VERIFI™

The Blurring of CP and CNP:

Remaining Secure & Scalable in a Technology and Regulation Driven Landscape

VERIFI WHITEPAPER

VERIFI™

The Blurring of CP and CNP:

Remaining Secure & Scalable in a Technology and Regulation Driven Landscape

All online merchants are targets to become the “supply-side” for counterfeit card and other types of fraud at brick-and-mortar locations.[1]

Between the rising popularity of NFC, the upcoming EMV liability shift and boost in mobile sales, and the advent of biometrics in mobile devices, the lines of card present and card-not-present continue to blur. These forces create additional sales opportunities for merchants who can quickly adapt to rapidly changing buyer behaviors and preferences.

There is a convergence on the fraud side as well. Data breaches and the fraudsters that perpetrate them do not discriminate between retail giants and smaller merchants – all online merchants are targets to become the “supply-side” for counterfeit cards and other types of fraud at brick-and-mortar locations.[1] So while EMV will all but eliminate counterfeit card production at EMV enabled merchants, there are still holes in security that will require additional tools and safeguards.

As NFC takes hold in the marketplace and merchants are guided by regulations and evolving industry standards like EMV, the lines of CP and CNP commerce are blurring and new needs are emerging when it comes to security and fraud prevention. Now is the ideal time for online merchants of all sizes to re-evaluate their current processing capabilities to see if they are effective and agile enough to keep pace with the changing landscape. The best way to shut down fraudsters and protect merchants across all channels will be implementing a comprehensive, layered fraud prevention strategy that utilizes tokenization, P2PE and various other fraud prevention tools that are customized for each merchant’s needs.

Goldman Sachs forecasts mobile commerce to account for almost half of all ecommerce by 2018

Current Mobile Landscape & the Blurring of CP and CNP

Experts predict 2015 will be the breakout year for mobile payments. Many merchants are beginning to integrate mobile into an overall retail shopping experience and some are optimizing mobile to meet the growing demands of the Omni-channel driven consumer. Goldman Sachs forecasts mobile commerce to account for almost half of all ecommerce by 2018, with roughly 525 million consumers making a purchase via mobile this year.[2] Global ecommerce (B2C) sales could top $1.7 trillion with mobile commerce accounting for about $300 billion of that.[3]

The line between what is considered a card-present and card-not-present transaction has already started to blur, thanks to mobile. As mobile transactions become as, or more, secure than card-present transactions, this may lead to a change in their interchange treatment.

The biggest drivers of change in mobile for 2015 will be the use of NFC as the de facto method to make mobile payments as well as EMV and its impact on merchant terminals. Merchants are in the process of installing terminals to enable EMV and a majority of these are NFC-capable. The Aite Group points out that most merchant terminals will be able to accept NFC transactions in the next one to three years.[4]

Near-Field Communication (NFC) Technology – How it works

NFC transactions occur when a cardholder initiates the transaction from an NFC-enabled mobile device in close proximity to a contactless POS terminal. Because of the intrinsic security elements of NFC, it is ideal for financial transactions. This includes a secure element (that can reside in a Universal Integrated Circuit, an embedded secure smart card chip on the handset or on the Subscriber Identity Module [SIM]) in which cryptographic keys related to card credentials are stored.[5]

Some recent applications involving NFC allow card credentials to be stored in the cloud and accessed via proxy credentials on the secure element. A third-party trusted service manager (TSM) – which allows providers engage with NFC wallet technology without sharing customer data – distributes card credentials to an NFC wallet within the mobile device.[6] These mobile wallets are not unlike physical wallets – they allow for consumers to add, store and access multiple cards, which can be accessed via a digital wallet application.[7]

In addition to being secure and reliable, NFC is – or will be – more mainstream. Many merchants are upgrading to hybrid contact and contactless POS terminals in preparation for the EMV migration.[8]

The propagation of this technology by both consumer preference and regulatory forces creates opportunities for merchants to drive increased sales through additional channels and targeted marketing efforts aided by the technology that includes couponing and special offers. NFC provides a fast and easy way for consumers to pay along with a myriad of other benefits (tracking baggage, turning WiFi on, checking-in for a flight, etc.) and enables merchants to benefits from the data and insights resulting from these capabilities. While many of these capabilities are not yet developed at scale, it signals the possibilities to come as NFC gains a foothold (for merchants who are equipped to harness this technology).[9]

On the other side of the token, the technology and regulatory standards bring added stress for merchants who may struggle to stay abreast of security changes and shifting fraud trends as the landscape evolves.

NFC Impact on Payments Landscape

There used to be a distinct line between CP and CNP payments. CP or offline payments included face-to-face transactions where a consumer would swipe their credit card to make a purchase and CNP or online purchases entailed typing in your credit card details on a computer. NFC and mobile wallets are a large contributor to the blurring – and perhaps disappearance – of this line. Payments made using mobile wallets fall under a third category called "cardholder present" and are awarded lower interchange fees[10] by MasterCard and Visa. This is to designate that these payments have considerably more security features in place than your typical CNP transaction and the rate is contingent on mobile wallet integration with biometric sensors (like Apple iPhone's Touch ID).[11] The rate difference can add up – CP rates average 1.5% of the purchase price while CNP rates average 2.75%.[12] Further illustrating the level of security afforded by technology like Apple Pay, banks actually agreed to consider Apple Pay transactions as CP and reduced the CP rate by 15 to 25 basis points due to the lower risk of fraud.[13]

As mentioned earlier, a lot of the bustle surrounding NFC technology and mobile wallet providers is tightly coupled with the EMV migration. Pricing rules may evolve if the current "chip and signature" rate is increased and MasterCard and Visa create this new category of transaction fee known as "cardholder present."[14]

EMV, NFC and Implications

So far, it looks like the migration to EMV will be matched by a migration to a contactless world. While mobile wallet volume will increase, it will be additive to the existing forms of payment, which will not go away. However, the majority of large retailers already carry NFC-compatible terminals and many more retailers will jump on board as they upgrade terminals to comply with EMV standards. The timeline for merchants who have not yet adopted NFC-capable terminals but plan to is within the next one to three years.[15]

As illustrated by the evolving transaction rates that brands are considering, it's evident that the security features of NFC rival – or even exceed – that of CP transactions. Mag-stripe cards currently fall prey to skimming, cloning and theft, while mobile wallets like Apple pay utilize biometrics like Touch ID for authentication and encrypt payment card data.[16] This security paired with widespread availability (almost 90% of smartphones shipped worldwide will be NFC-enabled moving forward)[17] has created a ubiquitous method for the exchange of data between POS terminals and mobile devices.

The prevalence of this technology and the related EMV migration will push fraud online at a rapid rate. Merchants that do not implement EMV standards by the liability shift along with those that offer gift cards, jewelry, technology or anything that can be easily monetized will be especially at risk.

Security Implications – What is a safe purchase?

The bottom line is that the commerce landscape is rapidly changing. With technology and industry regulations as catalysts, the distinction between CP and CNP transactions have blurred. Furthermore, fraud is shifting to the online channel, placing a renewed emphasis on transaction security as well as scalable solutions that can maintain pace with the dynamic requirements.

Blurring of the CP/CNP line has only accelerated with the emergence of new technologies such as near-field communication (NFC), mobile wallets, and other alternative payments.

Two-factor authentication is an important consideration when it comes to security implications as they related to NFC and mobile wallets. NFC can be considered superior to using a card for authentication because of the two-factor authentication element (x and biometrics through Touch ID). This is a stronger form of authentication than simply a signature. When paired with sophisticated fraud tools like IP geolocation, digital fingerprinting and risk profiles, the risk between selling online and in the "real world" is greatly diminished.[18]

It's important now more than ever that merchants employ payment-processing gateways with technology – and the agility – to handle the blurring of CP and CNP while effectively mitigating risk. This may include the capability to assess risk using factors as whether a fraud screen is used by the device, the location of transaction initiation and other elements, rather than by whether or not a card is present alone.[19]

Merchant Obstacles

There are a number of threats that merchants face given the changing circumstances and there are significant obstacles that stand in the way of merchants and safe, secure payment processing.

BRAND DAMAGE

Rising fraud can pose a significant threat to a merchant's good name. Data breaches have shown us that non-secure processing can critically damage your brand and your bottom line. Research shows that consumers avoid retailers who have the perception of inappropriate security measures or retailers who have been breached.

AGILITY TO PIVOT WITH NEW TECHNOLOGY

Omni-channel continues to gain steam, presenting increased sales opportunities as well as increased fraud. Optimizing and protecting multiple channels requires real-time insight and comprehensive reporting to reap the full benefits and profits and to full protect payments from end to end.

LIMITED IT SUPPORT

Updating legacy systems is expensive and drains staff and time. Most merchants are working with already stretched-thin (or nonexistent) IT departments that simply cannot take on another project. Managing transaction security and fraud prevention in-house can pose a significant burden to many merchants.

SCALABILITY AND FLEXIBILITY TO SUPPORT CHANGE AND BUSINESS GROWTH

Merchants with limited or inflexible processing systems experience bottlenecks, decreased efficiency, increased cost, more friction and an overall lowered customers experience.

How Verifi can help

Working with an outside vendor can save significant time, money and resources, especially merchants with limited IT resources…As the shifting landscape continues to evolve, new threats will emerge and security needs will become more complex. Now is the ideal time for merchants to reevaluate their processing operations to ensure they are not only robust enough but agile enough to evolve as technology and regulatory impacts come into play.

PROBLEM: End-to-end security facilitated by P2PE and Tokenization is critical to protect sensitive consumer data and brand reputation.

SOLUTION: Safe and secure processing environment to reduce the cost of compliance. Verifi's Global Super Gateway protects your sensitive data via safely storing customers' credit card and personal information and returning a "token" back to you for future processing needs so you don't have to worry about data breaches damaging your brand and helps to reduce PCI exposure.

PROBLEM: Deep, unified insights into consumer purchasing behavior is necessary not only to combat fraud, but to maximize profitability and as payments technology evolves.

SOLUTION: Deep analytics with a global view of your business priorities. Maintain line-of-sight into recent changes to business priorities through our in-depth performance, risk, profitability and chargeback analysis and reporting - all powerful, unique data available in a unified view and in real time. Develop custom strategies to maximize profitability and address the shifting economics of the business, better prepare for upcoming events and monitor and reduce risks.

PROBLEM: Evolving landscape and dynamic fraudsters creates unique fraud vulnerabilities for merchants, many of whom do not have the IT resources for numerous integrations and re-integrations.

SOLUTION: Comprehensive, layered fraud protection across the entire transaction lifecycle. Our end-to-end payments protection suite tightly couples the Global Super Gateway, Intelligence Suite and chargeback prevention and recovery services. so you can protect your revenue streams and process payments more securely and seamlessly:

- The proprietary rules engine gives you the ability to centralize and easily accept or decline transactions with pre-set business or custom rules and test and toggle the rules based on feedback.
- Minimize your risk through ONE integration. Layer and modify your fraud prevention strategy seamlessly to minimize risks, without adding IT costs or turning away good sales.
- Intelligence® Suite provides a comprehensive fraud management platform that enables you to cost-effectively layer, test and adapt this suite of best-of-breed tools as the marketplace – and fraudsters – evolve.
- Cardholder Dispute Resolution Network™ (CDRN) stops up to 40% or more of chargebacks through direct integration with banks and issuers, eliminating the middle men and putting you back in control.
- Chargeback Revenue Recovery (CBR) recovers up to 50% or more of unavoidable chargebacks, enabling merchants to focus their time, resources and effort on what matters – building their business and boosting profits.

PROBLEM: Static, fragmented and expensive payment processing solutions create bottlenecks and increased friction for customers, hindering the ability to grow the business.

SOLUTION: Verifi's Global "Super Gateway" is processor agnostic with the flexibility to manage both current and future needs. The Super Gateway supports over 65 major domestic and international acquirer and processing networks, and gives you the freedom to process your payments in the best manner for your business, minimizing your costs and remaining flexible and scalable as your business grows. Verifi's comprehensive platform provides broad, layered fraud protection that can be easily refined to let more successful and legitimate sales pass through without increased risk.

The End Game

As drivers like NFC and EMV continue to blur the lines between CP and CNP transactions and security becomes the spotlight focus, merchants should evaluate their current solutions and their ability to adapt to the changing needs as well as changing consumer behaviors. This year will separate the forward-looking merchants from those that will need to play catch-up in terms of security, Omni-channel and the ability to weather the perfect storm created by NFC, EMV and the evolving payments landscape…but by then, it may be too late.

Glossary of Terms

NEAR-FIELD COMMUNICATION (NFC) - Near Field Communication (NFC) technology enables devices in close proximity (within 4 centimeters) to communicate. NFC-enabled devices are highly secure and utilize XYZ technology, which is why mobile proximity payments like Apple Pay garner a card-present interchange rate. NFC is not relegated to payment applications; however, its high level of security makes it ideal for this use. NFC payments are utilized by all types of payment card issuers, including network-branded (open loop) and non-network-branded (closed loop).[20]

EMV - stands for Europay, MasterCard and Visa, a global standard for inter-operation of integrated circuit cards (IC cards or "chip cards") and IC card capable point of sale (POS) terminals and automated teller machines (ATMs), for authenticating credit and debit card transactions.

It is a joint effort initially conceived among Europay, MasterCard and Visa to ensure the security and global interoperability of chip-based payment cards.[21]

CARD-PRESENT (CP) – Represents transactions where the card and cardholder are present during payment processing, typically in a brick-and-mortar store.

CARD-NOT-PRESENT (CNP) – Represents transactions where the cardholder does or cannot present the actual card for face-to-face examination by a merchant during payment processing (e.g. mail-order transactions by mail or fax, telephone orders or orders completed over the Internet).

About Verifi

Verifi, an award-winning provider of end-to-end payment protection and management solutions, was founded in 2005 to help our clients effectively manage the payments challenges they face everyday. Verifi helps merchants safely process payments, combat fraud, prevent and resolve costly chargebacks, as well as increase billings and keep loyal customers. Our best-in-breed solutions and white glove support are trusted by a wide range of industries from emerging companies to the Fortune 500. Headquartered in Los Angeles, California, we process more than $20 billion transactions annually and currently serve more than 5500 accounts internationally.

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 http://cardnotpresent.com/email/predictions.htm

2 https://www.internetretailer.com/2014/03/10/mobile-commerce-will-be-nearly-half-e-commerce-2018

3 http://www.cio.com/article/2866080/e-commerce/how-ecommerce-businesses-can-beat-the-competition-in-2015.html

4 20150113-Top-10-Trends-in-RB-2015-NOTE-pdf_6713_18213_10125_10860.pdf

5 http://www.smartcardalliance.org/resources/pdf/Payments_Landscape_WP-111413.pdf

6 http://www.smartcardalliance.org/resources/pdf/Payments_Landscape_WP-111413.pdf

7 http://www.smartcardalliance.org/resources/pdf/Payments_Landscape_WP-111413.pdf

8 http://www.smartcardalliance.org/resources/pdf/Payments_Landscape_WP-111413.pdf

9 http://www.smartcardalliance.org/resources/pdf/Payments_Landscape_WP-111413.pdf

10 http://bankinnovation.net/2014/09/visa-mastercard-in-talks-with-mobile-wallets-for-cardholder-present-rate/

11 http://bankinnovation.net/2014/09/visa-mastercard-in-talks-with-mobile-wallets-for-cardholder-present-rate/

12 http://bankinnovation.net/2014/09/visa-mastercard-in-talks-with-mobile-wallets-for-cardholder-present-rate/

13 http://bankinnovation.net/2014/09/visa-mastercard-in-talks-with-mobile-wallets-for-cardholder-present-rate/

14 http://bankinnovation.net/2014/09/visa-mastercard-in-talks-with-mobile-wallets-for-cardholder-present-rate/

15 20150113-Top-10-Trends-in-RB-2015-NOTE-pdf_6713_18213_10125_10860.pdf

16 http://www.businessinsider.com/what-you-need-to-know-about-apples-new-payments-system-2014-9#ixzz3O9S5mZ7K

17 http://www.businessinsider.com/what-you-need-to-know-about-apples-new-payments-system-2014-9#ixzz3O9S5mZ7K

18 http://digitaltransactions.net/news/story/E-Commerce_-Just-What-Does-Card-Present-Mean-These-Days_

19 http://digitaltransactions.net/news/story/E-Commerce_-Just-What-Does-Card-Present-Mean-These-Days_

20 http://www.smartcardalliance.org/resources/pdf/Payments_Landscape_WP-111413.pdf

21 http://en.wikipedia.org/wiki/EMV