

Card-Not-Present Fraud in a Post-EMV Environment: Combating the Fraud Spike

Prepared for:



TABLE OF CONTENTS

INTRODUCTION	3
METHODOLOGY	3
U.S. CARD FRAUD: LET THE MIGRATION BEGIN	4
SQUEEZING THE BALLOON.....	4
SOLUTIONS TO CNP FRAUD	8
BEHAVIORAL ANALYTICS.....	8
TOKENIZATION.....	8
3-D SECURE	9
SOLUTION ATTITUDES AND ADOPTION	9
CONCLUSION	12
ABOUT AITE GROUP.....	13
AUTHOR INFORMATION	13
CONTACT.....	13
ABOUT RSA	14
RSA ADAPTIVE AUTHENTICATION FOR E-COMMERCE.....	14
RSA DATA PROTECTION MANAGER	14
RSA WEB THREAT DETECTION	14

LIST OF FIGURES

FIGURE 1: TIMELINE FOR U.S. EMV DEPLOYMENT	4
FIGURE 2: CANADIAN CNP AND POS CREDIT CARD FRAUD LOSSES, 2008 TO 2013	5
FIGURE 3: U.K. CNP FRAUD LOSSES 2004 TO 2013	6
FIGURE 4: U.S. CNP CREDIT CARD FRAUD LOSSES 2011 TO 2018.....	7
FIGURE 5: PERCEIVED EFFECTIVENESS OF SECURITY SOLUTIONS	10
FIGURE 6: MERCHANT ADOPTION OF SECURITY SOLUTIONS.....	10

INTRODUCTION

It's a tough time to be in the payment card issuance or acceptance business. U.S. credit card fraud is now a whopping 10 basis points, a 100% increase from just seven years ago thanks to increasing fraud at the point of sale (POS) and rising card-not-present (CNP) fraud, which now represents 45% of total U.S. card fraud. At the same time, U.S. online and mobile commerce is growing at a 15% annual rate, reinforcing the importance for merchants to balance fraud prevention measures with the user experience. Against this backdrop, EMV arrives as a new variable in the fraud prevention landscape.

Long an outlier, the United States is finally on its way to joining the more than 80 countries around the world in upgrading its payment card security to embrace the EMV standard, a framework for interoperable chip-based payment cards. The computer chip embedded in the card creates a dynamic code that is unique to each transaction and significantly reduces the risk of counterfeit card use at the POS.

While reduced counterfeit fraud is good news for the issuers that have been enduring rapidly rising fraud rates, criminals will not idly sit by and just absorb this hit to their bottom line. Every other country that has adopted EMV has seen a precipitous increase in attacks on the CNP channels, and the United States will be no exception.

The good news is that a number of technologies available to merchants and issuers, such as tokenization, behavioral analytics, and 3-D Secure (yes, 3-D Secure, with vast improvements over the initial product of years past), have the potential to blunt the impact of the rising tide of threats. This white paper begins with an update on the timeline for the U.S. migration and the expected impact on CNP fraud. It then provides an overview of key solutions that will reduce the impact, along with merchants' current and planned rates of adoption.

METHODOLOGY

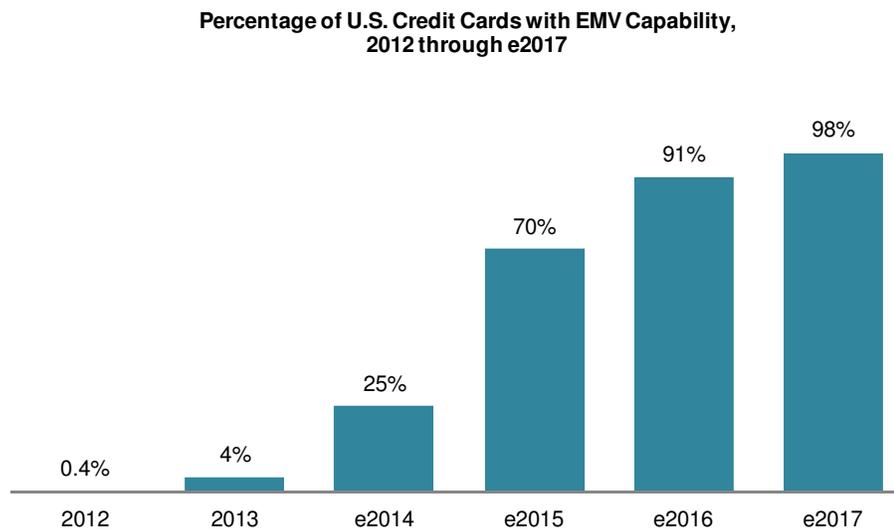
This white paper is based on data collected in two separate research efforts. In the first, Aite Group surveyed fraud executives at 36 large U.S. merchants from March to May 2014 to understand points of pain and planned solutions. Aite Group also interviewed card executives from payment networks and 18 of the top 40 U.S. issuers in April and May 2014 to understand the current levels of card fraud, as well as the pace of EMV deployment in the U.S. market.

U.S. CARD FRAUD: LET THE MIGRATION BEGIN

Judge Richard Leon's July 2013 ruling, rejecting the U.S. Federal Reserve's interpretation of the Durbin amendment, introduced substantial uncertainty into the U.S. EMV migration, slowing it to a snail's pace until the high-profile Target data breach, which became public in December 2013. While EMV would not have stopped the breach, it certainly would have impeded the criminals' ability to monetize it, and the lack of EMV technology in the United States took center stage in subsequent media coverage and congressional hearings. This scrutiny, combined with a ruling by the U.S. Federal Court of Appeals striking down Judge Leon's opinion in January 2014, have combined to re-energize the U.S. EMV migration, which once again is moving forward at full speed.

While many U.S. issuers began issuing EMV-enabled credit cards to international travelers as early as 2010, very few have begun general issuance. As the experience of other countries has shown, however, high rates of fraud losses are a powerful motivator. With much of the Durbin-related uncertainty in the past, many issuers are now moving aggressively to get chip-enabled cards in the market ahead of the October 2015 liability shift date. Figure 1 shows the expected timeline for cards to be deployed to U.S. consumers.

Figure 1: Timeline for U.S. EMV Deployment



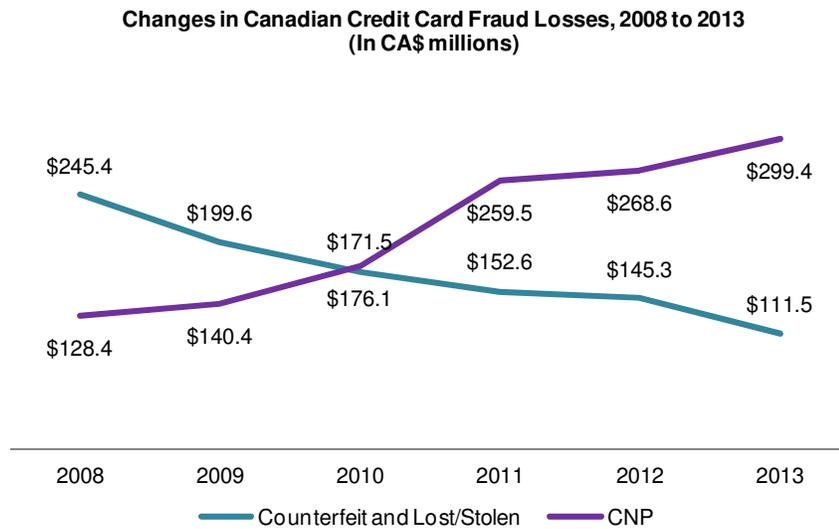
Source: Aite Group interviews with card executives from 18 of the top 40 U.S. issuers and payment networks, April and May 2014

SQUEEZING THE BALLOON

EMV will not result in an elimination of counterfeit fraud, nor will EMV spell an end to database breaches; it will merely force fraudsters to adjust their tactics and targets. The data from Canada's EMV migration paints this picture clearly; counterfeit and lost/stolen fraud enjoyed a

54% decline from the inception of the migration in 2008 through 2013, while CNP saw a corresponding increase, jumping a whopping 133% over the same time period (Figure 2).

Figure 2: Canadian CNP and POS Credit Card Fraud Losses



Source: Canadian Bankers Association

CNP fraud rose sharply in the wake of the U.K. liability shift as well, growing by 79% between the liability shift in 2005 and its peak in 2008. Development of more advanced fraud analytics by issuers and merchants as well as increased use of 3-D Secure technology helped to rein in the rising problem, although subsequent adjustments by fraudsters to target softer targets such as the call center are once again causing CNP losses to rise, as shown in Figure 3.¹

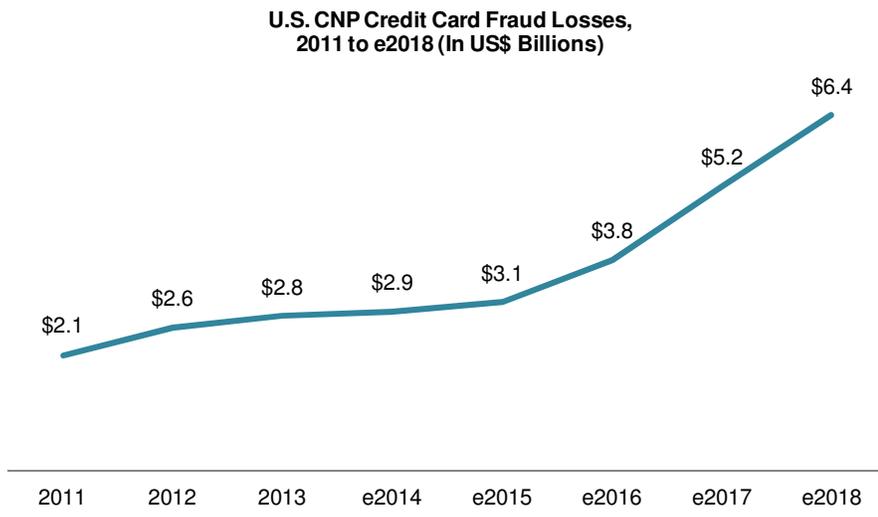
1. For more detail on 3-D Secure, see Aite Group's report *3-D Secure: Poised to Live Long and Prosper*, March 2013.

Figure 3: U.K. CNP Fraud Losses

Source: Financial Fraud Action UK

The U.S. market will not be exempt from this trend and should prepare for a jump in its CNP fraud rate as its migration takes place. The rise will likely be more gradual than it was in the U.K., since the U.S. market is much more fragmented, and some issuers will lag in upgrading their portfolios to chip-based cards. The CNP spike in the United States could be quite large, and CNP merchants in non-U.S. geographies should brace for an uptick in their fraud as well. Cross-border counterfeit fraud was a big problem when many other countries engaged in their EMV migration, as criminals still had the opportunity to use stolen card data in the magnetic-stripe-reliant United States. No equivalent outlet will exist as the United States effects its migration, so the full force of stolen card monetization will focus on the CNP channel. The ray of hope is that merchants and issuers alike have been bolstering their CNP fraud prevention capabilities significantly in recent years, and the technology investments appear to be paying off. The growth rate in U.S. CNP credit card fraud was flat from 2012 to 2013, for the first time since the invention of online shopping (Figure 4). Even so, U.S. CNP fraud losses will exceed US\$6 billion by 2018.

Figure 4: U.S. CNP Credit Card Fraud Losses



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

SOLUTIONS TO CNP FRAUD

A wide variety of solutions are available to secure the CNP environment; as with any type of fraud prevention, no single point solution will suffice. Instead, merchants and issuers need to take a layered approach to their defenses.

BEHAVIORAL ANALYTICS

Behavioral analytics are a key technology for merchants and issuers seeking to bring their fraud-mitigation technologies down to the transaction level. Behavioral analysis tools detect fraud by monitoring the user session and transactions to detect suspicious activities or patterns. Behavior analysis technologies can also examine Web navigation techniques to highlight anomalies indicative of suspicious activity, such as business logic abuse or unusual behavior during shopping or the checkout process. As with any tool, there is a certain level of false positives, and it is good to have a stepped-up authentication capability available to include the end user in the triage process.

TOKENIZATION

Tokenization is a great complement to EMV; it essentially picks up where EMV leaves off in the card security continuum. EMV secures the communication between the card and the POS terminal, using dynamic data to effectively prevent counterfeit fraud. EMV does nothing to encrypt the data, however, which still flows in the clear once the card data enters the merchant system. Tokenization can take over at this point, replacing the card data with a secure token.

Tokenization removes the account number on the payment card from merchants' databases and replaces it with a string of letters and numbers that serve as a proxy for the true cardholder data. There is a one-to-one relationship between the tokenized string and the account data stored at the acquirer or network level, so the merchant can use the token to facilitate settlement, recurring payment processing, chargeback processing, fraud management, etc., but the token is useless to criminals if the merchant's system is compromised. This technology is useful for removing card data from the scope of Payment Card Industry Data Security Standard (PCI DSS) and protecting the data from compromise in both physical and remote channels.

There are a couple of different approaches to tokenization in the market. Tokenization at the POS is a service that has been available to merchants for a few years, typically sold to them via their acquirer or processor. Initiatives to tokenize data at the issuer level are also underway, with two competing efforts led by EMVCo and The Clearing House. The acquirer and issuer tokenization efforts are fundamentally different and are more complementary than competitive. With the tokenization product that acquirers sell to merchants, the tokenization is applied to transactions as they flow through the POS, protecting all of the transactions within the merchant environment. Issuer-driven tokenization efforts are focused on the CNP channels. As a merchant sends a transaction to an issuer, that issuer will return a 16-digit numerical token that the merchant can store in lieu of the card number, over time protecting tokenizing issuers and their cardholders from merchant breaches.

3-D SECURE

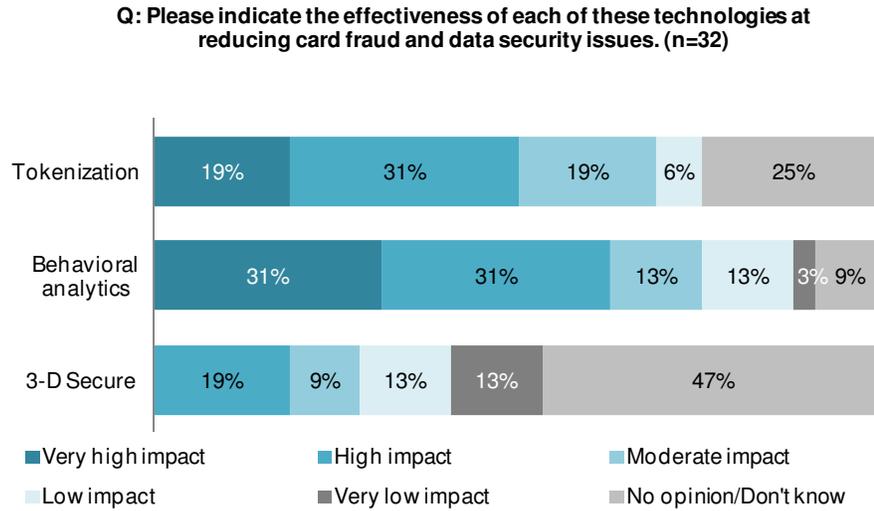
3-D Secure is a protocol designed to add an additional layer of authentication to CNP transactions. 3-D Secure refers to the underlying technology, which has been separately productized and marketed by the payment networks and their issuers as Verified by Visa, MasterCard SecureCode, and American Express SafeKey. A key value driver for merchants is that when they invoke 3-D Secure for CNP transactions, the fraud liability shifts to the issuer, even if the issuer does not have the corresponding Access Control Server infrastructure on its side to support the 3-D Secure request through risk assessment and stepped-up authentication prompts. The networks, issuers, and vendors associated with 3-D Secure have worked to address the early challenges associated with the protocol and have introduced a number of fundamental changes designed to improve the cardholder's experience and the solution's effectiveness:

- **Migration to dynamic data:** The authentication mechanism is migrating from static passwords (which are both easily forgotten by the genuine cardholder and easily compromised by the bad guys) to dynamic authentication, which is typically more user-friendly and more difficult to defeat.
- **Putting the merchant in control:** As opposed to the early implementations of 3-D Secure when use of the service was an all-or-nothing proposition, U.S. merchants now generally have the ability to selectively decide when they want to invoke 3-D Secure and for which transactions.
- **Transition to risk-based authentication:** Many issuers began taking a risk-based authentication approach to 3-D Secure, assessing the risk of the transaction based on enriched data flowing through the Access Control Server, as well as analysis of the transaction characteristics, and only requiring stepped-up authentication on those transactions that are deemed to be high risk. An additional benefit of the risk-based authentication approach is that it eliminates the need for cardholders to actively enroll to be eligible for 3-D Secure.

SOLUTION ATTITUDES AND ADOPTION

When asked about the effectiveness of tokenization and behavioral analytics, merchants are quite positive, with 62% of merchants believing that behavioral analytics have "high" or "very high" impact on fraud and data security issues, while 50% believe that tokenization have a "high" or "very high impact" (Figure 5). Twenty-eight percent of merchants surveyed believe that 3-D Secure has a "moderate" or "high" impact on fraud and data security issues, while the jury is still out for 47% of respondents. This actually represents a sea change compared to prior research and speaks to the changing opinion of 3-D Secure with the introduction of risk-based authentication and other enhancements to the user experience.

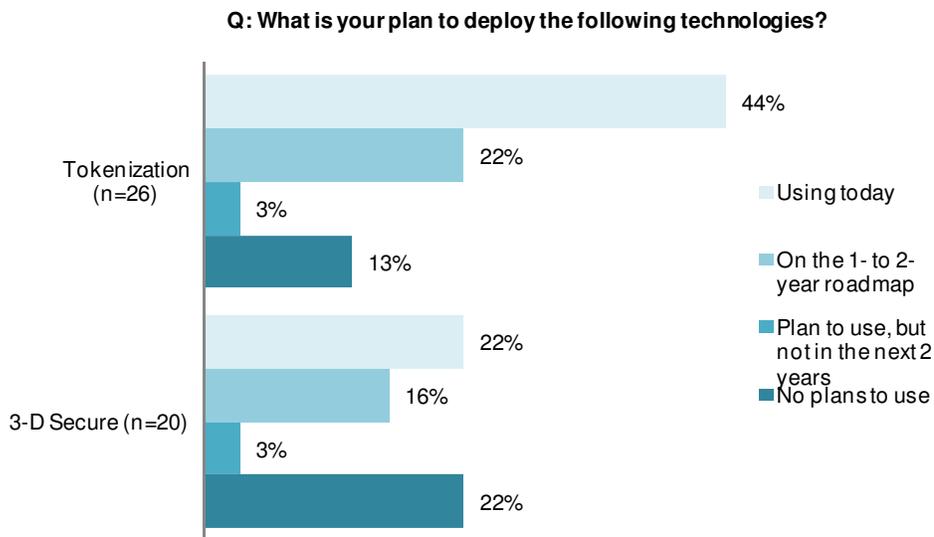
Figure 5: Perceived Effectiveness of Security Solutions



Source: Aite Group survey of 36 merchant fraud executives, March to May 2014.

When asked about use of technologies such as tokenization and 3-D Secure, 44% of merchants surveyed use tokenization in at least one of their channels today, and another 22% plan to introduce tokenization within the next one to two years. Twenty-two percent of merchants surveyed use 3-D Secure, while another 16% plan to deploy it within the next one to two years (Figure 6).

Figure 6: Merchant Adoption of Security Solutions



Source: Aite Group survey of 36 merchant fraud executives, March to May 2014.

A majority of the issuers with which Aite Group spoke either have already deployed risk-based authentication to support 3-D Secure or plan to do so within the next year. The combination of rising CNP fraud and an improved user experience should continue to make 3-D Secure a more attractive offering for merchants over time.

CONCLUSION

Card fraud is rapidly escalating at the POS and in CNP channels. The arrival of EMV will certainly help quell counterfeit fraud, but the experience of other countries shows that the arrival of EMV will do nothing to stop database breaches, and CNP fraud will rise precipitously unless preventative measures such as tokenization, behavioral analytics, and 3-D Secure are adopted. With the clock ticking away the minutes until the October 2015 liability shift, here are a few recommendations for merchants and issuers:

For issuers:

- **Invest in risk-based authentication for CNP transactions.** CNP fraud is not just a merchant problem anymore. Thanks to the growing U.S. adoption of 3-D Secure, as well as the competitive pressure to ensure a delightful cardholder experience, effective CNP risk assessment is a shared burden. Issuers will see increasing volume of 3-D Secure transactions along with any resulting fraud liability. Risk-based authentication will help issuers to better assess transaction risk with few false positives and minimal impact to the customer experience.
- **Embrace tokenization.** Merchant data breaches aren't going away. The best way to create a secure card environment is to remove the sensitive data from the merchant's system, so when the inevitable breach does occur, your cardholders will be protected.

For merchants:

- **Embrace tokenization.** In light of the current threat environment, you have to assume that the bad guys are going to get into your systems sooner or later. The best way to stay out of the headlines is to make sure that when they do get in, they don't get any valuable data.
- **Invest in behavioral analytics.** Behavioral analytics within the online and mobile channels are transparent to the end user and provide a great way to detect the patterns indicative of attacks that are either imminent or underway.
- **Deploy 3-D Secure.** The attacks on the CNP channel will spike in a post-EMV world. 3-D Secure not only adds additional security to the transaction but also relieves merchants of the fraud liability. Thanks to the recent enhancements to the product and the increasing use of risk-based authentication by issuers, 3-D Secure now provides these benefits with minimal intrusion on the user experience.

ABOUT AITE GROUP

Aite Group is an independent research and advisory firm focused on business, technology, and regulatory issues and their impact on the financial services industry. With expertise in banking, payments, securities & investments, and insurance, Aite Group's analysts deliver comprehensive, actionable advice to key market participants in financial services. Headquartered in Boston with a presence in Chicago, New York, San Francisco, London, and Milan, Aite Group works with its clients as a partner, advisor, and catalyst, challenging their basic assumptions and ensuring they remain at the forefront of industry trends.

AUTHOR INFORMATION

Julie Conroy

+1.617.398.5045

jconroy@aitegroup.com

CONTACT

For more information on research and consulting services, please contact:

Aite Group Sales

+1.617.338.6050

sales@aitegroup.com

For all press and conference inquiries, please contact:

Aite Group PR

+44.(0)207.092.8137

pr@aitegroup.com

For all other inquiries, please contact:

info@aitegroup.com

ABOUT RSA

RSA, the security division of EMC, is the premier provider of intelligence-driven security solutions. RSA helps the world's leading organizations solve their most complex and sensitive security challenges: managing organizational risk, safeguarding mobile access and collaboration, preventing online fraud, and defending against advanced threats. Combining agile controls for identity assurance, fraud detection, and data protection, robust security analytics, industry-leading GRC capabilities, and expert consulting and advisory services, RSA brings visibility and trust to millions of user identities, the data they create, the transactions they perform, and the IT infrastructure they rely on. For more information, please visit www.RSA.com.

RSA ADAPTIVE AUTHENTICATION FOR E-COMMERCE

RSA Adaptive Authentication for e-commerce offers financial institutions additional cardholder protection and fraud management tools to secure the online shopping experience. Based on the widely accepted 3-D Secure protocol and infrastructure, RSA Adaptive Authentication for e-commerce provides an additional layer of security for card not present (CNP) transactions without the need for enrollment, thereby offering a superior customer experience and reducing the risk of abandonment.

RSA Adaptive Authentication for e-commerce leverages RSA's proven risk-based authentication technology to evaluate each online transaction in real time. The solution evaluates over 100 fraud indicators per transaction to assess the associated risk level of a customer and the credit card being used for payment at time of checkout. RSA Adaptive Authentication for e-commerce meets the stringent requirements of the MasterCard SecureCode Certified Partner program and has attained the MasterCard SecureCode Partner designation.

RSA DATA PROTECTION MANAGER

RSA Data Protection Manager secures sensitive data at the point of capture with tokenization and/or data encryption and leverages a single platform for true enterprise-wide key management across the infrastructure. RSA Data Protection Manager helps ease the burden of compliance by removing sensitive data and applications from the scope of audit through tokenization and offers built-in audit logs for easy reporting. Through a centralized platform, RSA Data Protection Manager allows for management or protection of a variety of data types including payment card information (PCI) and personally identifiable information (PII).

RSA WEB THREAT DETECTION

RSA Web Threat Detection uses behavioral analytics to help identify anomalous activity across Web applications. The solution provides visibility into click stream data to show how users interact with a website and flags unusual behavior that may be indicative of a cyber attack. With the ability to analyze up to 300,000 clicks per second, RSA Web Threat Detection can identify myriad threats including account takeover, business logic abuse, site scraping, and DDoS.