FEDERAL RESERVE BANK OF BOSTON™

Payment Strategies

Mitigating Fraud Risk in the Card-Not-Present[1] Environment

February 12, 2016

By Susan Pandy, Director, Payment Strategies

I. Introduction

The Federal Reserve Banks of Boston and Atlanta convened a meeting of the Mobile Payments Industry Workgroup (MPIW) in November 2015 to discuss payments in the card-not-present (CNP) environment. Not only are consumers increasingly using mobile devices to initiate CNP payments; but the e-commerce fraud rate in the U.S. is expected to increase significantly as EMV[2] chip card migration progresses. Based on these two trends, the MPIW focused on: (1) differences between e-commerce and m-commerce;[3] (2) vulnerabilities and fraud associated with CNP transactions; and (3) fraud and risk management solutions to combat CNP fraud.[4]

As background, CNP fraud accounts for 25 percent of global fraud losses,[5] and CNP fraud represents 45 percent of total U.S. card fraud.[6] Several developed countries experienced significant spikes in CNP fraud post-EMV migration, e.g., Australia, Canada, France, and the UK.[7] The U.S. can learn from the experiences of other countries to start developing options to mitigate CNP fraud now, particularly with the rapid growth of online and m-commerce.

All industry stakeholders share in the responsibility to mitigate CNP fraud, and merchants are particularly vulnerable, as they pay higher costs for fraud. According to a LexisNexis 2014 study, every dollar lost to fraud in 2014 cost merchants $2.79, but every dollar lost to *online* fraud cost $3.10.[8] CNP fraud, whether

---

[1] Card not present (CNP) is a payment made for a purchase using a credit or debit card, where the cardholder/card are not physically present to allow the merchant to validate the cardholder at time of purchase, such as payments made by mail, over the phone, or internet. Source: EMV Migration Forum (2015, April). Card-Not-Present Fraud Working Committee White Paper: *Near-term solutions to address the growing threat of card-not-present fraud. Version 1.0.* Retrieved from http://www.emv-connection.com/wp-content/uploads/2015/04/CNP-Solutions-White-Paper-FINAL.pdf.

[2] EMV (Europay, MasterCard and Visa) is a global specification for credit and debit payment cards based on chip card technology that defines requirements to ensure interoperability between chip-based payment cards and terminals. The primary use for these chip-based cards is to perform payment transactions. The encrypted dynamic data supplied by the chip provides a higher level of protection against counterfeiting than magnetic striped cards. For more information, see http://www.emvco.com.

[3] E-commerce represents the buying and selling of goods and services over an electronic network, primarily the internet. M-commerce is a subset of e-commerce for purchases made using a wireless hand-held device, typically a mobile phone.

[4] CNP fraud involves the unauthorized use of a credit or debit card number, CVV code, and the cardholder's address details to purchase products or services either online, through a call center, on a mobile device or by mail order.

[5] Copper River Group (2015, Aug. 17). *EMV and payment card fraud: The impact of EMV on fraud trends*. Retrieved from http://www.copperrivergroup.com/cms20/CuteSoft_Client/CuteEditor/Dialogs/EMV-Payment-Card-Fraud_Research-Report_08-2015.pdf.

[6] Aite (2014, June). *Card-not-present fraud in a post-EMV environment: Combating the fraud spike*. Sponsored by RSA. Retrieved from https://www.emc.com/collateral/white-papers/card-not-present-fraud-post-emv-env-wp.pdf.

[7] For more information about post-EMV fraud in other countries, see the following: (1) King, D. (2012, Jan.). *Chip and PIN: Success and challenges in reducing fraud*. Federal Reserve Bank of Atlanta, Retail Payments Risk Forum. (2) Canadian Bankers Association (2015, July 13). *Payments security white paper*. Retrieved from http://www.cba.ca/contents/files/submissions/misc-2015-paymentssecurity-whitepaper-en.pdf. (3) Smart Card Alliance (2014, Feb.). *Card-not-present fraud: A primer on trends and authentication processes*. Retrieved from http://www.smartcardalliance.org/resources/pdf/CNP-WP-012414.pdf.

[8] LexisNexis (2014, Aug.). *2014 LexisNexis true cost of fraud study*. Retrieved from http://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf.

initiated from online or mobile attacks, grew 20 percent from Q1 to Q2 2015.[9] Merchants can benefit from assessing their existing solutions as well as emerging tools in order to enhance their fraud prevention capabilities.

II. Risks in the Mobile and E-commerce Environments

The U.S. Census Bureau reported that e-commerce accounted for 7.4 percent of total U.S. sales in 3Q 2015.[10] According to Internet Retailer's *2016 Mobile 500*,[11] m-commerce accounts for nearly one-third of all U.S. e-commerce sales, and as m-commerce continues to grow, fraudsters will target this channel.

A. Distinguishing between e-commerce and m-commerce

While there are obvious connections between the e-commerce and m-commerce channels, approaches and tools for fraud prevention will differ. For several reasons, the m-commerce channel is experiencing lower fraud than the e-commerce channel.

First, the volume of transactions made via m-commerce is much lower than total e-commerce volume. As of Q3 2015, m-commerce dollar sales reached a 16.4 percent share of total e-commerce dollar sales.[12] This may suggest that the market is in the midst of an inflection point in its long-term development.

Second, the m-commerce channel requires consumers to enroll in a payment service that creates an account, which is commonly done via a mobile app. With mobile apps, merchants and processors have more visibility into the user's profile and transaction history based on the registration and characteristics about the mobile device. On the other hand, customer access to the e-commerce channel is less dependent on registration services and does not match in the amount of data available through a mobile device, leaving e-merchants with less information to help validate the buyer.

Third, some industry experts consider it more difficult for fraud to scale in the m-commerce channel. Because the e-commerce environment is browser-based and ubiquitous, it is fairly straightforward. The mobile channel utilizes multiple handsets, operating systems, wireless networks, mobile apps, and a mobile browser, which makes large-scale fraud more complex. Despite this complexity, m-commerce is still at risk from mobile malware, fraudulent mobile apps, digital wallet fraud, and account takeover (ATO).[13] ATO is when fraudsters use stolen credentials harvested from data breaches and stolen identities to create new accounts.[14]

It is important for merchants to track fraud for all channels. According to a 2015 Kount study, less than 40 percent of merchants differentiate or track fraud losses between the mobile and standard e-commerce channels and 61 percent of all organizations have no idea whether mobile fraud is growing faster or slower

---

[9] Correa, D. (2015, Nov. 20). CNP and ATF fraud grew at alarming rates in Q1 and Q2 2015, *SC Magazine*. Retrieved from http://www.scmagazine.com/cnp-and-atf-fraud-grew-at-alarming-rates-in-q1-and-q2-2015/article/455410/.
[10] See https://ycharts.com/indicators/e-commerce_sales_as_percent_retail_sales.
[11] Available for purchase at https://www.internetretailer.com/mobile500/#!/.
[12] comScore (2015, Dec. 1). *State of the U.S. online retail economy in Q3*. [Presentation]. Retrieved from https://www.comscore.com/Insights/Presentations-and-Whitepapers/2015/State-of-the-US-Online-Retail-Economy-in-Q3-2015.
[13] J. Gold Associates (2015, Feb.). *Mobile e-commerce friend or foe? A cybersecurity study*. Retrieved from https://www.comscore.com/Insights/Presentations-and-Whitepapers/2015/State-of-the-US-Online-Retail-Economy-in-Q3-2015. http://www.emc.com/collateral/analyst-reports/h13939-mobile-e-commerce-friend-or-foe.pdf.
[14] ThreatMetrix (2015). *ThreatMetrix cybercrime report Q2 2015*. Available for download at https://www.threatmetrix.com/threatmetrix-labs/fraudfacts/.

than their mobile transaction volume.[15] Therefore, merchants should distinguish between fraud trends identified in their online and mobile channels to gain a better understanding of how and where fraud is evolving. Merchants with at least $50 million in annual revenues are more likely to track fraud attempts and losses by channel than smaller merchants. However, smaller merchants can develop in-house approaches to tracking fraud or leverage third-party service providers.

B. CNP fraud vulnerabilities raised by security experts

Customer account opening/creation

This is becoming the new big fraud risk. It will be important to secure the account opening process and prevent ATO fraud. Leveraging the multiple functionalities of the mobile device (unique device identification, geolocation, biometrics, etc.) and examining mobile device patterns and usage can help to address this risk. Implementing KYC[16] is also critical in the CNP user account opening process. Companies should build and maintain customer profiles to help understand instances of ATO by using rules, machine learning,[17] and pattern identification.

Data breaches

This continues to be a major risk, but fraudsters are shifting from getting payment card (i.e., PAN) data to stealing personally identifiable information (PII, or identity information), e.g., SSN, and finding ways to monetize that data. Security solution providers are trying to determine how they can obtain the data they need to prevent this type of breach from occurring.

Small e-commerce merchants

Small e-commerce merchants (with less than $100 million in sales) are at greater risk of CNP fraud. These merchants lack the resources to build risk management systems used by larger e-commerce merchants. Furthermore, because small merchants do not consider fraud prevention part of their core business, they may not understand or invest in the best security solutions to protect their business. These merchants tend to treat risk management similar to other business software needs and either buy solutions off the shelf or outsource to third party providers. Security solution providers should recognize the needs of the small e-merchants and develop targeted and affordable solutions to support them.

Access to CNP fraud data

Shared access to CNP fraud data is difficult. While stakeholders would be able to make better authentication and payment decisions if they had more fraud data; legal, policy, and privacy restrictions prevent broad data-sharing. Current issues include how and what fraud data is shared, who has access to the data, and limited

---

[15] Kount (2015). *Mobile payments & fraud: 2015 report*. Available for download at http://info.kount.com/mobile-payments-reports-2015.

[16] Know your customer (KYC) is the process of a business verifying the identity of its customers.

[17] Machine learning is a method of data analysis that automates analytical model building. Using algorithms that iteratively learn from data, machine learning allows computers to find hidden insights without being explicitly programmed where to look. As models are exposed to new data, they are able to independently adapt. They learn from previous computations to produce reliable, repeatable decisions and results and turn background knowledge and examples (input) into knowledge (output).

collaboration. The payments industry should look for ways to break down these barriers to allow more CNP fraud data to be shared across stakeholders.

III. CNP Fraud /Risk Management Solutions

A. Authentication

Authentication is being used as an end-to-end risk management tool to validate every step in the transaction process. It begins at registration, rather than at the point of transaction. It is being applied in ways that help to assess perceived risk versus acceptable risk. Therefore, the less comfortable a merchant or issuer feels about the transaction, the more willing it should be to inconvenience the customer to prevent fraud, and ensure that the authentication tools applied match the level of transaction risk. However, authentication can negatively impact the customer experience when too many methods are used. For example, knowledge-based authentication (KBA) (i.e., challenge questions) is often used as an added layer of authentication. If the user cannot recall the answer to his challenge questions, it creates a negative consumer experience that may result in shopping cart abandonment. Balancing the trade-offs, authentication tools should be combined or coordinated to minimize customer friction, so that the 99 percent of transactions that are good move quickly, while only the small percentage that are fraudulent are impacted.

Authentication verifies the identity of a user who wants to login to an account, and ensures that the user is authorized to access that account. Authentication solutions may be layered, and start with username and password, adding other elements such as mobile phone number, email address, billing or shipping address, out-of-band authentication (OOBA), KBA, one-time passwords (OTPs), biometrics, address verification services (AVS), cardholder verification (CVV/CVN), etc. Other information such as IP address, geolocation, and device fingerprint may be collected during the process to (1) increase confidence in the transaction, (2) identify and isolate suspect transactions, and (3) determine the validity of the customer who initiates the transaction.

B. 3 Domain Secure (3DS)

3-D Secure (3DS)[18] authentication verifies the cardholder and the account to the merchant/acquirer, issuer and network. It enables issuers to authenticate cardholders during an online purchase to reduce fraudulent use of payment cards. The merchant, cardholder, and card issuer all must participate in this authentication process.

3DS 1.0 was originally developed to support the growth of e-commerce as a tool that would make online transactions more secure by removing the need for the user to enter his payment credentials directly on a merchant website. 3DS 1.0 was not user-friendly. It required consumers to enroll with a password, and interrupted 100% of the online transactions with additional authentication checks, creating a negative consumer shopping experience. This resulted in higher levels of customer abandonment during checkout, which led to low merchant adoption of 3DS in the U.S., where it was not mandated.[19]

[18] 3 Domain Secure (3DS) is an XML protocol designed to add an additional layer of authentication to CNP online transactions, supported by Visa as Verified by Visa, MasterCard SecureCode and American Express SafeKey.

[19] In 2013, only about 3 percent of U.S. merchants were using 3DS and currently, adoption is around 10 percent.[19] U.S. Congressional Research Service (n.d.). *The EMV chip card transition: Background, status, and issues for Congress.* Retrieved from https://www.fas.org/sgp/crs/misc/R43925.pdf.

With changes to how consumers pay online (e.g., mobile) and availability of other security tools such as payment tokenization, the card networks looked at the overall shopping experience and tasked EMVCo[20] to develop a risk-based version (3DS 2.0) that would reduce friction. 3DS 2.0 is currently in development.[21]

There are several benefits to using 3DS. It not only reduces fraudulent transactions, it also shifts the fraud liability from the merchant to the issuer, whether or not the issuer supports the 3DS request through risk assessment and stepped-up authentication prompts. 3DS 2.0 introduces other changes intended to increase merchant acceptance, improve the cardholder experience, and make the solution more effective:

(1) Applies risk-based authentication to validate the transaction. Because 3DS 2.0 is risk-based, it will be less intrusive to most customers; only interrupting transactions considered high-risk for stepped-up authentication.
(2) Uses dynamic data authentication, shifting away from static passwords.
(3) Gives merchants more control over when and where they want to invoke 3DS. Merchants will be able to decide whether to reject a transaction or to require further authentication of the consumer before approving the payment, even if the issuer has already accepted the transaction.
(4) Eliminates the need for cardholders to actively enroll to be eligible for 3DS.[22]

IV. Conclusion

The payments industry recognizes the potential for increased fraud in the mobile/digital channels and CNP environment. Stakeholders are beginning to evaluate and implement a range of available fraud prevention solutions to help develop a course of action. The industry has an opportunity to leverage existing fraud prevention tools, adopt emerging technologies, and learn from past experience in order to minimize the expansion and impact of CNP fraud, particularly as fraud moves to the mobile channel.

A summary of key industry considerations include: (1) Authentication continues to evolve. Some existing tools, such as challenge questions or passwords, are becoming outdated, and fraudsters continue to find new ways to break security tools. (2) It is important to focus on the money movement and adjust fraud solutions, so industry stakeholders need multiple tools in their risk management/fraud tool box to achieve this. (3) Finally, it is important to recognize that the human factor is still important despite advancements in fraud prevention and detection technologies.

Given these considerations, industry collaboration is required on several fronts: consumer/industry education; fraud information sharing; and potential partnerships in development of solutions for CNP payment transactions. For example, merchants may want to consider partnering with a third party service provider that can bundle various fraud solutions together into a single point of integration (i.e., software development kit) rather than managing multiple services and solutions. Industry collaboration can make both e-commerce and m-commerce more secure and create a better user experience for the consumer.

The MPIW will continue to monitor trends and developments in CNP fraud and conduct research to share with the industry in 2016.

---

[20] EMVCo LLC is a consortium that manages the EMV standard for chip and tokenization specifications. It is jointly owned by American Express, Discover, Visa, MasterCard, JCB, and Union Pay.
[21] For more information, see https://www.emvco.com/.
[22] Aite (2014, June). *Card-not-present fraud in a post-EMV environment: Combating the fraud spike*. Sponsored by RSA. Retrieved from https://www.emc.com/collateral/white-papers/card-not-present-fraud-post-emv-env-wp.pdf.