THE POST EMV CHALLENGE
CARD NOT PRESENT FRAUD

CAPCO

White Paper

Introduction

The introduction of EMV chip technology has impaired the ability of perpetrators to facilitate fraud at the point of sale. With EMV continuing to diminish incidents of fraud where the card is present, issuers and acquirers now must find solutions to address the long-standing challenge that EMV adoption does not alleviate – card not present fraud (CNP fraud) – exploring and pursuing new tools that can address it. Herein, we revisit some of the existing tools to counter CNP fraud and discuss upcoming solutions to consider.

History and background

Payments card industry professionals have heard the repeated warnings about increasing CNP fraud rates after EMV adoption country by country over the last few years. Now that the U.S. payments market is actively transitioning to EMV chip technology – after years of resistance, general misunderstandings and high-profile litigations – if predictions are accurate, the U.S. will soon experience the long-standing post-EMV migration trend of spikes in CNP fraud rates. Chiefly because of EMV chip adoption, credit card CNP fraud losses within the U.S. market are expected to increase to $6.4 billion by 2018, roughly doubling U.S. CNP fraud rates prior to EMV adoption.

Figure 1 - U.S. Card Fraud Losses 2012 to 2018* (in US$ billions) - source: Aite Group

The need for short- and long-term strategies

Both card issuers and merchants should actively explore and pursue short- and long-term CNP fraud prevention and reduction strategies.

Short-term strategies should include features that issuers and merchants can support today. For example, issuers and acquirers who haven't begun discussions with their processors to understand how and when 3D Secure 2.0 will be rolled out should do so now. This will help issuers and acquirers understand the effort needed to support and include the appropriate plans within product and technology road maps.

While having one eye on a short-term strategy, the other eye should begin evaluating future solutions. Instead of reacting to the spike in CNP fraud, issuers and merchants should explore potential solutions that can properly authenticate cardholders. The cost to deliver these future solutions will be far less expensive in the long term than the anticipated CNP fraud losses. An effective CNP fraud strategy should cover every channel, for example: online, mobile and alternative payment methods, including digital currencies.

“

Instead of reacting to the spike in CNP fraud, issuers and merchants should explore potential solutions that can properly authenticate cardholders. The cost to deliver these future solutions will be far less expensive in the long term than the anticipated CNP fraud losses.

Current approaches for fighting CNP fraud

Before defining a long-term CNP fraud strategy, one must become familiar with the current day authentication methods that cardholders encounter during the checkout process. Additionally, like any fraud strategy, one must strive to achieve the perfect balance between authenticating/approving transactions and potential checkout friction or transaction declines that ultimately damage the online purchase experience.

The effectiveness of the various types of cardholder authentication practices varies dramatically based on volumes, combinations of fraud mitigation tools and aggressiveness with regard to declining valid transactions (called “false positive declines”).

Some of the common current approaches to cardholder authentication, typically dependent on merchant adoption during checkout, are shown in the table below.

Authentication Approaches	Description	Value Perspective	CNP Acceptance Channels		
			Mobile Wallet	Online	Mail/ Tele
3D Secure (3DS)	An authentication protocol, dating back to 1999, that typically requires a password linked to the card before it can be used for a purchase. 3D Secure also requires card issuer support and individual cardholder setup. During 2015, 18 percent of all e-commerce transactions traveled across the 3DS infrastructure. 3DS brands within the U.S. include MasterCard SecureCode, Verified by Visa, Discover ProtectBuy and American Express SafeKey. EMVCo members (including MasterCard, Visa, American Express and Discover) are about to support the next generation of this protocol, called 3D Secure 2.0. Specifications have been released.	This procedure can cause friction for the cardholder and lead to unacceptable checkout abandonment rates. This solution is slated to be revamped significantly.	x	x	
CVV Validation	The three or four-digit number found on the back of a debit or credit card.	This form of validation is thought to be questionable, because this information is readily available on stolen cards.	x	x	x
Tokenization	Tokenization intercepts the card information (typically card number) at the point-of-sale terminal or online payment interface and replaces the cardholder data with randomly generated proxy numbers (“tokens”).	This solution is increasingly used and favored by merchants, because it prevents hacking of critical data elements. The card data is never stored intact anywhere, making it nearly impossible for hackers to reassemble it through decryption or reverse engineering.	x	x	
PINs	The use of personal identification numbers has been traditionally associated with face to face point of sale or kiosk transactions. However, the PIN debit networks have been expanding support to a limited number of CNP transactions.	While use of a PIN in a CNP purchase transaction is extremely limited, it has proven to be a valid authentication method. The PIN Debit Networks have partnered with Acculynk to offer this service in a limited capacity.		x	

Authentication Approaches	Description	Value Perspective	CNP Acceptance Channels		
			Mobile Wallet	Online	Mail/ Tele
User Credentials	Validation of any type of association between a cardholder's accounts and email address.	Merchant-based solution applicable to repetitive purchases.	x	x	x
Trust Tags	Digital labels that are applied to a cardholder's persona to indicate their trustworthiness. Typically, repeat customers are considered more trustworthy.	Merchant-based solution applicable to repetitive purchases.	x	x	x
Knowledge-based Authentication	Online merchants sometimes will ask cardholders to create a checkout account with their site to answer personal questions that only the cardholder would know.	This procedure can cause friction for cardholders if they forget the appropriate responses.		x	x
Personal ID	The capturing of email addresses, accounts, devices, IP addresses and address of the cardholder to validate the cardholder.	Merchant-based solution applicable to repetitive purchases.	x	x	
Phone Number Verification	This approach asks the cardholder for their phone number and then sends a code via text message that the purchaser must enter to complete the transaction.	Merchant-based solution resulting in some degree of consumer friction.		x	
Biometrics	Today, biometrics are predominantly used in conjunction with mobile payments. Previous concerns focused on validation failures and on the ability to lift fingerprints from the glossy surface of a mobile phone.	This approach is making great strides that ultimately will play a key role in the go forward validation of cardholders. Biometrics is still viewed as one factor in a multifactor authentication strategy.	x	x	
Multifactor Authentication	This approach requires the completion of more than one authentication protocol to authorize the transactions.	Using more than one authentication protocol logically adds value. If one factor is compromised or broken, the attacker still has at least one more barrier to breach before successfully breaking into the target.	x	x	x

In evaluating the current approaches, only a handful of the methods could be universally available, but they are insufficient to wholly prevent CNP fraud. A new solution, or combination of solutions, is necessary to effectively fight CNP fraud across all channels in the future.

Planning for the Future

Three evolving approaches for combatting CNP fraud in the future are biometrics, 3D Secure 2.0 and development of standards through the FIDO Alliance.

BIOMETRICS

Biometrics have been used in high-security applications for many years, and with advances in the associated technologies, they should now be on issuer and merchant road maps for improving customer authentication. Physical biometrics offer commonly known options, such as fingerprint, iris and voice recognition technologies.

Today, the use of biometrics is gaining support within the mobile CNP payments market. Within the last few years, the capabilities of consumer devices have evolved, and dependencies on specialized hardware have diminished, resulting in an environment where biometrics could become the preferred authentication capability. Biometrics will eventually become mainstream, largely driven by mass-market mobile devices and consumers gradually accepting this method. MasterCard has been trialing biometric authentication within the U.S. under the MasterCard Identity Check brand.

When considering biometrics, financial institutions must consider impacts to all stakeholders and potential constraints across all business units, including fraud management, call center operations, back-office operations, information technology, security, compliance and legal. Implementing a successful authentication solution requires understanding the implications it has for all touch points.

3-D SECURE 2.0

EMVCo, which is owned by the world's six leading payment card companies, designed the new 3-D Secure protocol, 2.0, which supports a layered approach to the authentication of e-commerce transactions. The roadmap for 3-D Secure 2.0 encompasses an extended period of time, with the initial rollout targeted for 2018. It would appear that EMVCo has developed this solution to appeal to a wide audience.

EMVCo designed the new protocol to address the issues and challenges associated with the original solution, and it includes security for technologies that did not exist when 3-D Secure was first introduced. Reported enhancements include improvements in the transaction flow to address transaction latency, enriched transaction data to be shared between merchants and issuers to enhance transaction risk modeling, elimination of static passwords, support for browser-based transactions and integration into mobile applications, including support for application-based purchases.

FIDO ALLIANCE STANDARDS

The FIDO Alliance is a consortium created to develop an open set of technical specifications and promote technology standards for identity verification and authentication. Its members include the leading card networks, PayPal, Google, Microsoft and others.

FIDO's objective is to reduce the dependency on usernames and passwords, through support of an interoperable architecture that supports multiple vendors through interoperable standards. This method ensures that future solutions do not marginalize or omit elements of the strategy. Enablement of additional technological abilities through the advancement of technology will add to and enhance the solution, rather than force restrategizing with each new technology.

The Evolution of Combating CNP Fraud

In defining a future fraud strategy to address the anticipated growth in CNP fraud, issuers and merchants must understand what solutions will be available, how well the new solutions will work and how they will ultimately impact cardholders attempting to make valid transactions. Some experts have suggested that the cost of false positive declines can sometimes near the cost of actual fraud.

For cardholder authentication and combatting CNP fraud, no silver bullet may arise that works across all channels. The optimal approach is to support a combination of tools and solutions that balance the costs of implementation with the expected benefits of managing CNP fraud losses.

Issuer and merchant strategies could include the use of tools that have yet to be proven and thus require analysis before launching. The tools and strategies that issuers and merchants deploy must work cohesively together with the individual components and be revised or replaced periodically based on the overall fraud management strategy.

For the interim, financial institutions are faced with fractured and inconsistent cardholder experiences based on differences in merchant capabilities and multiple and evolving technologies that can integrate with various types of authentication practices.

The Need for Standards around Identity Verification and Authentication

In an ideal world, there would be a unified, layered approach to combatting CNP fraud.

The outermost layer is the short-term solution. This would include development of the standards and high-level strategy that the industry will use to combat CNP fraud. Current technology will limit the short-term solution, which will need to utilize available capabilities to their full potential or in new and innovative ways to put a stop-gap solution in place. The short-term strategy needs to move quickly, faster than current technology can evolve alongside. Technology will develop a road map to catch up in the second layer.

The second layer is a plan for a long-term strategy that utilizes the lessons learned globally to combat CNP fraud. This would likely involve new technology that enables the industry to present a unified front against fraud. The challenge in this layer is aligning a critical mass of industry participants to the ideal long-term solution. This alignment is vital for avoiding solution fragmentation across the industry and for preventing CNP fraud from shifting to weaker industry participants.

The third layer is adoption and implementation and is arguably the most difficult to achieve. For full effectiveness, the entire industry must adopt the plan, or CNP fraud will shift to segments of the industry that remain fragmented. The hurdle of adoption across the industry will be the single most difficult element in combatting CNP fraud. Although the industry is seeing indications that suggest a move to open standards that will accelerate adoption of technology and encourage interoperability, it is not there yet.

The core of the approach is the technological solution. It should be developed to fit the standards and strategy outlined by the outer layer, not vice versa. Technology must fit the long-term needs such that the functionality and strategic vision of the industry does not need to be compromised and potentially weakened.

Conclusion

Management of card fraud is an ongoing and evolving process, and its most current evolutionary stage, EMV chip technology, has helped reduce fraud at the point of sale. However, detecting and preventing fraud when the card is not present continues to pose challenges and requires industry mandates to adopt capabilities that are not fully developed.

Nevertheless, issuers and merchants must stay abreast of new authentication methods and prepare to implement solutions when they become available. Exploring options and developing strategies in advance of this will shorten implementation timing and accelerate realization of reduced CNP fraud losses.

AUTHORS

Vince Forte vincent.forte@capco.com
Joe Sienko joseph.sienko@capco.com

ABOUT CAPCO

Capco, an FIS™ company, is a global management consultancy with a focus in financial services including banking and payments, capital markets, and wealth and asset management. We combine innovative thinking with unrivalled industry knowledge to deliver business consulting, digital, technology and transformational services. Our collaborative and efficient approach helps clients reduce costs, manage risk and regulatory change while increasing revenues. Visit us at www.capco.com and follow us on Twitter @Capco.

CAPCO WORLDWIDE:

BANGALORE
BRATISLAVA
BRUSSELS
CHICAGO
DALLAS
DÜSSELDORF
EDINBURGH
FRANKFURT
GENEVA
HONG KONG
HOUSTON
KUALA LUMPUR
LONDON
NEW YORK
ORLANDO
PARIS
SINGAPORE
TORONTO
VIENNA
WASHINGTON D.C.
ZURICH

CAPCO.COM