The Impacts of EMV:

WHY CARD NOT PRESENT ("CNP") MERCHANTS NEED TO BE PREPARED

As EMV rolls out in the U.S., CNP fraud is predicted to more than double by 2018, from $2.8 billion to over $6.3 billion.[1] Given the recent data breaches and overall increases in ecommerce fraud, account takeover and card fraud are top of mind for merchants. The rollout of EMV is widely expected to increase these risks as the CNP channel becomes the most accessible and profitable route for fraudsters.

So what should CNP merchants be doing to strengthen their risk management against emerging and increasing threats online? Our white paper will explore the projected growth rate of both e-commerce and CNP fraud and how the EMV rollout will compound this already alarming problem. We will also discuss some prudent, preventative measures to consider in advance of EMV implementation to protect their business as the CNP landscape evolves.

EMV in simple terms

EMV chip technology has been deployed in other countries for years and is quickly becoming the global standard for helping secure physical credit and debit card payments. The name represents the combined effort of Europay, MasterCard® and Visa® to develop a smart chip technology that embeds microprocessor chips that securely stores cardholder data on payment tools (payment cards, mobile phones and others). In the U.S., this technology is known as "chip cards."

More secure than the traditional magnetic strip (magstripe) card technology, these "chip cards" allow for dynamic authentication whereas magstripe data is static.

More secure than the traditional magnetic strip (magstripe) card technology, these "chip cards" allow for dynamic authentication whereas magstripe data is static.

Static data can be easily skimmed with card reading devices and reproduced by fraudsters as a counterfeit card used to make fraudulent retail and card-not-present (CNP) purchases. EMV's dynamic authentication capabilities allow the technology to easily circumvent counterfeit fraud because the dynamic values within the chip must be verified by the point-of-sale device to authenticate the card for each transaction.[2]

Global adoption of EMV

France – while it was not adherent to the EMV standard at the time – was the first to use EMV technology in 1992. Today the technology is used in a majority of countries around the world, with more than 1.24 billion chip cards and 15.4 million POS terminals utilizing the standard.[3] The U.S. is the only major country that hasn't implemented this almost-global standard and happens to be the largest user of payment cards in the world.[4]

As the last holdout in deploying EMV technology, the U.S. has seen an increase in counterfeit card fraud, which now makes up 37% of U.S. card fraud losses. Additionally, aggregate fraud rates doubled from 2007 to 2014, jumping from five basis points to 10.[5] Currently, MasterCard and Visa are aiming for a liability shift date in October 2015 for the U.S.[6] Another motivational point for deploying this technology was Visa's announcement in 2011 that card fraud liability would shift to the merchant.

A painful history for CNP merchants on prior EMV implementations

To get a clearer picture of the implications of EMV as it rolls out in the U.S. market, it is helpful to look at a couple of countries that have successfully deployed the technology and the aftermath.

The UK deployed a pilot of EMV in 2003 and completed a nationwide deployment in 2004, with the liability shift occurring in January 2005.[7]

THE POSITIVES: EMV sharply eradicated both counterfeit and lost/stolen card fraud in the UK. In 2005, counterfeit fraud cost roughly £97 million and lost/stolen fraud cost roughly £89 million. Fraud losses fell steeply through 2013, where counterfeit fraud losses equaled £43 million (a 56% decrease) and lost/stolen fraud losses totaled £59 million (a 34% decrease).[8]

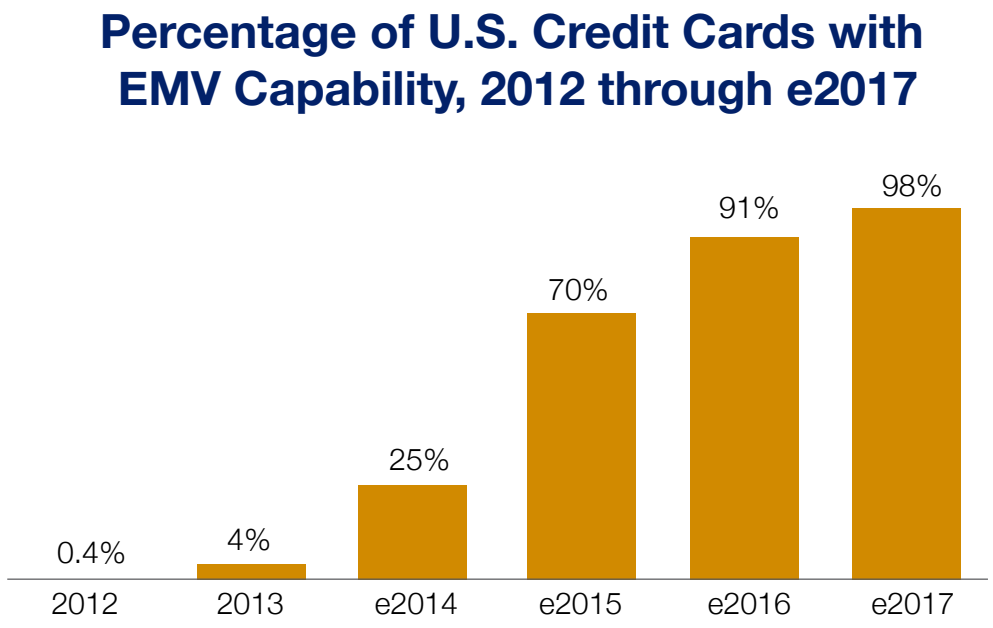
THE NEGATIVE FOR CNP: The other side of the coin is that CNP fraud rose dramatically after the UK liability shift, spiking to 78% in 2008. This increase required the development and implementation of 3D Secure technology and more sophisticated fraud analytics by issuers and merchants.[9] Counterfeit fraud ballooned at £169.8 million in 2008 and managed to deflate to £43.4 million in 2013, illustrating the effectiveness of enhanced fraud prevention tools.[10]

Australia began industry-wide implementation of EMV in 2008, though fraud was not the primary driver of the country's migration to EMV. Australia's payment card authorizations occur in real-time online and credit card fraud at the time of the first chip card migration forum in 2007 was just six basis points.[11] MasterCard's ATM and POS liability shift occurred in April 2012, and the Visa liability shift date for POS and ATM transactions took place in April 2013.

THE POSITIVES: The migration to EMV-enabled cards and terminals resulted in declining counterfeit losses on network-branded cards. Additionally, the spike in CNP losses after rollout of EMV – and the subsequent migration of fraudsters to the online commerce channel – decreased from $198.1 million in 2011 to $183.1 million in 2012, likely the result of increased use of fraud analytics and tools like 3-D Secure.[12]

THE NEGATIVE FOR CNP: The decline in fraud losses on network branded cards were accompanied by a spike in cross-border fraud in 2011 – up to $42 million from $22 million in 2010 – as criminals began using Australian payment cards in countries without EMV.[13] Additionally, Australia shared in the UKs experience of sharp increases in CNP fraud as card-present fraud is largely subdued by EMV and digital commerce continues to gain popularity.

Timeline for U.S. EMV rollout



Source: Aite Group interviews with card executives from 18 of the top 40 U.S. issuers and payment networks, April and May 2014

There are a number of upcoming key dates that merchants should be aware of in order to prepare for the impacts:

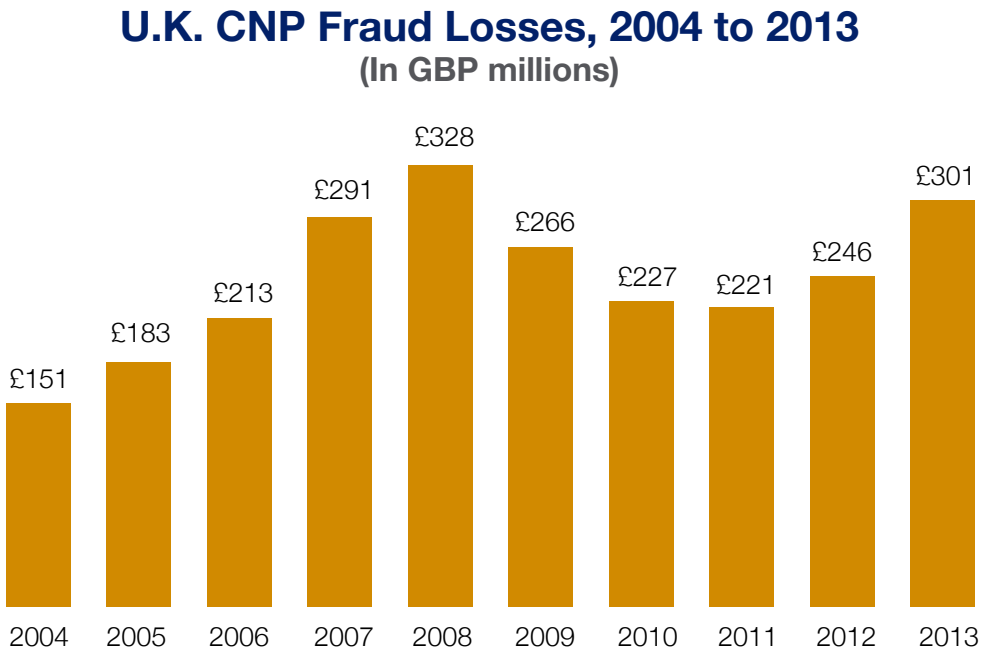
OCTOBER 1, 2015 – For Visa merchants, liability will shift to acquirers if the merchant lacks an EMV-enabled POS device for both domestic and cross-border counterfeit fraud card-present POS transactions.[14]

For MasterCard, merchants that process at least 95% of MasterCard transactions on EMV devices, ADC relief will take effect (100%). The liability shift will also occur for MasterCard merchants, barring fuel dispensers.[15]

OCTOBER 1, 2017 – For both MasterCard and Visa, the liability shift takes effect for transactions generated from automated fuel dispensers.[16] This shift occurs later to, allowing time to accommodate higher equipment and pump costs.[17]

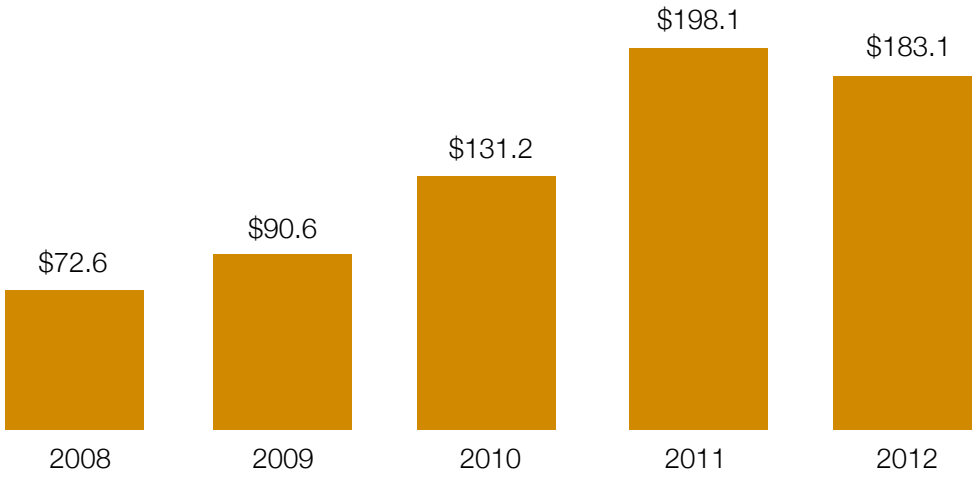
Why EMV matters to CNP merchants

While EMV promises to be a boon for eliminating card-present fraud, it is another story for the CNP channel. The Aite Group projects that CNP fraud will more than double by 2018, due largely to the migration of fraudsters to online and e-commerce channels, which will be more vulnerable.[18] Countries that have already rolled out EMV have experienced this shift.



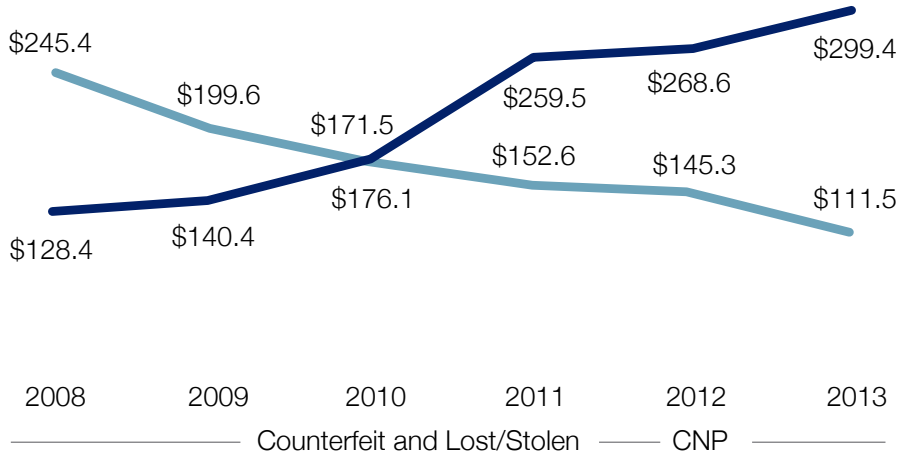
Source: Financial Fraud Action UK

CNP Fraud in Australia, 2008 to 2012
(In AU$ millions)



Source: Australian Payments Clearing Association

Canadian CNP and POS Credit Card Fraud Losses, 2008 to 2013
(In CA$ millions)



Source: Canadian Bankers Association

Ecommerce projections

Online spending in the U.S. is expected to rise from 262.3 billion in 2013 to $440 billion by 2017 (compound annual growth rate of 13.8%),[19] signifying a quick boost in online transactions. This, in addition to the EMV rollout, will contribute to the increase in CNP fraud.

Online merchants lost roughly $3.5 billion to payment card fraud in 2012, equaling more than a third of global card fraud losses.[20] The Aite Group estimates card fraud costs at about $8.6 billion per year in the U.S., a number that some analysts regard as understated.[21] In fact, some analysts put the number closer to $15 billion when taking into account the forensics, fraud that goes undetected, lawsuits and misclassified issuer losses.[22]

Merchants must start now to increase security against the more sophisticated types of attacks that will emerge. Current tools will likely no longer be enough to secure your business and your customers against fraudsters. The Aite Group says that nearly 75% of all retailers have no idea that a new "chip and pin" system is about to be introduced, leaving more businesses at risk. The key will be to find the appropriate tools for your business to deploy in your pre sale and post sale process to address these increased risks without turning away perfectly good sales.

The best fraud prevention strategy will allow you to manage multiple tools in real time based on analytics from your fluid data points and back-end feedback loops. Proactive use of this information and the ability to adjust quickly will be key to protecting your business. Unfortunately, often times this will be complicated as a result of having to juggle multiple vendors or integrations.

Enhanced 3D secure is a valuable tool for fighting CNP fraud

One of the biggest vulnerabilities in CNP commerce is authentication. The method of authenticating users by username and password doesn't work as is evident with the recent data breaches. Even after a business's data is compromised and users are informed that they should change their password, that doesn't guarantee that the customers will. Scarier yet is the fact that an estimated 55% of users have the same combination of username and password for all their online accounts – which can range from 15 to 20.[23]

HOW ENHANCED 3-D SECURE CAN HELP

The 3D Secure service is offered by the major card brands under several names: Verified-by-Visa, MasterCard SecureCode, American Express SafeKey, JCB International J/Secure and Diners Club ProtectBuy.[24] 3D Secure offers a number of benefits, particularly when use in conjunction with EMV chip cards. The tool gives merchants and issuers more control over card fraud and chargebacks by authenticating cardholder identities and assessing transaction risk while creating very little friction in the customer purchase process to provide a seamless and secure checkout.[25]

Previously, this tool did not have the shiniest reputation with retailers, as it caused several points of friction:

- Pop-up windows were confusing customers, who often had a hard time remembering passwords and ended up bailing at checkout.[26]
- No differentiation or scoring among customers and transaction caused unnecessary friction during checkout by requiring everyone to enroll and contributed to higher card abandonment.[27]

There have been a number of enhancements to 3D Secure that make it more secure an also improve the cardholder's experience:

DYNAMIC AUTHENTICATION eliminates static passwords that are inconvenient to remember for the cardholder and more vulnerable to compromise by fraudsters.[28]

CONTROL OF 3D SECURE IMPLEMENTATION has shifted to benefit the merchant, who can now decide when and for which particular transactions they want to utilize the 3D Secure feature, as opposed to the previous all-or-nothing standard.[29]

RISK-BASED AUTHENTICATION allows issuers to assess the risk of each transaction based on the data via the Access Control Server and an analysis of the transaction characteristics. Heightened authentication is only required on transactions designated as high risk, eliminating the requirement for cardholders to actively enroll before being eligible for 3D Secure.[30]

Rules-based authentication benefits merchants by providing flexibility to implement a customized authentication strategy for the transactions on which the issuers still require authentication. By implementing 3D Secure when and where it is most needed, low risk transactions are not disrupted and the customer process is streamlined, reducing cart abandonment.[31]

Layered and balanced protection is merchants' best bet to address the expected EMV impacts on CNP fraud

Fraud is expensive. Merchants in the U.S. reject approximately 3% of online orders for suspicion of fraud. Globally, that rate soars to 7.3%.[32] In addition to false positives and the potential to lose good sales, processing suspicious orders costs has its own costs. About 25% of ecommerce orders are flagged for manual review, a process that can range from 5 to 15 minutes per order.[33]

That is a huge time and resource commitment for merchants.

Merchants need to focus on their biggest vulnerabilities and ensure they are using the right tools at the right time and to the right degree. Some examples of tools that – when used in a combination tailored to your business – can create fortified layers of protection:

DIGITAL FINGERPRINTING: IP address sourced geo-location and proxy-piercing information, provides in depth, non-invasive insight into the risks involved with accepting transactions from specific IP addresses.

GUARDS AGAINST: Fraudsters masked by anonymizing proxies use stolen payment card data to make purchases or commit click fraud.

BUT DON'T: Rely on this tool alone without other validation efforts, which may result in false positives and lost sales. Underutlization of this tool can result in higher-than-average instances of fraud that could be prevented.

DEVICE FINGERPRINTING: Device information and reputation scoring, deep packet inspection and additional proxy piercing capabilities expose the fingerprint and personality of the true device submitting the transaction.

GUARDS AGAINST: Digital fingerprinting technologies that are stunted by criminals that have learned to thwart cookies and other inconsistent identifiers when making fraudulent purchases online.

BUT DON'T: Set scoring levels too high. This can result in false positives and subsequently, lost sales. Balancing Device Intelligence with IP Intelligence can strengthen controls without allowing one factor to override legitimate sales.

3D SECURE: As mentioned previously, 3D Secure or 3 Domain Secure is a cardholder authentication protocol for eCommerce transactions or card-not-present (CNP) purchases and covers 60% of U.S. shoppers and 90% cardholders internationally and helps eliminate chargebacks. It helps prevent "I don't recognize" or I didn't do it" chargeback disputes from occurring.

GUARDS AGAINST: Merchants are falling prey to increasing cases of friendly fraud where chargebacks are used as a form of shoplifting and customers claim they never received goods or services because of buyer's remorse.

BUT DON'T: Over-rely on this tool. Used alone, 3D Secure does not provide adequate coverage as banks choose the mechanism they deem appropriate in verifying the authenticity of the purchaser, which may not always be foolproof.[33] Instead, fortify with other intelligence measures that have been tested and toggled to meet a merchant's specific risk threshold.

POST BILLING CHARGEBACK ALERTS: Immediate notification of cardholder disputes from the credit card Issuer helps stop the fraudulent shipments of orders before they become a loss and gives the merchant an opportunity to respond to the dispute and resolve the issue before it becomes a chargeback.

GUARDS AGAINST: Lack of communication between card issuers and merchants means transactions suspected as fraud and cardholder initiated disputes snowball into chargebacks rather than potentially being avoided through issuer/merchant cooperation in addressing the issue, processing a refund or issuing a credit, ultimately preventing the chargeback.

BUT DON'T: Rely on issuer alerts alone. Front-end fraud prevention tools are necessary to maintain an acceptable chargeback ratio. Instead, augment fraud prevention tools with pre-chargeback notifications to dial back front-end fraud prevention tools, decreasing false positives while respecting the limits of the risk threshold.

Uniting these tools through a flexible, scalable solution with feedback loops that takes into account end-to-end transaction data and analytics allows you to fine-tune fraud controls in a way that maximizes sales while properly mitigating threats.

OUTSIDE SPECIALISTS CAN HELP STREAMLINE OPERATIONS

Working with a specialist can not only minimize the internal cost of time and resources but also can provide flexibility and improve the effectiveness of a merchant's overall risk mitigation strategy and maximize ROI.

Verifi's Intelligence Suite® solution was developed because we recognized the fine "art" of customizing fraud prevention. One size does not fit all and merchants' needs change over time as new threats emerge and businesses grow. Intelligence Suite serves as a "fraud hub" that facilitates rapid integration and fine-tuning of fraud controls based on real-time analytics and feedback loops, allowing merchants to remain agile, adjust on-the-fly and dial back front-end protection to maximize sales. The hub can be configured simply and corrected with our Intelligence Suite rules engine and gives merchants the ability to test and toggle various fraud prevention tools and customize continuously based on results. It's also a great tool for customer intelligence to aid marketing efforts and supports maintenance of industry compliance standards. When used in combination with our award winning Chargeback Dispute Resolution Network ("CDRN"), up to 30% of chargebacks can be identified and resolved post sale, allowing merchants to minimize fraud loss without losing sales on the front-end to false positives or overly restrictive pre sale fraud policies.

There is no one "silver bullet" to protect card-not-present transactions from fraud. History has shown that EMV can be very effective in eliminating counterfeit and lost/stolen card fraud; however, it has also served as a lesson that fraudsters adapt and CNP commerce is at risk. With proper preparation, merchants can mitigate this risk and ensure the protection of their online transactions.

Safeguarding against the upcoming onslaught of CNP fraud will prove to be a full-time task that may best be achieved by employing outside help. 3D Secure can provide strong support in fighting CNP fraud as EMV rolls out but should be augmented with additional fraud prevention measures. Merchants need a layered and balanced approach to fraud prevention that implements both network security measures (3D Secure) and a unique combination of tools tailored to the business needs and its particular fraud and risk situation. By leveraging proven technologies to evaluate and analyze the type of fraud they are experiencing and tailoring solutions to their business, merchants can achieve thorough fraud prevention without turning away good sales.

ABOUT VERIFI

Since 2005, Verifi has been a leading provider of global electronic payment and full-suite risk management solutions, helping card-not-present merchants improve their bottom line. The highly customizable payment and real-time reporting platform serves as a foundation for Verifi's suite of fraud solutions and management strategies. With a commitment of reducing risk while increasing profitability for clients, Verifi's multi-layered approach enables transaction risk management and mitigation, business optimization strategies, cardholder authentication and chargeback prevention and recovery services for all major credit card brands and Pay Pal. Verifi is PCI Level 1 certified and headquartered in Los Angeles, California.

VERIFI™

For More Information

Main Phone: (323) 655-5789 Mon-Fri 8:00 AM – 5:00 PM PST

Main Fax: (323) 655-5537

Email Address: info@verifi.com

Mailing Address: 8391 Beverly Blvd., Box #310, Los Angeles, CA 90048

Citations

1 *Aite 20140630-Merchants-and-Cybercriminals-Duke-It-Out-Note-pdf_5983_18210_10125)10241-3.pdf*

2 *https://www.chasepaymentech.com/faq_emv_chip_card_technology.html*

3 *https://www.chasepaymentech.com/faq_emv_chip_card_technology.html*

4 *https://www.chasepaymentech.com/faq_emv_chip_card_technology.html*

5 *20140605-EMV-Lessons-Learned-and-the-US-Outlook-Report-pdf_5898_18213_10125_10179.pdf*

6 *20140605-EMV-Lessons-Learned-and-the-US-Outlook-Report-pdf_5898_18213_10125_10179.pdf*

7 *http://www.mastercardadvisors.com/_assets/pdf/emv_us_aquirers.pdf*

8 *20140605-EMV-Lessons-Learned-and-the-US-Outlook-Report-pdf_5898_18213_10125_10179.pdf*

9 *20140605-EMV-Lessons-Learned-and-the-US-Outlook-Report-pdf_5898_18213_10125_10179.pdf*

10 *20140605-EMV-Lessons-Learned-and-the-US-Outlook-Report-pdf_5898_18213_10125_10179.pdf*

11 *20140605-EMV-Lessons-Learned-and-the-US-Outlook-Report-pdf_5898_18213_10125_10179.pdf*

12 *20140605-EMV-Lessons-Learned-and-the-US-Outlook-Report-pdf_5898_18213_10125_10179.pdf*

13 *20140605-EMV-Lessons-Learned-and-the-US-Outlook-Report-pdf_5898_18213_10125_10179.pdf*

14 *http://www.tsys.com/acquiring/engage/white-papers/United-States-EMV-Adoption.cfm#5*

15 *http://www.tsys.com/acquiring/engage/white-papers/United-States-EMV-Adoption.cfm#5*

16 *http://www.tsys.com/acquiring/engage/white-papers/United-States-EMV-Adoption.cfm#5*

17 *http://www.tsys.com/acquiring/engage/white-papers/United-States-EMV-Adoption.cfm#5*

18 *Aite 20140630-Merchants-and-Cybercriminals-Duke-It-Out-Note-pdf_5983_18210_10125)10241-3.pdf*

19 *http://christophermalloy.weebly.com/uploads/2/7/1/0/27101405/analytical_report.pdf*

20 *http://images.demand.cybersource.com/Web/CyberSource/CyberSource_2013_Online_Fraud_Report.pdf?utm_campaign=Fraud%20Report%202013%20-%20Form%20auto-reply&utm_medium=email&utm_source=Eloqua*

21 *Aite 20140630-Merchants-and-Cybercriminals-Duke-It-Out-Note-pdf_5983_18210_10125)10241-3.pdf*

22 *http://www.tsys.com/Downloads/upload/2013_TSYS_EMV_3D_Secure_Report_PC_Video_FinalV1.pdf*

23 *http://go.authentic8.com/blog/recycling-is-good-for-the-environment-not-your-passwords*

24 *http://www.tsys.com/Downloads/upload/2013_TSYS_EMV_3D_Secure_Report_PC_Video_FinalV1.pdf*

25 *http://www.tsys.com/Downloads/upload/2013_TSYS_EMV_3D_Secure_Report_PC_Video_FinalV1.pdf*

26 *http://www.pymnts.com/exclusive-series/2014/looking-beyond-3-d-secures-rocky-past/#.U-UYmeCnBG5*

27 *http://www.pymnts.com/exclusive-series/2014/looking-beyond-3-d-secures-rocky-past/#.U-UYmeCnBG5*

28 *http://www.emc.com/collateral/white-papers/card-not-present-fraud-post-emv-env-wp.pdf*

29 *http://www.emc.com/collateral/white-papers/card-not-present-fraud-post-emv-env-wp.pdf*

30 *http://www.emc.com/collateral/white-papers/card-not-present-fraud-post-emv-env-wp.pdf*

31 *http://webcache.googleusercontent.com/search?q=cache:-CqrzX6YLGMJ:www.redworldwide.com/wp-content/uploads/2013/09/3D-Secure-expert-opinion-US.pdf+3d-secure-expert-opinion-us.pdf&cd=1&hl=en&ct=clnk&gl=us&client=safari*

32 *http://www.tsys.com/Downloads/upload/2013_TSYS_EMV_3D_Secure_Report_PC_Video_FinalV1.pdf*

33 *http://images.demand.cybersource.com/Web/CyberSource/CyberSource_2013_Online_Fraud_Report.pdf?utm_campaign=Fraud%20Report%202013%20-%20Form%20auto-reply&utm_medium=email&utm_source=Eloqua*

34 *https://blogs.cisco.com/security/the_3d_secure_protocol_implementation_flaws_and_possible_resolutions/*