The Long Road to EMV

An In-Depth Look at EMV & How It Will Impact IADs

Sponsored by

ATMIA and Kahuna ATM Solutions

As the staggering amount of losses attributed to card fraud attest, it's not difficult to copy or skim data from a magnetic stripe and create a duplicate card that can be used at any ATM or point-of-sale terminal. Criminals around the world buy and sell stolen card data and the means to create fake cards. The technology to this is not complicated and it's relatively inexpensive.

— David Tente, ATMIA

Why is the U.S. Moving to EMV?

ATM security is an on-going arms race. Like the days of the Cold War, one side gains a technological advantage and then the other side finds a way to defeat it.

With the advent of the EMV standard, the payment card industry feels they have developed the mother of all deterrents to crime.

EMV, which stands for Europay, MasterCard and Visa — three of the major card brands that developed and adopted the smart card technology, incorporates a microchip embedded with cardholder data and software. The chip holds more data than the mag stripe, including new data that is unique to EMV, and is also capable of storing multiple payment applications.

EMV technology provides a set of requirements to ensure interoperability between chip-based payment cards and acceptance devices. The card brands, American Express, JCB, MasterCard and Visa, established EMVCo to manage the EMV specification and ensure global interoperability of chip-based payment cards with acceptance devices, including ATMs and point-of-sale terminals.

An EMV card is the same size and thickness as a standard magnetic-stripe card. However, it includes a contact on the front of the card which accesses a microprocessor embedded in the small cavity behind the contact plate. EMV transactions require chip contact throughout the process. This will change the current card swipe practice.

So far, criminals have not been able to clone or create fake EMV cards.

Sponsored by

ATMIA ATM INDUSTRY ASSOCIATION

KAHUNA ATM Solutions

According to the Smart Card Alliance, a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology; chip cards are more difficult to copy because the card includes a secure microprocessor chip that can store information securely and perform cryptographic processing during a transaction. The credentials prevent card skimming and cloning.

"As the staggering amount of losses attributed to card fraud attest, it's not difficult to copy or skim data from a magnetic stripe and create a duplicate card that can be used at any ATM or point-of-sale terminal," says David Tente, Executive Director of the ATM Industry Association (ATMIA) U.S. Chapter.

"Criminals around the world buy and sell stolen card data and the means to create fake cards. The technology to do this is not complicated and it's relatively inexpensive."

Historically, skimming has been a larger problem in Europe and other countries than it is in the United States. Since the implementation of EMV, fraudulent withdrawals have fallen in countries that have adopted the standard and shifted to markets that still rely on the mag stripe card.

Most of the world has already or is in the process of implementing EMV, including Europe, Canada, Africa, Mexico, Latin America, the Caribbean, the Middle East and Asia-Pacific countries.

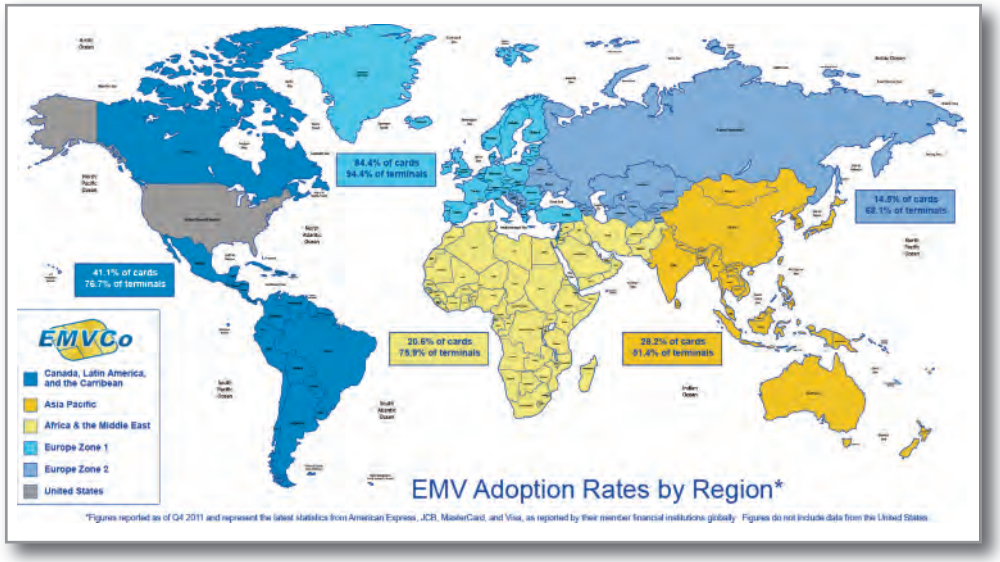
The U.S. market was one of the last holdouts, until Visa and MasterCard announced their liability shift timetables in August 2011.

EMV by the Numbers

Worldwide Adoption

45% **of the world's payment cards are EMV capable**

76% **of the world's payment terminals are EMV capable**



EMV's Impact on Fraud

25% **Australian drop in skimming**

36% **reduction in fraud in Europe**

69% **UK decline in fraud**

80% **decline in fraud in Brazil**

84% **Malaysian counterfeit decline**

Source: EMVco

Steps to EMV Migration

1. ***Agreement on Debit Solution***
2. ***Network Testing & Certification***
3. ***Processor Testing & Certification***
4. ***ATM Testing & Certification***
5. ***Installation of Software & EMV Level 1 Card Reader on ATMs***

The Long Road to U.S. EMV Migration

Although the card brands have announced deadlines for the liability shift, there is, technically, no mandate compelling ATM owners and operators to upgrade their terminals to EMV technology. The deadlines are for the liability shift. Any party in the chain that is not EMV compliant could be held liable for fraud losses that occur after the deadline.

The full liability shift for ATM MasterCard transactions is scheduled for Oct. 1, 2016. Visa has scheduled its ATM liability shift for Oct. 1, 2017.

"There are many steps that must be taken before EMV transactions can be processed at ATMs in the United States," says Tente, who represents the ATM industry on the EMV Migration Forum, an independent, cross-industry body created by the Smart Card Alliance to address issues that require broad cooperation and coordination to promote the effective migration to EMV-enabled cards in the United States.

"To accept and process EMV transactions, each step in the transaction process — the networks, processors and ATM manufacturers — must test and certify software to the EMV standard. Then the software must be installed on ATMs and each ATM unit must have an EMV-capable card reader installed."

A Common EMV Standard

However, before any of that can be done, a common EMV debit standard or Application Identifier (AID) consistent with network routing requirements established under the Durbin Amendment to the Dodd-Frank Wall Street Reform and Consumer Protection Act that can still allow routing choice, must be agreed upon for the United States.

An AID is the numerical code that points to an application on the chip embedded on the card. There may be multiple AIDs on a chip when you have debit and credit on the same card, or both domestic and international debit. In order to initiate the transaction, the network, terminal and card must have an AID in common.

"Agreement on a debit solution is a major step in moving along the path to EMV implementation," says Tente.

It's one of the differences in the U.S. market compared to other countries, he continues. In many countries, there are only one or two debit-processing networks. In the U.S. there are numerous privately owned networks. To simplify the acceptance and routing of transactions, issuers and networks must agree on how applications and AIDs will be implemented on the card.

As part of an acquirer's EMV migration, ATMs must be configured to support AIDs that are appropriate for ATM transactions, and POS terminals must be configured to support AIDs that are appropriate for POS transactions.

Per the EMV specifications, when a chip card is used at a chip-enabled ATM or POS device, the card and the terminal must have at least one AID in common in order for the transaction to proceed. In a country with only one debit-processing network, the same AID is used by everyone.

Determination of a debit solution is essential for the EMV adoption process to move forward. The Secure Remote Payments Council, a group of non-card brand regional debit networks, adopted a common debit AID application based on a solution from Discover. However, other networks have not yet adopted it. Without an agreement on a common AID, there could be at least three in the U.S. — one for MasterCard, Visa and Discover.

"Until there is an agreement involving both Visa and MasterCard, ATM owners really don't know where to start," said Bryan Bauer, President of Kahuna ATM Solutions. "The lack of a common debit solution could severely impact the readiness of the ATM industry to meet the liability shift deadlines."

And there is reason to worry, says Tente.

Network officials are saying certification in the U.S. will take at least six months. "In Canada it took as long as two years for Visa to complete certifications and there's only one debit network there. The U.S. market is much more complex and EMV transactions must meet network routing requirements established under the Durbin Amendment," he says.

Once a debit solution is agreed upon, software must be developed, tested and certified by the networks. The software must then be rolled out to acquirers and operators for their own testing and certification, says Tente.

Agreement on a debit solution is a major step in moving along the path to EMV implementation in the U.S.

In many countries, there are only one or two debit-processing networks. In the U.S. there are numerous privately owned networks. To simplify the acceptance and routing of transactions, issuers and networks must agree on how applications and AIDs will be implemented on the card.

Although most ATM models in the field today have already been certified in other countries, each manufacturer will have to have their terminals certified on U.S. networks. Only then will EMV software be ready to be installed on ATM machines with an EMV-capable card reader in the field, he says.

"The move to EMV in the U.S. should have started two years ago to realistically meet the liability shifts set by the networks," says Stuart Mackinnon, President of Columbus Data Services. Columbus Data serves financial institutions, ATM operators and merchants with over 73,000 ATMs.

Even though CDS has completed the required processor certifications and have terminals processing EMV live today, the sheer number of manufacturers, models and configurations that remain to be certified for our customers is substantial, says Mackinnon.

It's a time consuming process with each ATM taking about a month to certify, he says. Couple that with the fact that the current certifications may not guarantee interoperability once the U.S. Debit AID decisions are made and it adds up to uncertainty and added costs for everyone involved.

"All of this takes time and time is running out," says Tente.

Working Towards a Realistic Deadline for Migration

ATMIA and other industry groups have asked the networks to delay their liability shift deadlines; requesting a realistic, consistent deadline for chip card migration for ATM deployers and operators in America.

One EMV milestone has already passed. MasterCard implemented a liability shift for all counterfeit ATM transactions performed on the Maestro debit network on April 19, 2013.

The Maestro liability shift caused quite an uproar in the industry.

According to a survey of ATM owners and operators conducted by ATMIA, an overwhelming majority (88 percent) of respondents said they would not be able to deploy a single EMV-capable ATM by the April 2013 liability shift. Only nine percent of respondents said they even had access to solutions that would be required for the processing of EMV transactions.

Prior to the April liability shift, MasterCard announced a new set of acquirer-based fraud detection tools. According to a press release from the company, Fraud Rules Manager (FRM) will help protect the industry from fraud by blocking Maestro transactions at U.S. ATMs that averaged no more than one Maestro transaction per month in 2012. This action covers a purported 80 percent or more of the nation's ATMs, removing for the time being, the risk of fraudulent transactions to ATM deployers. In addition, the company said they would monitor the remaining 20 percent of ATMs.

"It remains to be seen if MasterCard's new fraud tool is blocking every low-volume terminal that qualifies or if it is working to prevent ATM deployers from being responsible for fraud," says Tente.

U.S. Liability Shift Deadlines

+ **Oct. 1, 2015: Merchant POS Terminals**
  Merchants become responsible for card fraud at POS terminals. Excludes fuel selling automated terminals.

+ **Oct. 1, 2016: MasterCard ATM Transactions**
  Liability shifts to ATM owners for fraud committeed with MasterCard-branded debit cards.

+ **Oct. 1, 2017: Visa ATM Transactions**
  ATM owners become responsible for fraudulent transactions committeed with Visa-branded debit cards.

+ **Oct. 1, 2017: Automated Fuel Terminals**
  Liability shifts to merchants for card fraud committed at automated fuel-selling terminals.

Cost: Fraud vs. EMV Migration

Because of the cost to the payment eco-system, many in the payments industry question whether EMV migration will reduce fraud losses with enough magnitude to justify a solid business case for anyone but card issuers to make the change.

Industry estimates for upgrading ATM hardware for EMV start at about $300 for a new EMV-capable reader for an off-premise machine.

"But that does not include the technician's labor nor any software costs, installation or testing that might be required," says Mark Smith, Kahuna Vice President of Financial Services.

Overall the upgrade costs could run $2,000 to $4,000 per ATM according to estimates from Aite Group, a Boston-based research firm focused on business, technology and regulatory issues, and their impact on the financial services industry. In the off-premise space that's comparable to a new machine. By comparison, ATM skimming losses per incident have risen from $30,000 a few years ago to more than $50,000. Aite Group estimates POS terminal upgrades may cost $200 to $300 each.

Still, card skimming represents 80 percent of all attacks against the ATM — the number one ATM crime globally. A Mercator Advisory Group report estimates U.S. card issuers' total losses from credit and debit card fraud at $2.4 billion. In addition, merchants suffer billions of dollars in fraud losses every year.

Industry experts estimate that replacing 600 million debit/credit cards will cost $3 billion and replacing POS terminals will cost merchants more than $6 billion. ATMIA research estimates the cost of upgrading the U.S. ATM fleet at about $800 million. As of March 31, 2013, Visa had issued only 3.5 million chip cards, compared to more than 716 million Visa cards in circulation at the end of 2012.

The question facing the industry is — will winning the arms race be worth the cost.

U.S. EMV Upgrade Costs

+ $6 Billion for Debit/Credit Cards
+ $3 Billion for POS Terminals
+ $800 Million to Upgrade ATM Fleet

U.S. Fraud Costs

+ $50,000 Per ATM Skimming Attack
+ $2.4 Billion Annually in Card Losses

Technology also offers alternatives to EMV, which perpetuates the use of payment cards. Given the growth of mobile payments, card payments could become a thing of the past.

Technology offers realistic alternatives to EMV. With the technology available, should we be skipping over EMV? Would we be better off investing in tokenization or mobile transactions, for example?

— Bryan Bauer, Kahuna

EMV addresses only certain types of card fraud. Statistics from countries that have adopted the standard show that chip and pin technologys reduces face-to-face fraud, especially domestic counterfeit and lost or stolen card fraud, but it does not effectively prevent card-not-present fraud. Card-not-present fraud continues to increase because there are few viable chip and PIN solutions for online merchants.

For example, since the rollout of EMV in Canada, card-not-present fraud increased from C$128 million to C$259.5 million in 2011, according to The Federal Reserve Bank of Atlanta.

Also, recent major breaches have occurred at the processor level, with criminals stealing data and creating bogus cards. The ATMs operated normally and were not at fault in the breaches.

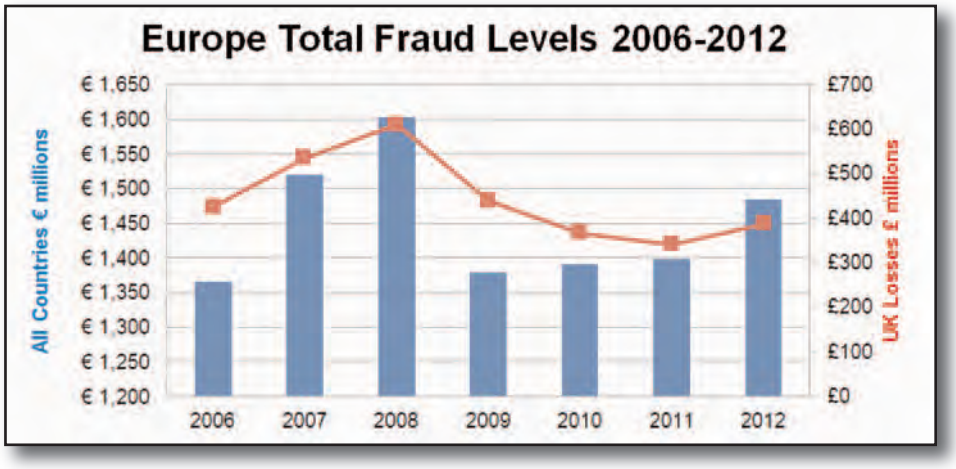
Technology also offers alternatives to EMV, which perpetuates the use of payment cards. Given the growth of mobile payments, card payments could become a thing of the past.

"With the technology available, should we be skipping over EMV?" said Bauer. "Would we be better off investing in tokenization or mobile transactions, for example?"

On the POS side, merchants that rely on chip and signature face potentially greater exposure to fraud compared to ATMs and other payments channels that use chip and PIN. Industry experts fear signature fraud could continue with stolen cards. For PIN fraud, it is more difficult because the PINs have to be stolen as well.

Will EMV Benefit IADs?

Data provided by: Euromonitor International



The cost of a skimming incident in the U.S. has risen to $50,000 on average, up from $30,000 a few years ago, according to a report from the U.S. Secret Service.

How much is it worth to ATM deployers to stop such losses? And is EMV up to the job?

Take the experience in Europe. In its first Fraud Update for 2013, the European ATM Security Team (EAST) reported that all but one of the 21 countries in the Single Euro Payments Area where EMV has been implemented reported skimming attacks. There were skimming increases in eight countries and decreases in four countries.

EAST reported skimming losses in Europe declined through 2011. By then, 99 percent of all European ATMs were EMV compliant. However, EAST reported an increase of 12 percent in skimming costs in 2012, totaling $335.7 million.

EAST and Europol estimate that 80 percent of fraud on European cards occurs in the U.S., followed by the Dominican Republic, Brazil and Mexico, noted Lachlan Gunn, Coordinator and Director of EAST.

In addition to the loss of cash, there are other costs to fraud. "Consumers' cards must be re-issued and there's often damage to the machine. Less easy to calculate is the loss of confidence in the card brand, ATM and perhaps the merchant location," comments Bauer.

Industry leaders point to other solutions that might cost less to implement.

"There are other ways to mitigate fraud, moving to PIN-based transactions would make a difference because signature fraud is more prevalent than PIN-based transactions," said Bauer.

Tackling skimming directly at the ATM could be a more cost-effective option as well. "Instead of investing in EMV, a low-cost anti-skimming device may be enough to prevent skimming," Smith said.

In its first Fraud Update for 2013, the European ATM Security Team reported that skimming losses in Europe, where 99% of ATMs are EMV compliant, increased by 12% in 2012, totalling $335.7 million.

The Move to Mobile

Technology could leapfrog the need for EMV by removing cards from the payments equation altogether. Mobile payments applications for the ATM, some of which are in pilot tests now, show promise in using secure tokens like QR codes for payments rather than cards.

Diebold, NCR and Wincor Nixdorf have demoed prototypes of mobile ATM interactivity.

“The smartphone has changed the way we embrace technology and has created a demand that services are provided anytime and anywhere,” says Chad Bruhn, Vice President of Sales, Banking Division with Wincor Nixdorf, Inc. “It is no different for banking which is why we’ve seen so much growth in mobile banking services.”

“When you think about the convenience of the mobile wallet, there is a real possibility that it will replace the traditional ATM card in the future,” says Bruhn.

“We have introduced solutions that allow consumers to use their mobile device — instead of a card — to authenticate and perform value-added transactions at the ATM. This enhances the customer experience while adding new capability to the ATM channel. For many financial institutions, it’s a step into offering a multi-channel experience that today’s consumers expect,” he continues.

Using Wincor Nixdorf’s mobile ATM application, Mobile Cash, consumers can pre-stage and complete an ATM transaction without using a card and, in some cases, to send secure authorization for a remote withdrawal. The system uses a QR code displayed on the ATM that can be scanned by the phone or some other one-time use digital token.

Once the transaction has been prepared on the phone, the consumer is sent a QR confirmation code and directions to the nearest ATM that supports Mobil Cash, if necessary. At the ATM, the customer simply selects the Mobile Cash function on the machine and scans the phone under the barcode reader or by a camera on the ATM, says Bruhn.

Technology could leapfrog the need for EMV by removing cards from the payments equation altogether.

Diebold, NCR and Wincor Nixdorf have demoed ATM/mobile interactivity. Users can pre-stage and complete an ATM transaction without using a card.

According to Bruhn, the Mobile Cash app sends information from the phone to the application server which generates a token in the form of a QR code. The QR code, which is stored in Apple Passbook or Wincor Nixdorf's Mobile Cash app, is read at the ATM replacing authentication via a debit card. If the financial institution chooses, a transaction PIN can also be required as an additional security feature.

Android phones can also use near field communication (NFC), a set of standards for smartphones and similar devices to establish radio communication with each other by touching them together or bringing them into close proximity, for cardless ATM transactions. Apple has not yet enabled the iPhone for NFC.

"If you can leave your card at home you don't have to worry about someone capturing the data on it and you can share that transaction with other people," Bauer said.

"But it's such a chicken-and-egg type of thing. You have to have quite a few locations lined up before you can build it and in order to get locations lined up you have to build it," says Bauer.

Early use for mobile/ATM convergence point to additional services for financial institutions. The business case for independent ATM deployers is less clear.

"With IAD-operated ATMs, the types of transactions that can be performed are more narrow," said David Albertazzi, Senior Consultant with the Aite Group. "They usually don't have all the bells and whistles that banks offer their customers."

However, EMV compliance could set the stage to make mobile transactions more feasible. In addition to smart cards, EMV can also support contactless cards and NFC payments.

If you can leave your card at home you don't have to worry about someone capturing the data on it.

When you think about the convenience of the mobile wallet, there is a real possibility that it will replace the traditional ATM card in the future.

An NFC-enabled device can operate in smart-card emulation mode, which allows it to serve as a contactless payment card, according to the Smart Card Alliance. An NFC mobile device can serve as a secure means of payment in many scenarios where speed of transaction is important, such as transit tickets.

The sheer magnitude of EMV migration is going to be much bigger than other mandates we've seen.

Using data from Canada, a market where EMV conversion was completed at the end of 2012, we're estimating:

+ 45% of U.S. retail ATMs will need to be upgraded
+ 50% will need to be replaced
+ 5% will be retired

— James Phillips, Triton

Implication of the Liability Shift for U.S. ATMs

The Smart Card Alliance recommends ATM owners review their equipment's hardware, software, approval and upgrade capabilities. The ATM will need a contact and, optionally, a contactless reader that is approved for EMVCo Levels 1 and 2, plus meets brand-specific requirements.

Although the U.S. is not ready to process EMV transactions today, all major vendors offer EMV-capable ATMs and, in many cases, existing ATMs can be upgraded. Online PIN is the only cardholder verification method supported by ATMs, and approved PIN pads are already available due to mandated Triple DES upgrades. The ATM software must contain a certified EMV kernel for contact transactions and can also support contactless transactions as desired.

Because most manufacturers have experience with EMV in other markets, hardware issues should be minimal. It's the software development and testing that could present challenges, says Smith. "The manufacturers have to do their own testing and get all the bugs shaken out before it's released to their customers."

"We've already begun to see financial institutions and larger ATM deployers ordering new ATMs with EMV card readers," says James Phillips, Vice President of Sales and Marketing with Long Beach, MS-based Triton Systems.

Using data from Canada, a market where EMV conversion was completed at the end of 2012, Triton is estimating that 45 percent of terminals will need to be upgraded, 50 percent will need to be replaced and five percent will be retired. Phillips says, the sheer magnitude of EMV migration is going to be much bigger than other mandates we've seen like PCI and Triple DES.

According to statistics compiled by Triton, if the industry delays EMV migration until Q3 of 2015 — two full years before the liability shift — it will require ATM deployers to complete 12,000 monthly site visits, upgrade 5,625 terminals and purchase 6,250 new ATMs each month in order meet the current deadline.

"We are encouraging our customers to start preparing for EMV migration now — to choose the EMV option when buying new machines and to begin upgrading those already in the field," continues Phillips. "We're also pre-loading EMV software on new ATMs. For ATMs already

equipped with activated EMV readers in the field, but not turned on, Triton Connect will offer ATM deployers the ability to remotely enable EMV transactions, saving them a site visit once their processor is ready to begin supporting EMV transactions."

"To upgrade ATMs already in the field, owners will need to exchange the existing card reader for one that accepts and reads the chip embedded on the card, as well as new software once a final debit solution has been agreed upon by the networks," says Smith.

In some cases, implementation of EMV may require modifications to other parts of the ATM, or even replacing an ATM, Smith continues. It may not make financial sense to upgrade some older machines that don't have the computing capacity to handle the software.

"My advise to IADs and financial institutions is to educate yourself on this issue and stay on top of any changes," says Rob Evans, Product Manager with Nautilus Hyosung.

Just purchasing EMV capable card readers isn't enough. ATM owners need to know what the roadmap is going to be, how it's going to affect your business and to have a plan, he says.

Evans suggests ATM deployers ask the following questions and keep asking them as things change:

- When is your processor going to be ready to conduct EMV transactions?
- What is the card scheme going to be?
- Will EMV affect network routing choices and, if so, how?
- Is an upgrade to Windows 7 necessary?
- How can you upgrade machines in a timely manner without making multiple trips to the ATM?
- How are you going to educate your customers about the differences between an EMV and magstrip transaction?

Because EMV is a temporary project, many manufacturers may be reluctant to employ the working capital needed to triple production capacity to meet demand, particularly when post-EMV hardware demand will almost certainly plummet to new historical lows.

"If ATM owners wait until the last minute to move to EMV, there will be shortages from all manufacturers of new machines and upgrade kits to meet deadline dates. Every day that passes between now and the liability shifts make it that much more difficult for all parties to meet the sheer demand requirements," says Phillips.

Another question is the availability of technicians to visit each ATM and make the required hardware and software installations. Since EMV migration is a short-term project, service companies may be reluctant to add staff to handle the field work, Bauer said.

Although it may be tempting to get ahead of the pack, it may be more prudent to wait until more issues are settled. EMV-capable machines in the field may need additional software upgrades once the debit solution issues are decided and software is certified, said Tente.

"Chances are some of the software components will change depending on how many applications we have on the chip," Tente said. "Even the software kernel on the terminal may change. Anybody that certifies today will have to recertify once all the issues are sorted out."

However, as we saw in Canada, if IADs wait processors may simply decide to turn off large numbers of high risk, non-EMV ATMs, rather than take the risk of chasing shallow-pocketed IADs for fraud claims, says Phillips.

In the end, to upgrade now versus waiting is a cost and inconvenience that each operator will have to weigh," says Tente.

Photo courtesy of GetBranded.com

Kahuna's Bryan Bauer suggests ATM operators stock up on card readers and develop a communication plan with merchant-level operators, route operators, first-line maintenance providers and consumers on how EMV cards differ from mag stripe cards.

Consider using:

+ On-Screen Messaging

+ Physical Signage

Education is the Key

As consumers begin receiving their new smart cards, education will need to take place on how to use the new card readers and how they differ from mag stripe readers.

An EMV transaction requires the card to remain in the slot the whole time. That means consumers who are used to swiping cards at ATMs, gas pumps and self-checkouts will have to change their behavior.

Educational campaigns are in the works to let consumers know their experience with card readers will be different with the new cards. "We'll start to see marketing campaigns to get consumers aware of how chip and pin cards will need to be used," Tente said.

"ATM operators should think about educating consumers as well," comments Bauer. "IADs should develop a communication strategy with merchant-level operators, route operators, first-line maintenance providers and consumers that are regularly using terminals."

"We would suggest on-screen messaging and physical signage that tells users, ''Transaction Initiating – Please Don't Remove Card Until Prompted!,'" he said. "Since most retail ATMs currently involve a dip-style reader where the card is immediately removed, we must prepare cardholders and change their behavior."

Without education campaigns, the transition to EMV in the United States could cost ATM operators even more money, says Bauer. "We recommend IADs keep extra card readers in stock. We estimate that card readers will fail on retail ATMs at a higher rate in the post-EMV era."

For IADs, the early consensus among EMV experts is to start doing your homework, and keep your eyes and ears open.

"IADs need to talk to their manufacturers, service people, networks and processors, and find out what they know and what their plans are," says Bauer. "Pretty soon things will start moving faster and you don't want to wait until the last minute. Stay tuned in and don't stick your head in the sand."

About the Sponsors

The ATM Industry Association is a global non-profit trade association with over 3,700 members in 60 countries. The mission of ATMIA is to promote ATM convenience, growth and usage worldwide, to protect the ATM industry's assets, interests, good name and public trust; and to provide education, best practices, political voice and networking opportunities for member organizations. To learn more about the association, visit www.atmia.com.

Kahuna ATM Solutions is the ATM industry's ONLY business development service company dedicated to the success and profit maximization of independent ATM deployers and ATM operators. Originally founded in 1995, Kahuna ATM Solutions has been considered a trusted industry leader for over a decade. Currently, the Kahuna affiliate network contracts for the processing and management of more than 22,000 ATMs across the United States; accounting for over 70 million transactions annually. To learn more, visit www.KahunaATM.com or call 1-888-357-8472.

ATMIA Disclaimer