Understand the Business Impact of EMV Chip Cards

3 What About Mail/Telephone Order and eCommerce?
3 What Is EMV
3 How Chip Cards Work
3 Contactless Technology
4 Background: Behind the Curve
4 Liability Shift
5 Should You Adopt Chip Technology?
5 Possible Reasons to Wait
6 Who’s Ready and Who’s Not?

Upgrading Card Security at the Point of Sale
A revolution in credit and debit card technology is underway to make card-present transactions in the U.S. more secure. While companies of all sizes are making changes, many do not understand what is happening.

U.S. companies are encouraged to update their technology for reading credit and debit cards from the swipe system to a more secure one that involves reading data on microchips embedded in payment cards. This EMV technology, named for the companies that developed it – Europay, MasterCard and Visa – can significantly reduce the risk of card-present counterfeit, as well as lost and stolen card fraud because chip cards are nearly impossible to counterfeit. There is unique information both in the chip and the magnetic stripe to indicate that it is a chip card. The card information if skimmed could only be used for card-not-present transactions.

Chip cards have been widely used in other countries since 1986. U.S. companies have been reluctant to adopt them primarily because the new technology is expensive and both cardholders and merchants tend to avoid change. However, as of Oct. 1, 2015, merchants and card issuers that haven’t switched to the EMV system will be held responsible for any future card fraud.

High-profile breaches of card data at major retailers such as Target, Home Depot and Neiman Marcus have publicized the problem of fraud in the U.S., which adds up to $8.6 billion a year, a number only expected to increase, according to FIS Payments Leader, a top provider of payments technology.

EMV technology can significantly reduce the risk of card-present counterfeit and lost and stolen card fraud. Chip cards have been widely used in other countries since 1986, but U.S. companies have been reluctant to adopt them because the new technology is expensive and both cardholders and merchants tend to avoid change.
What About Mail/Telephone Order and eCommerce?

EMV does nothing to cover the growing number of transactions made via the Internet, mail or phone (i.e. card-not-present) — a kind of fraud that is expected to rise as EMV is implemented and card present fraud opportunities decrease. Card data stolen from chip cards can still be used online and additional fraud prevention measures for these companies should be implemented.

What Is EMV

The new EMV system is more advanced than magnetic cards and readers because they transfer a few simple data points, such as the credit card numbers and expiration dates. This is information that can easily be hacked and reused.

By contrast, the encrypted microchips in EMV cards hold multiple pieces of information that can be relayed between the processor and the card to create a unique code for each transaction. Users then authenticate the transaction with a signature or PIN number. Initially, the majority of U.S. cards will use a signature for cardholder verification instead of a PIN because that process is familiar to cardholders and easier to implement for card issuers.2

How Chip Cards Work

Instead of swiping cards, consumers insert EMV chip-cards into EMV enabled devices, chip-end first and facing up during the entire transaction.

Customers authenticate their transactions with signatures or PINs.

The device will then prompt the cardholders to remove the card when the sale is complete.

Contactless Technology

Most EMV devices can also process contactless, or near field communication, technology that allows customers tap their cards or their digital wallets, such as Apple Pay or Android Pay, against a scanner. Initially, most cards in the U.S. will require insertion into terminal.
Background: Behind the Curve

EMV has been used by many banks and businesses in Europe, the Middle East, Africa, Asia, Canada, Mexico and the Caribbean for decades. By the end of last year almost 97 percent of Western European transactions made at the point of service were EMV transactions (over 85 percent in Canada, Mexico and the Caribbean), only 0.12 percent in the U.S. were EMV transactions as of June 2014.3

EMV has proven to be a successful antifraud strategy abroad. According to the UK Cards Association, “Fraud on lost and stolen cards is now at its lowest level for two decades, and counterfeit card fraud losses have also fallen and are at their lowest level since 1999.” Interac Association (Canada) announced that Interac debit card fraud losses to financial institutions resulting from skimming declined to $70 million in 2011 from $119 million in 2010 and a high of $142 million in 2009.4

Liability Shift

However, the pressure is on for companies to adopt the new technology. Visa®, MasterCard®, Discover® and American Express® announced a “liability shift” will start on Oct. 1, 2015. While banks or debit and credit card issuers previously picked up the tab for card-present counterfeit merchant fraud, going forward, any bank that doesn’t issue the chip card or merchant that doesn’t process the new chip cards by inserting will have to cover the costs of the products or services sold, as well as associated chargeback fees. Visa ATM processors are liable beginning on April 1, 2015,5 and for Discover the deadline was extended until October 1, 2017, for fuel dispensers or pay at the pump.6

According to the UK Cards Association, “Fraud on lost and stolen cards is now at its lowest level for two decades, and counterfeit card fraud losses have also fallen and are at their lowest level since 1999.” Interac Association (Canada) announced that Interac debit card fraud losses to financial institutions resulting from skimming declined to $70 million in 2011 from $119 million in 2010 and a high of $142 million in 2009.
Should You Adopt Chip Technology?

Increased Security
Increased security is the primary reason to switch. While EMV cards and terminals won’t eliminate all kinds of fraud, they will protect businesses from fraud at the point of service or card-present transactions related to counterfeit and some lost, stolen card fraud.

Increased Cost
Prior to Oct. 1, 2015, companies do not know what their exposure is since card issuers have never passed on this liability. The shifted cost could be detrimental to doing business and significantly increase expenses if companies do not upgrade.

Increased Reputation
Merchants that adopt EMV will be a leader to peers and generate goodwill among customers, who can feel more secure about using their card.

Support New Technology
Most EMV devices can also process contactless, or near field communication, technology that allows customers to tap their card or their digital wallet against a scanner. Initially most cards in the U.S. will not include this capability.

International Business
Many European merchants and banks will decline transactions because the U.S. had not implemented chip card acceptance thus making it easier for their clients to experience fraud. By enabled chip card acceptance, companies will be able to accept card payments by their international customers.

High-end Merchandise
Any company that does not upgrade is a target for fraud after Oct. 1, 2015, but especially companies that sell luxury goods such as jewelry and electronics with high resale value will increase as targets for fraud as EMV is implemented.

Possible Reasons to Wait

Expense
Cost, time, and training will be an initial charge to your bottom line. Businesses have to install both EMV-enabled hardware and update the integrated internal software to process chip cards. Hardware may have a chip card slot but not the software to recognize the card being inserted and processed.

Many companies still use analog phone lines to process card transactions, which will cause severe delays in processing time. An upgrade to a high speed internet connection is recommended for speed of the transaction, but can also bear significant installment and ongoing monthly fees. EMV transactions will need to send a much larger amount of information and will take an average of four times the current processing time on analog and two times the current time for IP.

Tension at the Point of Sale
A small downside for customers is that inserting the card in the terminal and waiting for it to communicate with the reader takes longer than a swipe. The cashier or cardholder will also need to know how to insert the card to make the transaction complete.

Difficult to Upgrade
The ability to upgrade may not be available to the company depending on the current merchant services acquirer, processor, point of sale system, device and/or software in device. Many systems, devices, and internal software are not going to be ready to accept chip cards by Oct. 1, 2015, so even if the company wants to, they cannot or they will have to switch the component listed above that is the outlier. Many point of sale systems are targeting 2016 to be EMV enabled.

Unknown Value of Risk
Again, since companies cannot monetize the risk of fraud versus the cost to upgrade, some will be willing to wait initially and take the risk of fraud.
Who’s Ready and Who’s Not?

The process of full U.S. adoption is expected to take several years. As a result, new cards issued will continue to have magnetic strips. However, if the chip card is swiped the card data is in jeopardy and the company will still be liable for potential fraud. But many companies have already switched. For example, Target spent $100 million to install new terminals at its stores in February.8

According to research consultant the Aite Group, 47 percent of U.S. terminals should be EMV-ready by 2016; and 70 percent of credit cards and 41 percent of debit cards should also be in place.9 Smaller businesses are less prepared. About half of those surveyed in July 2015, weren’t even aware of the Oct. 1 deadline, according to a Wells Fargo/Gallup Small Business Index survey. Of those who were aware, 31 percent said their credit card processing system accepts chip-enabled cards, 34 percent intend to make the change after Oct. 1 and 21 percent never plan to switch.10

Fraud has doubled in the past seven years, according to Aite.11 Smart companies will want to avoid even the possibility of a breach of customer information. Customer privacy is increasingly important in the age of social media as is a company’s reputation. Merchants that adopt the system sooner can increase their status with customers and employees by clearly communicating they are now providing an additional and vital security service by protecting card data.

Conclusion

EMV chip cards could drastically affect payment processing as we know it today. Your business will need to develop a strategy on upgrading equipment if you have not done so already, even if that strategy is to do nothing. BB&T is prepared to offer EMV-equipped solutions with chip credit and debit cards and payment acceptance devices. Go to BBT.com/ChipCard to learn more.

---

1 http://www.bankinfosecurity.com/interviews/history-emv-i-933
6 http://www.nacsonline.com/News/Daily/Pages/ND0207131.aspx#Vdx33xViko
9 http://www.bizjournals.com/sanfrancisco/blog/2014/02/target-visa-mastercard-senate-hearing.html, 11 BB&T PowerPoint