magnetic stripe cards because it's harder to steal and clone the sensitive cardholder data from the embedded chip. In addition, the chip contains information that can authenticate a legitimate cardholder and authorize a payment, even when transactions are conducted offline.

Payment cards based on chip technology are more secure than magnetic stripe cards because it's harder to steal and clone the sensitive cardholder data from the embedded chip.

With EMV chip + PIN cards, the consumer's PIN is encoded onto the chip, along with the primary account number (PAN). When the consumer swipes/inserts/taps his card with a reader, the PIN that he enters at the POS terminal is compared to the PIN embedded on the chip. This form of user authentication is especially important in Europe and other regions where payment authorization is frequently an offline process. At the very least, the merchant's POS terminal or an ATM can authenticate the consumer based on something he has (the card) as well as something he knows (the PIN). Theoretically, this prevents the use of a cloned white plastic card in a card present situation where a chip-enabled card is expected. (Of course, this assumes that merchants are no longer accepting magnetic stripe cards. However, in most EMV implementations, magnetic stripe cards are accepted for a period of years until they can be phased out.)

Some EMV chip + PIN cards also store the value of a consumer's account on the card. When a purchase is made, the value is decremented from the card. This takes the place of real-time authorization and, in the case of debit cards, real-time decrementing of the consumer's demand deposit account.

In addition to the reduction of credit and debit card fraud worldwide, there are other possible benefits of EMV-enabled smart cards, such as:

→ Growth of card-based transactions, as secure offline "anytime, anywhere" transactions are now possible
→ Multi-application interoperability as one card can support multiple applications
→ New innovative concepts based on the EMV standard; for example, loyalty programs and mobile payments

A Look at the Worldwide Use of Chip + PIN Based on the EMV Standard

EMVCo reports that, as of 2009, there were more than 944 million EMV compliant chip-based payment cards in use worldwide—virtually all of them outside the United States. In many countries, the central bank is backing the move to EMV-enabled cards, which despite the initial implementation costs is expected to save FIs and merchants money in the long run due to reduced fraud costs. Moreover, the cards hold the promise of new revenue sources as they provide a platform for launching new value-added services.

Europe, in particular, has embraced EMV chip + PIN cards, largely due to a mandate from the European Payments Council (EPC) as part of the full implementation of the Single Euro Payments Area (SEPA). The EPC has been driving a single rulebook so that more than 8,000 banks throughout Europe can process credit and debit payments in a standard fashion. Due to the success of EMV in Europe, the EPC recently announced that it's considering a ban on magnetic stripe cards within the next couple of years.[14]

Adoption of the EMV standard in Asia/Pacific has been relatively swift. Government mandates, fraud prevention initiatives, and industry competition are driving adoption in Japan, Malaysia, Korea, Indonesia, Taiwan, Australia and many other countries. One sign of progress is the number of EMV-compliant cards being issued, and as of 2008, more than 40 percent of the total payment cards issued in Japan and Cambodia were EMV-compliant.[15]

In the Middle East, the United Arab Emirates central bank is encouraging FIs to move to EMV. In Africa, South Africa has seen swift adoption, with more than a million MasterCard-branded EMV cards issued by the end of 2008, and more than one-fourth of all POS devices upgraded to accept EMV cards.[16] In the Americas, Canada, Brazil and Mexico are far along in their deployments. Canada's payment association Interac has set deadlines for the industry: all ATMs in the country must be EMV chip + PIN compliant by the end of 2012, and merchant terminals must be compliant by the end of 2015.

In the realm of major financial markets, the U.S. stands alone in its hesitancy to adopt EMV. As we'll explore in more detail below, there are many reasons for this hold-out position.

The impact of EMV chip + PIN on fraud

As one of the earliest adopters of EMV chip + PIN cards, the United Kingdom has been a sort of pilot program for other countries which are observing the results. First Data confirms that payment card fraud losses in the U.K. dropped from 18 basis points to 12 basis points between 2001 and 2008 as a direct result of EMV adoption.

However, the U.K. Payments Administration (formerly APACS) says the U.S. reluctance to adopt EMV is impacting the U.K. market. According to APACS, domestic card fraud in the U.K. dropped 32 percent in 2007, while counterfeit card fraud increased by 46 percent the same year. APACS claimed the increase was "due to fraudsters copying U.K. cards and using these stolen cards in countries which do not yet have chip + PIN."[17] The situation improved somewhat by 2009, when APACS reported card-not-present (CNP) fraud dropped by 19 percent and showed the first ever decrease since 1999. APACS cites the increasing use of sophisticated fraud screening detection tools by retailers and banks as the reason for the decrease.

In all, the success of chip + PIN has meant that losses on retail transactions in the U.K. have declined by 67 percent, from £218.8m in 2004 to £72.1m in 2009.[18] This is certainly good news for FIs and merchants that made the significant investments necessary to deploy the technology.

Below are some of the specific types of fraud that EMV chip + PIN has been able to address:

→ Mail non-receipt of cards
→ Lost and stolen cards
→ Counterfeit fraud within the geographic footprint of the issuer
→ ATM skimming losses when the ATMs are EMV-compliant

Despite the progress, eCommerce fraud continues to be a concern. In the 10th Annual CyberSource Survey report from 2008, it was reported that thieves stole $4 billion from online merchants, a figure that increased from $3.7 billion in 2007. Unfortunately, EMV chip + PIN does little to reduce CNP fraud.

The Current State of Card Technologies in the U.S. Market

An estimated 5 billion magnetic stripe payment cards are in use worldwide. There are 15 million magnetic stripe POS terminals in the U.S. alone, according to market researcher The Nilson Report. This is an enormous amount of infrastructure to support payments initiated via magnetic stripe cards. Despite the international pleas to bring EMV chip + PIN payments to the U.S. market, it's not likely to happen in the near term—if it happens at all. To do so could be compared to ripping out our entire national highway system to replace it with high speed trains.

Are EMV-enabled payments inevitable in the United States?

No one knows for certain if EMV is inevitable for the U.S. market. Even proponents believe we need more incentives to make the transition. Consider the statement made by Richard Oliver, Executive Vice President of the Federal Reserve Bank of Atlanta's Retail Payments Risk Forum: "We may become the only substantial economic power dependent on a payments standard that is less secure than that of the rest of the world." Oliver suggests it's time for the U.S. government to develop a "well-thought-out, participatory, multi-year plan to move this country to the emerging global payments standard."[19]

> **"We may become the only substantial economic power dependent on a payments standard that is less secure than that of the rest of the world." – Richard Oliver, Executive Vice President, Federal Reserve Bank of Atlanta**

Certainly one incentive is the idea of a dramatic drop in CP fraud, as Europe has seen. Another incentive might be that EMV provides a technological platform for launching value added services and new products in the future, such as self-service POS stations, loyalty applications on the payment chip card, and offline payments in remote locations. Can you envision a small vendor at a weekend farmers' market being able to accept an offline debit payment using a palm-top POS in exchange for his fruits and vegetables? The convenience of such offline payments could dramatically increase the total volume of electronic payments overall, and along with it, increase FIs' revenue from interchange.

The Durbin Amendment could potentially provide another incentive to implement EMV. Some industry pundits interpret this law to mean that the Federal Reserve Board could allow higher interchange rates for FIs that adopt the strong security measures of EMV. This is all speculation at this point, however, and may never come to pass.

Global retailers based in the United States are also pushing for EMV-enabled chip + PIN payments. Such merchants have had to deploy EMV-compliant solutions in their stores outside the U.S., and now they would like to implement this same payment standard for all of their stores worldwide. In fact, all of Wal-Mart's U.S. payments terminals are able to accept chip + PIN transactions today; however, the merchant has not yet developed the software and other payments processing technologies the transactions require for the U.S. market.[20]

Considerations for Bringing EMV to the U.S. Market

If there are so many benefits of EMV chip + PIN, and it is already entrenched in every other major financial market in the world, what is holding the U.S. market back from adoption? Let's have a look at some of the considerations for bringing EMV to the United States.

Time and cost for full deployment

Perhaps the biggest barrier to implementing EMV chip + PIN in the United States is the time and cost that would be required for full implementation. Just what would it take to replace 15 million point-of-sale devices[21], more than 360,000 automated teller machines[22] , 576.4 million credit cards, and 507 million debit cards?[23] Javelin Strategy & Research pegs the total cost at $6.75 billion to replace all those POS terminals; an additional $1.4 billion to issue EMV-compliant cards; and about $500 million for ATM upgrades. All told, it's at least an $8 billion proposition to implement the new anti-fraud technology.

A significant portion of the cost will be borne by merchants who already balk at the burden that card security places on their businesses. For example, multi-lane merchants are likely to spend at least $500 per lane in the migration process.[24] And unlike Europe, U.S. banks have little influence over the merchant card processing infrastructure, so banks cannot dictate the use of EMV chip + PIN.

Dual cards and applications...for a while

Of course, the transition to EMV chip + PIN can't happen overnight, so there would be a period of time – likely five to ten years – when FIs and merchants would need to support the old magnetic stripe cards as well as the new chip-based cards. This is precisely what has happened in every market that has already adopted EMV. This means that interim cards, equipment and applications may be required; for example, an EMV-compliant card that also has a magnetic stripe on the back for use at retail locations and ATMs that have not yet deployed EMV.

Many merchants in Europe traded their magnetic stripe card reader for an EMV card reader and now cannot (or will not) accept a magnetic stripe card. This has put Americans at a disadvantage when traveling abroad because many merchants and various kinds of kiosks don't accept the American consumers' magnetic stripe payment cards. The problem is expected to grow as Canada and Latin America progress in their roll-outs of EMV-compliant environments. According to The Nilson Report, many issuers in the U.S. will accommodate their top customers by providing them an EMV-compliant card to be used abroad.[25] There's a lesson to be learned from this situation: if EMV does eventually roll-out in the U.S., merchants will need to accept both magnetic stripe and EMV cards for a time so as not to inconvenience customers and lose business.

For FIs, the process of distributing new EMV-compliant cards can be factored into the normal three-to-five year lifecycle of card replacement. Today's magnetic stripe-only cards are being replaced with hybrid cards that have both a magnetic stripe and a chip for contactless. In the next upgrade cycle, the cards could include an EMV chip and possibly eliminate the magnetic stripe. In this way, the process of replacing cards would include the incremental cost of the EMV chip, but it wouldn't require a wholesale upgrade of tens or hundreds of millions of cards at once.

Trends in contactless and mobile payments

The EMV solutions that have been deployed around the world to date have almost exclusively been based on contact cards; that is, physical contact between the card and the card reader is required. The unfortunate aspect of this required contact is that it's at odds with the growing market for mobile payments, such as using a chip-enabled smart phone to make a purchase. EMV-compliant applications on contactless cards and other devices are now being tested in Europe; however, when EMV implementation initially began some years ago, there wasn't much demand for contactless and mobile payments, as there is today. The European market, therefore, did not plan ahead for these emerging technologies, and will need to develop a migration plan to implement contactless EMV chip + PIN in the future.

MarketResearch.com estimates that mobile payment transactions in the U.S. will experience a compound average growth rate of almost 50 percent by 2015, reaching a value of $56.7 billion by then. The firm further estimates that the U.S. market in 2015 will represent 11 percent of the global mobile payment transactions business.[26] A movement to EMV in contact-only mode would be a severe hindrance to this natural growth in mobile payments.

The U.S. market has the opportunity to leapfrog the EMV contact-only technology and go straight to a contactless implementation of EMV, according to Steve Mott of the consulting firm BetterBuyDesign. "Contactless EMV is a lot more affordable for merchants, who will bear three-quarters of the cost to move away from magnetic stripe acceptance, so why not start with EMV contactless?" asks Mott. "PINs can be required for higher-dollar, higher-risk transactions."[27]

> ***"The issue to me seems more of an issue of contact versus contactless EMV. It's really hard to think about how you would get to mobile NFC without either going through a phase or implementing some aspect of the EMV chip + PIN associated with cards."***
> **– Richard Oliver, Federal Reserve Bank of Atlanta**

Richard Oliver of the Federal Reserve Bank of Atlanta sees a direct connection between mobile payments and the issues of magnetic stripe and EMV chip + PIN. "I certainly believe there is a tie between EMV chip + PIN and mobile, simply because of the technologies involved," Oliver explained in an interview with Bank Information Security. "While EMV chip + PIN has been implemented in Europe, for example, as a contact technology, where the card actually is passed through the machine and there is contact, card technology using chip + PIN is on the rise in many different forms and different pilots." He adds, "EMV is also developing a contactless technology for near-field communications or NFC, which is the technology that will be used by the phone. So, consequently, the issue to me seems more of an issue of contact versus contactless EMV. It's really hard to think about how you would get to mobile NFC without either going through a phase or implementing some aspect of the EMV chip + PIN associated with cards."[28]

Whether or not the U.S. market eschews contact-only chip + PIN and goes straight for a contactless implementation, we must accommodate the growing need for contactless and mobile payments. This isn't as hard as it sounds. The Smart Card Alliance explains that U.S. and EMV contactless cards use identical construction and communication protocols, and as a result, the physical contactless reader interface is the same for both U.S. and EMV contactless cards. What differs is the logic within the card application. Contactless, then, is a good lead-in technology that can take the U.S. market to EMV chip + PIN in the future.

A Chip + PIN Solution for the U.S. Today

At best, it would be a decade before EMV chip + PIN could be fully deployed in the United States, and unless we leapfrog contact-only and directly deploy contactless EMV, the implementation would be obsolete before it's complete due to the swift uptake of mobile and contactless payments. Rather than wait for EMV and watch losses from fraud mount in the meantime, FIs have a new option that's available today for a hybrid solution of EMV chip + PIN and contactless which has been strengthened with stronger security using one-time card numbers. And, this debit solution fits right into the current U.S. payments system.

STAR CertiFlash is a new patent-pending PIN-based solution that advances POS security using one-time card number technology. The STAR CertiFlash technology is programmed onto a contactless chip embedded within a payment device. For each transaction a consumer makes, the chip encrypts and transmits a card number that is good for only a single use.

The STAR CertiFlash technology is programmed onto a contactless chip embedded within a payment device. For each transaction a consumer makes, the chip encrypts and transmits a card number that is good for only a single use.

STAR CertiFlash has added several layers of security over and above other contactless products that are currently available. These layers include fraud mitigation technologies to prevent consumer card number exposure to merchant data breach, skimming, and frauds due to stolen cards—the same threats that EMV was designed to combat.

Avivah Litan, a vice president and analyst at Gartner Inc., a market research company based in Stamford, Conn., calls STAR CertiFlash a "good, practical technology" that can help combat card fraud.[29] According to Litan, "If criminals steal the data they can't use it again."[30] This is critical for organizations across the payments systems, as rising fraud threatens profits, as well as relationships with customers. When it comes to card purchases, consumers view security as a growing concern. Among consumers who are impacted by fraud, Javelin Strategy & Research found that 17 percent would ultimately leave their primary financial institution, while 43 percent would avoid merchants they believe could compromise their data again.[31]

What's necessary for implementation of the one-time number solution

Implementation of a one-time card use technology like the STAR CertiFlash solution is potentially less costly and less complex than implementing EMV, and it can be deployed now and take the market into the years ahead—even if EMV is eventually rolled out. To take advantage of this solution, STAR's bank partners need to reissue debit cards or other types of payment devices with an embedded contactless chip with a custom STAR CertiFlash application installed on it and activated by the bank. The STAR CertiFlash application can reside side by side on the chip with other applications, such as those from MasterCard, Visa or some other network. In the future, those networks could likely deploy a variation of EMV chip + PIN, which can also reside on the same chip as STAR CertiFlash, thus increasing the value of the card because it can support more services. To ensure the use of the secure one-time card number at the POS, the bank should define a preference for merchants' card readers to use the STAR CertiFlash application ahead of other debit applications.

Merchants need to have or install contactless card readers with the STAR CertiFlash application on them. For merchants who already have contactless readers, this could mean in many cases a simple firmware download can add the CertiFlash application support on the reader.

The "heavy lifting" of how this solution works is done by the STAR Network as described in the following section. A pilot program involving the STAR CertiFlash technology, launched October 6, 2010, and STAR member banks will run until the end of 2010, with full commercial roll-out of the solution intended for early 2011.

How the one-time card number technology works

The consumer taps the payment card or other device on the contactless reader. The chip in the device creates a one-time card number that is passed to the merchant terminal and is carried in the transaction. The light on the contactless reader flashes, indicating the card has been read.

The terminal determines whether a PIN is required and prompts the consumer to enter his PIN if necessary. The PIN is required for transactions greater than $25 or when cash back is requested. The $25 limit is a starting point and may be raised or lowered. The terminal then sends the transaction to the STAR Network.

The transaction data read from the chip includes a one-time card number, transaction counter and dynamic cryptogram. STAR uses a hardware cryptographic process to translate the one-time card number back to the real PAN and to validate the dynamic cryptogram, then STAR validates the transaction counter prior to passing the transaction with the real PAN to the financial institution for funds authorization. The financial institution validates the PIN (if present) and verifies funds availability to then respond with an approval or denial.

The merchant's terminal receives the authorization response and completes the transaction by printing the customer receipt, just like any other transaction. The last 4 digits of the consumer's real PAN number are printed on the receipt to assist in reconciliation.

The security advantages of this approach

There are numerous security advantages afforded by this approach to debit payments. The chart below compares this new one-time number contactless solution to magnetic stripe cards and traditional contactless programs.

Limitations of Current Magnetic stripe Cards and/or Other Contactless Programs	Advantages of STAR Contactless with a One-Time Use PAN
No encryption of private data (PAN, name, etc.).	Encryption isn't necessary as a one-time use only number is generated that is not tied to the consumer's account.
Easily skimmed and reproduced as a white plastic to be used to withdraw money at ATMs.	Any data skimmed is not usable to withdraw cash at ATM or initiate transactions at a POS terminal.
Consumer's name is contained in the transmitted data.	Consumer name is not contained in the information generated. The name cannot be reconstructed from the information available.
Card number and expiration date are same between card face and magnetic stripe or chip, allowing for easy fraudulent replication.	The information on the card face is encrypted on the chip but since the PAN number is different for each transaction, it cannot be used to conduct another transaction.
Consumer names and card numbers are stored in merchant records.	The consumer's name and real PAN number are never exposed to merchants or their processors.
No set limit to require additional authentication for large purchases.	Purchases over $25 (or amount specified by merchant) triggers PIN-entry requirement for additional security.
Magnetic stripe cards that are signature based incur more fraud, and they do not allow cash back	Any cash back requests associated with a purchase will also trigger PIN-entry requirement

There are other benefits as well:

- The STAR CertiFlash application is compatible with EMV standards. When and if the U.S. financial industry goes to pure EMV, the STAR CertiFlash application specification does not need to be modified. The two applications can reside on the same chip.
- The STAR CertiFlash application for a one-time card number offers customer convenience, especially for low-value transactions that don't require PIN entry. The consumer can simply tap his card/payment device at a reader and be done. In addition, consumers can be assured that their transactions are secure and their cards are not vulnerable to skimming, data breaches and other concerns.
- Integration within a card is the first step in the STAR CertiFlash road map. This application also can be embedded into payment fobs and payment stickers and is designed to support mobile payments. Eventually it will be migrated to the Internet to support web-based payments as well, helping to curtail CNP fraud.

Conclusion

Fraud is a problem for all types of electronic payments, and there is no single silver bullet that will address all areas of fraud. Unfortunately, we need to apply numerous security measures and anti-fraud technologies in order to cover all bases and stay ahead of (or catch up to) the techniques used by fraudsters.

The U.S. payments industry is being nudged (or some might say "shoved") in the direction of adopting EMV chip + PIN technology. While the industry continues to debate full EMV deployment, STAR CertiFlash is available today to address the security issues EMV was designed to address. STAR CertiFlash is EMV-compatible; contactless to support mobile payments; and strengthened with even more security than EMV by using one-time card numbers. Moreover, this solution continues to function within the advanced real-time authorization systems that are an advantage the U.S. has over other countries.

FIs and merchants can address the costly issue of debit fraud and provide a value-add service to customers by implementing one-time card number technology at the POS. This solution is commercially available today and is easy to deploy. Moreover, it is a logical step toward EMV payments as well as mobile and Internet payments in the future.

Sources:

[1] American Bankers Association, 2009 ABA Deposit Account Fraud Survey, 2009

[2] Tim Brady, "One Year Later—A Veteran's Perspective," July 21, 2010

[3] Portio Research, "Mobile Payments 2010-2014"

[4] Mobile Marketing and Technology, "Mobile Payments Will See 55% User Growth," Gary Kim, October 13, 2010

[5] Smart Card Alliance, "Will the Durbin Amendment lead to Chip + PIN in the US?" June 23, 2010, http://www.smartcardalliance.org/articles/2010/06/30/will-the-durbin-amendment-lead-to-chip-pin-in-the-us

[6] Smart Card Alliance white paper, "Fraud in the U.S. Payments Industry: Fraud Mitigation and Prevention Measures in Use and Chip Card Technology Impact on Fraud," October 2009, p. 5-6

[7] First Data, "The True Cost of Fraud," March 2009

[8] June, 2010 Data Breach Prevention and Response: Causes, Consumer Consequences, and Tools for Layered Defense, Javelin Strategy and Research

[9] National Cyber Security Alliance, Anti-Phishing Working Group survey, August 2010

[10] Verizon Business RISK Team, "2009 Verizon Business Data Breach Investigations Report," 2009

[11] Robert Siciliano, "Credit Card Data Breaches Cost Big Bucks," Jul 8, 2010, www.infosecisland.com

[12] Rick Van Luvender, First Data, "Fraud Trends in 2010: Top Threats From a Growing Underground Economy," April 2010

[13] American Banker, "Fraud Woes Prompt Bank to Forgo Signature Debit Revenue," August 19, 2010, http://www.americanbanker.com/issues/175_159/signature-debit-1024299-1.html

[14] Beverly Blair Harzog, "U.S. magnetic stripe credit cards on brink of extinction?", August 4, 2009, www.creditcards.com

[15] Banking & Payments Asia, "EMV: The Story So Far," May 2009

[16] Banking & Payments Asia, "EMV: The Story So Far," May 2009

[17] Tracy Kitten, www.bankinfosecurity.com, "Is U.S. Ready for Chip & PIN?" Jun 1, 2010, http://www.bankinfosecurity.com/articles.php?art_id=2593&pg=2

[18] U.K. Payments Administration, Card Fraud Facts and Figures, http://www.ukpayments.org.uk/resources_publications/key_facts_and_figures/card_fraud_facts_and_figures/-/page/645/

[19] Richard Oliver, Federal Reserve Board of Atlanta, "Soccer balls and payment cards: A push for global standards," Portals and Rails blog sponsored by the Retail Payments Risk Forum of the Federal Reserve Bank of Atlanta, July 19, 2010

[20] Kate Fitzgerald, "Wal-Mart Claims Issuers Block Progress of EMV Cards in U.S.," American Banker, May, 2010

[21] The Nilson Report

[22] ATM & Debit News says there were 360,659 ATMs in service in 2007

[23] Ben Woolsey and Matt Schulz, "Credit card statistics, industry facts, debt statistics," http://www.creditcards.com/credit-card-news/credit-card-industry-facts-personal-debt-statistics-1276.php

[24] "How Soon 'til United States of Chip and PIN?", Digital Transactions, October 2010

[25] "Chip Cards in the U.S.," The Nilson Report, #930, July 2009

[26] Mobile Marketing and Technology, "Mobile Payments Will See 55% User Growth," Gary Kim, October 13, 2010

[27] "How Soon 'til United States of Chip and PIN?", Digital Transactions, October 2010

[28] Tracy Kitten interview of Richard Oliver, "EMV, Chip & PIN, Contactless Payments," Bank Information Security, November 3, 2010

[29] American Banker, "First Data Antifraud System Relies on Contactless Chips, One-Time Card Numbers," August 27, 2010

[30] DigitalTransactionsNews, "With CertiFlash, Star is First EFT Network to Offer Contactless," August 26, 2010

[31] ATM & PIN Fraud, Javelin Strategy & Research, February 2010

The Global Leader in Electronic Commerce

First Data powers the global economy by making it easy, fast and secure for people and businesses around the world to buy goods and services using virtually any form of payment. Serving millions of merchant locations and thousands of card issuers, we have the expertise and insight to help you accelerate your business. Put our intelligence to work for you.

About The Authors

Julie Saville is vice president, Product Management, for First Data's STAR® Network. Saville joined STAR in 1991 and currently manages product development for the payments network.

During her tenure, the network has introduced such market-leading services as the STAR Prepaid Reload Network, STARsf surcharge-free network and STAR Expedited Transfers. Most recently, she has overseen the development of STAR CertiFlash, a contactless solution that protects debit transactions with multiple security layers, including the generation of one-time card numbers; and the product launch of STAR Online Partner, which allows STAR cardholders to link their card to a PayPal account online.

Saville's career spans more than 30 years of EFT expertise. Before she began managing major product initiatives at STAR, she held several management positions — which included vice president, EFT Product Management; EFT Business/Systems Analysis; and EFT operations management — for Great American First Savings Bank, a savings bank with $17 billion in assets.

Saville earned a bachelor's degree in marketing from San Diego State University and a master of business administration in computer information systems from National University in San Diego.

Nancy Loomis is a Director in the STAR® Network product development and management group. Nancy is the product owner for STAR CertiFlash, a PIN debit secure contactless solution – a First Data enterprise-wide initiative.

Nancy was a key force in developing and promoting the STAR Biller-Direct service, and previously managed key product initiatives from the technology perspective from the STAR Processor Relations group. Nancy has also managed numerous STAR internet and alternative business opportunities including mobile banking and payments.

Nancy has been active in the industry and has worked collaboratively with other networks and payment systems – such as with the NACHA Internet and NACHA Electronic Billing and Payment Councils - to further electronic payments. Nancy served as the work group leader for the successful Internet Secure ATM Purchase pilot (ISAP) that was facilitated by NACHA and piloted by STAR in 2001.

Prior to joining STAR in 1991, Nancy worked in the branch and systems retail banking divisions of Great American First Savings Bank. Nancy earned her Bachelor's and Bilingual Education degrees from San Diego State University.

For more information, contact your
First Data Sales Representative
or visit firstdata.com.

The information contained herein is provided as a courtesy and is for general informational purposes only. This article is not intended to be a complete description of all applicable rules, policies and procedures. The matters referenced are subject to change. Individual circumstances may vary. The information contained herein includes, among other things, a compilation of documents received from third parties. First Data shall not be responsible for any inaccurate or incomplete information. Nothing contained in this presentation is intended to supplement, amend or modify any applicable contract, rule or regulation.