EMV AND THE LIABILITY SHIFT:

How EMV Affects Card-Not-Present Businesses

BluePay

Summary

On October 1, 2015, the EMV liability shift will go into effect within the United States. This shift will determine which party – either the merchant or the card issuer – will be responsible for the financial losses resulting from fraudulent counterfeit, lost, or stolen card-present transactions. EMV, a chip technology being utilized around the globe, is proven to have visibly reduced fraudulent card present transactions. However, as the ability to use counterfeit cards in brick and mortar stores diminishes, thieves are expected to turn to other forms of fraud that prey on the vulnerabilities of card-not-present merchants. Unfortunately, this pattern has been noticed globally where EMV has been implemented.

In this paper, we will discuss:

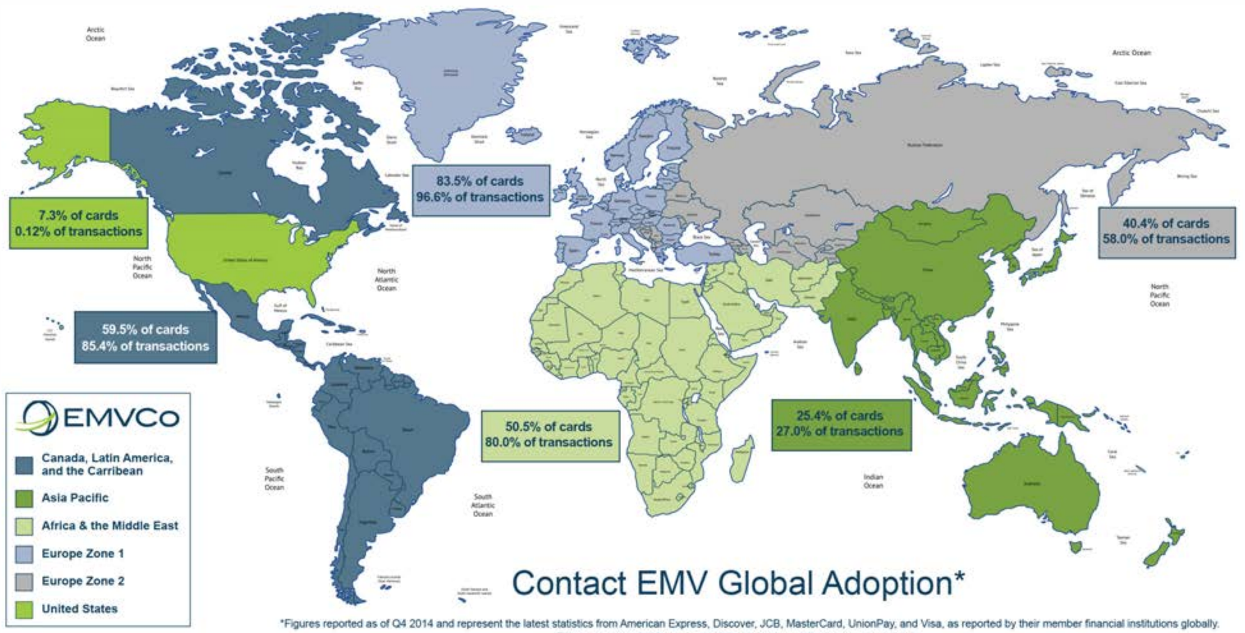
- EMV chip technology
- Implementation in the U.S.
- The impact on CNP fraud after the liability shift
- Merchants who are most likely to be affected
- Technology and tools to help reduce fraud

EMV – A Little Chip with a Big Impact

EMV (Europay, MasterCard, and Visa) is a global payment system with fraud-reducing technology that can help protect issuers, merchants and consumers against losses from the use of counterfeit and lost or stolen payment cards at the point-of-sale (POS). EMV cards, or smart cards, are embedded with a microprocessor, or smart chip, which interacts with the merchant's POS device to ensure that the payment card, combined with a PIN number or signature, is valid and belongs to the person using the card. This kind of chip technology adds layers of security against fraud and is virtually impossible to duplicate.

EMV technology has been criticized by some for its exclusion of protection for card-not-present transactions. And although many mistakenly believe that the technology protects against data security breaches, the Payment Security Task Force (PST), a cross-industry task force comprised of card networks, issuers, acquirers, processors, and retailers, continues on its course of shepherding the migration to the EMV standard.[1]

Many countries have seen the benefit in adopting EMV technology. According to the Aite Group, since the United Kingdom introduced EMV cards in 2005, counterfeit fraud has fallen 56 percent. In Australia, counterfeit fraud is down 38 percent, and Canada has seen a 49 percent reduction.[2]



Contact EMV Global Adoption*

*Figures reported as of Q4 2014 and represent the latest statistics from American Express, Discover, JCB, MasterCard, UnionPay, and Visa, as reported by their member financial institutions globally. Figures are reported by region and do not imply country-by-country statistics.

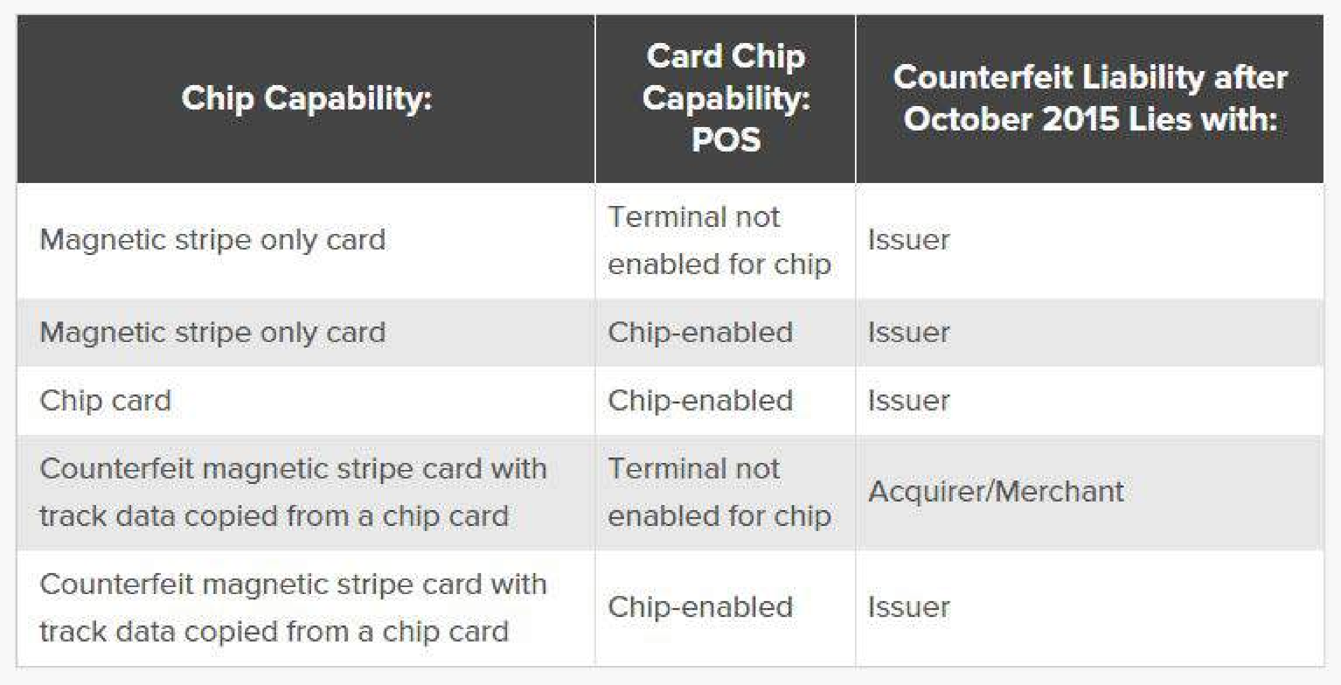
Better Late Than Never – The U.S. Prepares to Implement EMV

The U.S. is one of the last regions to implement EMV. For nearly a decade, the payment technology was resisted by merchants and issuers because of increased costs to upgrade POS equipment and manufacture chip cards. Within the U.S., the geographic locations that claim to have the most fraud include: Florida, Georgia, Nevada, Michigan, and Delaware. According to some reports, counterfeit-credit-card fraud accounts for approximately 40 percent of total credit-card fraud in the U.S.[3] The outdated 40-year-old technology of the magnetic stripe has given way to this statistic by making it easy for fraudsters to counterfeit cards and use them in card-present environments.

What is the motivation for the U.S. to migrate to chip cards now? The motivation is the substantial amount of money that could be lost to fraudulent transactions if the U.S. doesn't. Forbes estimates that number will top $10 billion if the U.S. continues with magnetic stripe transactions.[4] With the liability shift approaching, the largest card issuers in the U.S. have begun issuing cards enabled with the chip technology. The PST stated that by the end 2017, nearly 98 percent of the cards issued by the eight largest card issuers, accounting for about half of U.S. payment card volume, will contain EMV chips.[1] Boston-based Aite Group reports that 70 percent of U.S.-issued credit cards and 41 percent of all U.S. debit cards will be chip enabled.[3]

Merchant or Card Issuer – Who's Responsible?

Regardless if every merchant or card issuer is ready or not, the liability shift will take place in the U.S. on October 1, 2015. When it comes to counterfeit, lost, or stolen card-present transactions, the party who has not adopted chip technology will be held responsible for the financial losses resulting from fraudulent activity. If a consumer presents a chip card at a merchant that does not have EMV-enabled equipment, the liability will shift to the merchant. If a traditional magnetic stripe card is presented at a merchant with EMV-enabled equipment, the card issuer will be responsible for any financial liability resulting from fraudulent transactions.



Chip Capability:	Card Chip Capability: POS	Counterfeit Liability after October 2015 Lies with:
Magnetic stripe only card	Terminal not enabled for chip	Issuer
Magnetic stripe only card	Chip-enabled	Issuer
Chip card	Chip-enabled	Issuer
Counterfeit magnetic stripe card with track data copied from a chip card	Terminal not enabled for chip	Acquirer/Merchant
Counterfeit magnetic stripe card with track data copied from a chip card	Chip-enabled	Issuer

Post-EMV Effects on CNP Fraud

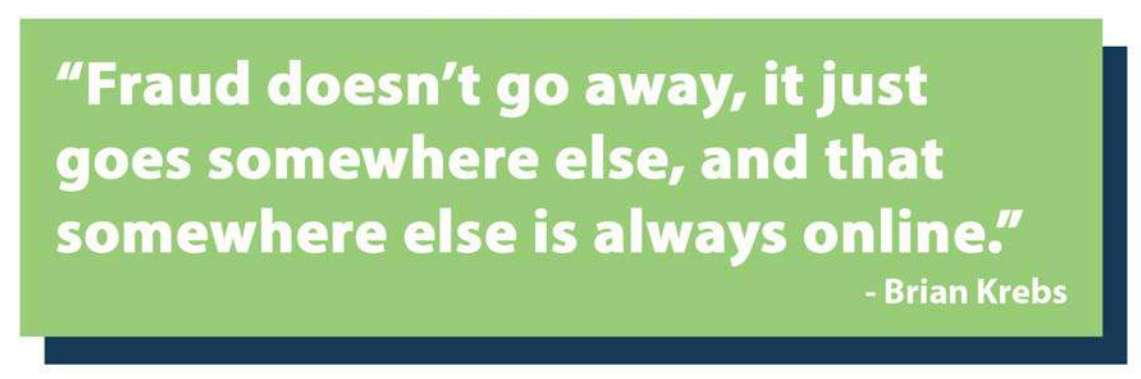
Between the time EMV technology was conceived and the time it was implemented – first in the United Kingdom and Europe, followed by other countries around the world – thieves found a new way to utilize stolen payment card information…e-commerce. Although EMV provides an extra layer of protection for card-present transactions, it does not account for fraud initiated through e-commerce or other card-not-present channels.

In 2004 when the EMV rollout began in the U.K. (the liability shift was in 2006), fraud losses from counterfeit credit cards dropped from a high of nearly £128 million ($199 million) to £47.8 million ($74.4 million) last year, according to the U.K. Cards Association. In 2004, CNP fraud losses totaled nearly £151 million ($239 million).

Those losses climbed to more than £183 million ($285 million) a year later and peaked in 2008, two years after the liability shift, at £328.4 million ($510 million).5 CNP fraud also more than doubled in Australia and Canada.[2]

CNP fraud is the unauthorized use of a credit or debit card number, the security code printed on the card (if required), and the cardholder's address to purchase products or services in a setting in which the merchant and customer are not physically present or face-to-face. These transactions are typically made through e-commerce websites, mail orders, or telephone calls.

According to online fraud expert, Brian Krebs, every country that has switched to EMV cards has seen a jump in online fraud. "Fraud doesn't go away, it just goes somewhere else, and that somewhere else is always online," says Krebs. He continued, "The thieves can still steal the card number and expiration date, which still can be used online. So that's generally what will happen. We'll see a pretty big uptick in card-not-present fraud."[6] Credit card details are widely accessible on the black market.



"Fraud doesn't go away, it just goes somewhere else, and that somewhere else is always online."

- Brian Krebs

As the U.S. migrates to EMV adoption, online fraud rings are expected to flourish.[2] They're very organized and well-funded to perform sophisticated CNP attacks, that could possibly spill over into other countries.

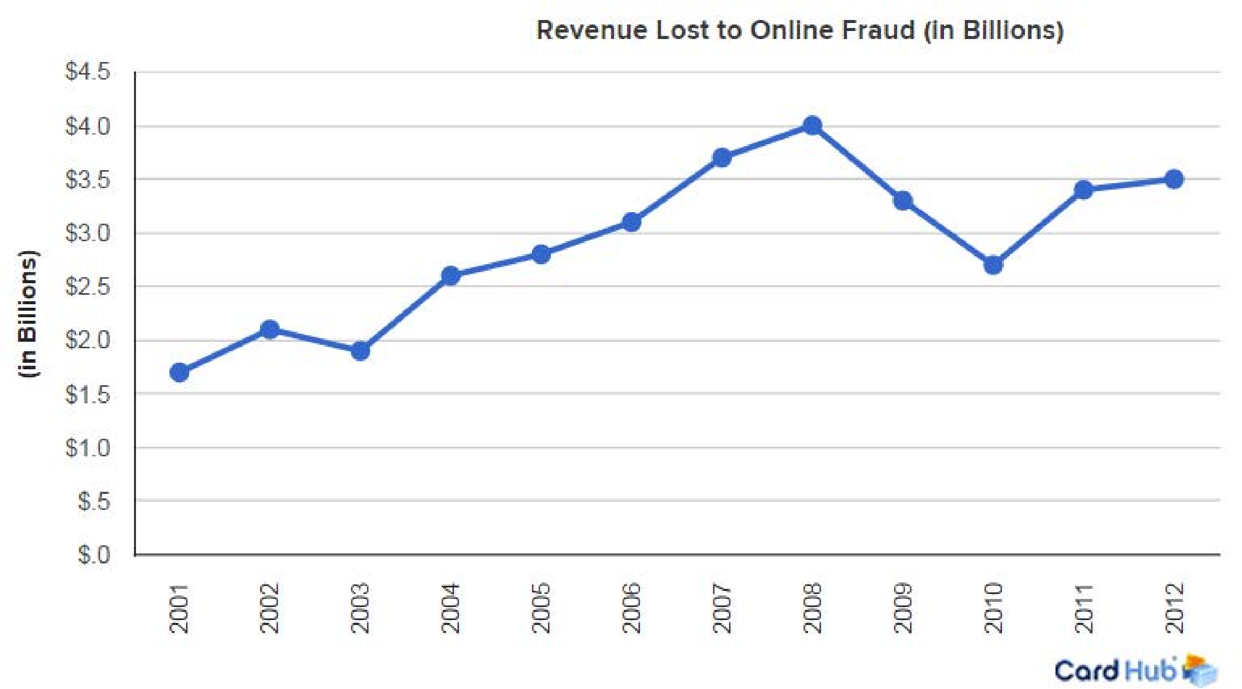
Is EMV Really to Blame?

Some experts believe that the increase in CNP fraud in Europe was a coincidence due to the increase in CNP transactions as a whole during that time. Many merchants were moving to online stores and consumers were switching from brick and mortar shopping to the convenience of being able to shop from home. Fraudsters realized that penetrating CNP transactions was easier, safer, and anonymous as compared to in-store counterfeit fraud.[7]

A closer look shows online fraud experienced growth prior to EMV. In 2010, online credit card fraud throughout the U.S. and Canada totaled $2.7 billion. In 2011, it was $3.4 billion.[8]

Al Pascaul, Director of Fraud and Security at Javelin Strategy & Research explains, "Without the widespread adoption of new CNP fraud-mitigation technologies, we expect CNP fraud to grow to $19 billion by 2018.

EMV is not the primary driver as CNP fraud was already trending in that direction, growing in tandem with legitimate transaction activity (which is consistent with other markets where EMV was deployed). While U.S. merchants and issuers have gotten better at detecting and preventing CNP fraud over the past decade, the rate of improvement has largely flat lined."[7]

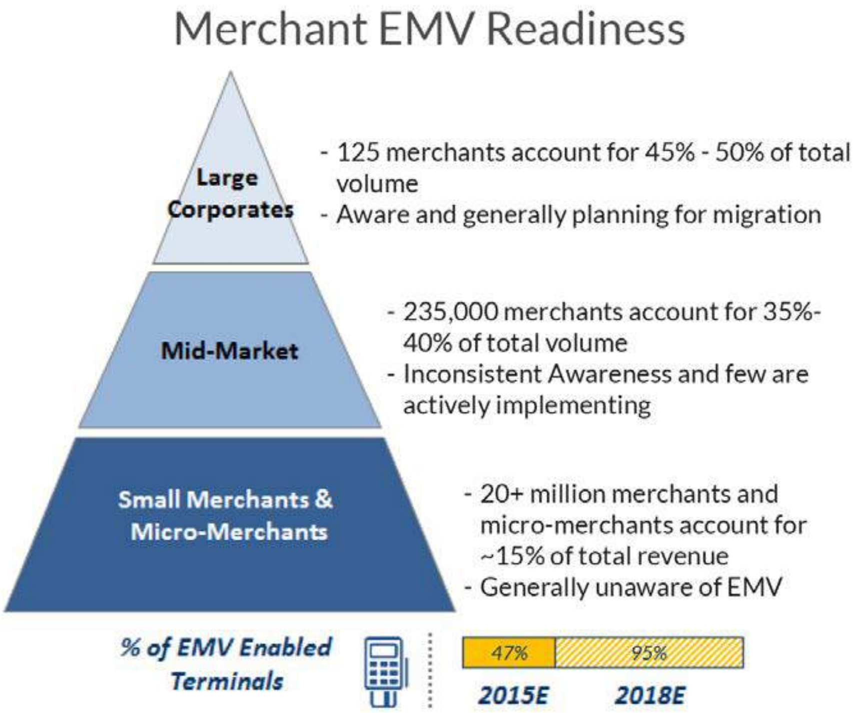


Who's Most at Risk?

Small to midsize businesses (SMBs) tend to be easy targets. Most are less educated and prepared, and they may not even be aware of EMV or the liability shift. They may have existing vulnerabilities within their payment systems, and until they work to fill those gaps, they are "sitting ducks". Larger merchants are doing a better job identifying threats and preventing fraudulent transactions. They are more educated on fraud prevention, interchange optimization, and useful tools. According to Tim Sherwin, EVP and co-founder of Cardinal Commerce, "If a fraudster tries to make a purchase with a stolen credit card at a large e-tailer and it's canceled, they won't just give up. Instead, they'll go to a smaller retailer who carries the same product, but may not be as up-to-date with their fraud strategy and rules."[7]

Found on the back of the card for Visa and MasterCard and the front for American Express, the Card Verification Value (CVV) is an anti-fraud security feature used to verify that the person making the purchase is in possession of the card during a CNP transaction. Charles Henderson, VP of Managed Security for Trustwave says, "The CVV is different in card-not-present transactions than it is in card-present transactions." Henderson continued, "From a criminal's perspective, if I'm going to look for cards I can use in card-not-present fraud, I'm going to look for a card-not-present target. This should be the million-dollar eureka moment for card-not-present retailers. That's why they should be paying attention."[9]

Thieves do not play favorites when it comes to using counterfeit cards; however, there are some types of merchants that are more at risk than others. Among the list are specialty retail stores, gift and novelty stores, liquor stores, and restaurants to name a few.



Source: Payments Security Task Force and First Annapolis Consulting analysis.

Surviving EMV with ET – Education and Tokenization

Based on data from fraud losses in 2013, the Federal Reserve estimates that approximately 70 percent of card-not-present fraud is shouldered by the merchant.[10] So, how can a merchant protect its customers and its business? Experts suggest that merchants ramp up and stay educated about the latest fraud trends and tools available. New methods and technologies are being developed all the time, and merchants simply can't rely on what worked a year ago. Additionally, merchants should schedule regular review periods to test new technologies and services to evaluate the effectiveness of their fraud protection.

Although it isn't a new technology, tokenization is expected to be a major security solution in the CNP environment going forward. Implemented in 2004 shortly after PCI standards came into place, tokenization is the process of substituting a customer's primary account number (PAN) with a "token" – information that is useless to a hacker. The merchant stores the token in its system in place of the sensitive payment information, and it can be used for a number of tasks like chargebacks, remittance, and order fulfillment. Tokens aren't just for payments anymore. They can be used for any sensitive data that a company handles such as social security numbers, healthcare information, and other personal information that could be used for identity theft.

There are actually two different types of tokenization: security tokenization and payment tokenization. Security tokens are generated after a customer submits a card for payment. The latest trend in contactless payments, Apple Pay, uses payment tokens. These are generated before a transaction has started and is stored within a secure element on a device, like an iPhone. Only major card brands can initiate payment tokenization.

In a recent report, Forrester Research predicts "more secure, encrypted, and tokenized transactions on digital wallets, mobile-device-based near-field communications (NFC) virtual cards, and EMV contactless payments will prove strong competitors to plastic EMV chip-and-signature and chip-and-PIN payments in the U.S."[11]

Other Tips, Tools, and Technology to Lessen the Blow

Pro-EMV industry group, the EMV Migration Forum, has coordinated a Card-Not-Present Fraud Working Committee that recommends a multi-layered approach that includes stronger authentication methods, dedicated fraud tools, and implementation of 3D Secure and tokenization. Randy Vanderhoof, Director of the EMV Migration Forum, says, "No single security mechanism can protect against all possible fraud scenarios. Instead, the best practice to protect against card-not-present fraud is to use a systematic, multi-layered approach using tools that work together to create a successful fraud reduction program."[12]

> **"No single security mechanism can protect against all possible fraud scenarios. Instead, the best practice to protect against card-not-present fraud is to use a systematic, multi-layered approach using tools that work together to create a successful fraud reduction program."**

In addition to using AVS (Address Verification) and CVV (Card Verification Value), many processors offer fraud management tools to help merchants protect their accounts and minimize security risks. These tools allow merchants to adjust certain parameters to prevent fraudsters from testing cards on their account, making transactions from blocked countries, and purchasing amounts larger than the products/services offered by the merchant to name a few.

3D Secure, a technology that authenticates the user in real-time and shifts liability from the merchant to the issuer, is standard in online transactions. In the wake of high-fraud rates post EMV conversion, many governments have mandated it. In the U.S., however, only three (3) percent of businesses currently use it, partly because both the merchant and the card issuer must be on the same page.[13]

The technology authenticates consumers using information from the card issuer, which sometimes means entering an additional password during checkout. Some merchants feels this negatively impacts conversion, but most conversions can be done with little or no impact to the consumer. 3D Secure has greatly evolved due to lessons learned in the U.K. post EMV. Passwords were very efficient in reducing fraud, but became a challenge for consumers who were again asked to remember another password. A more layered approach was implemented using device recognition, behavioral patterns, geolocation and occasional use of one-time passwords.

There are several interesting security methods currently in development. One of those methods is the use of biometrics. MasterCard is currently making strides on launching low-friction services to allow consumers to verify themselves with a “selfie”-based solution.[7]

Another fascinating first-of-its-kind technology, Motion Code, is currently in development with Oberthur Technologies. With Motion Code, the CVV code appears on a mini screen right on the card. The code updates every hour. It’s powered by an ultra-thin lithium battery that has a life of approximately three (3) years. Adding an extra layer of security for online transactions, the technology doesn’t imply any changes for the consumer or e-tailer. The issuer or processor would need to have a specific server installed in their facility that synchronizes with the algorithm used to generate the codes. Pilot testing is expected to begin in late fall 2015. Motion Code is to card-not-present transactions what the EMV chip is for card-present transactions; however, Motion Code is an all-in-one card and can be used for all transactions.[14]

At the time of the EMV switch in Europe, merchants were not as prepared technologically to identify and prevent CNP fraud as merchants are today. Since 2006, there has been a major increase in third-party providers creating solutions to flag orders that probably would have shipped years ago.[7] One such solution is fraud scoring, a system of predictive fraud detection models that payment processors can use to detect high-risk transactions in the CNP environment.

Don’t Forget PCI

All businesses that elect to accept payments must adhere to and comply with the PCI Data Security Standard (PCI DSS), created and updated annually by the PCI Security Counsel. The Counsel provides an actionable framework for developing a robust payment card data security process – including prevention, detection, and appropriate reaction to security incidents. At a minimum, all merchants are required to complete an annual SAQ (Self-Assessment Questionnaire) to determine if they are PCI DSS compliant. PCI compliant processors have already taken the steps to employ the highest levels of data security and guide merchants in taking the right steps to increase protection and improve business.

Ways to Prevent Card-Not-Present Fraud from Impacting Your Business

- Work together with the card brands and issuers on authentication
- Enroll in tokenization
- Create a fraud strategy using the right combination of tools for your business
- Identify customer personas
- Stay educated on new fraud tactics and ways to prevent them

Rising CNP Fraud Got You Worried? BluePay Has You Covered.

So how can you protect your customers and your business? Using AVS and CVV are definitely steps in the right direction, but we highly recommend strengthening your protection with additional CNP tools available through BluePay. Our full suite of robust fraud management tools will allow you to set up your parameters in the BluePay Gateway and begin taking advantage of the benefits of having that extra protection on your merchant account. Paying the minimal extra cost per month will save you maximum dollars in the long run.

Providing the highest levels of data security in the industry, we ensure that our customers – and their customers – have the right tools in place to reduce their PCI scope and the risk of fraudulent transactions. Our dedicated, knowledgeable support staff is on hand 24/7 to address your questions or concerns, and our risk team is vigorously monitoring our customers' accounts for fraudulent activity on a daily basis.

BluePay is a leading provider of technology-enabled payment processing for enterprise, small, and medium-sized businesses in the United States and Canada. Through physical POS, online, mobile interfaces, and software integration, BluePay processes business-to-consumer and business-to-business payments while providing real-time settlement, reporting, and reconciliation, along with robust security features such as tokenization and point-to-point encryption (P2PE). Headquartered in Naperville, Illinois, BluePay also has offices in Chicago, New York, and Toronto, along with two geographically diverse data centers in the U.S. for absolute security.

For more information on BluePay and our comprehensive, secure CNP solutions, visit www.bluepay.com, or contact us at 800-350-2983.

Resources

1 - **CardNotPresent.com**, May 2015: “EMV Groups Update Readiness Projections, Debit Technical Framework”

2 - **CreditCards.com**, November 19, 2014: “Online fraud may surge after EMV chip card roll out”

3 - **CardNotPresent.com**, June 2015: CNP Series Report “EMV Part One: The Long Run”

4 - **PYMNTS.com**, July 28, 2015: “TSYS Examines the Current State of Chip Migration”

5 - **CardNotPresent.com**, July 2015: CNP Series Report “EMV Part Two: CNP Fraud Surge Post-EMV – It’s Logical

6 - **CreditCards.com**, November 18, 2014: “Spam Nation author Brian Krebs sheds light on card data black market”

7 - **CardNotPresent.com**, August 2015: CNP Series Report “EMV Part Four: Take It from Me”

8 - **CardHub.com/edu/credit-debit-card-fraud-statistics,** 2013: Source: CyberSource Table “Online Fraud Losses by Year (U.S. and Canadian Merchants)

9 - **CardNotPresent.com**, June 11, 2015: “EMV Will Result in More E-Commerce Breaches”

10 - **PYMNTS.com,** July 17, 2015: “Will Motion Code Slow Online Fraud’s Momentum”

11 - **CardNotPresent.com**, May 4, 2015: “Widespread Adoption of EMV Could be Delayed Until 2020”

12 - **CardNotPresent.com**, April 16, 2015: “EMV Group Addresses Expected Jump in CNP Fraud with Best Practices”

13 - **CardNotPresent.com**, May 19, 2015: “EMV – What to Expect at Crunch Time”

14 - **PYMNTS.com**, July 17, 2015: “Will Motion Code Slow Online Fraud’s Momentum?”