FEDERAL RESERVE
BANK OF BOSTON™

BRIEF

Understanding the U.S. Card-not-Present (CNP)[1] Fraud Landscape and Identifying Key CNP Fraud Mitigation Tools and Strategies

December 11, 2017 (Revised February 8, 2018)

By Susan Pandy, Ph.D., Director, Payment Strategies

The U.S. migration to EMV[2] chip cards for the card present (CP) environment (i.e., retail point-of-sale) has shifted the focus of fraud to the CNP channel. Several other developed countries experienced increases in CNP fraud following their EMV card implementations. The 2016 Federal Reserve Payments Study[3] reported that U.S. CNP fraud totaled $1.6 billion in 2012. Industry resources now estimate that U.S. CNP fraud represents approximately 50 percent of total fraud losses sustained.[4]

Consumers are buying more goods online with their computers, tablets, and mobile devices, creating more opportunities for fraud.[5] Increases in CNP fraud can also have significant consequences for businesses of all sizes, which requires the need to be prepared with the proper fraud mitigation tools and strategies. Accordingly, the Accredited Standards Committee (ASC) X9[6] Retail Payments Subcommittee[7] drafted a Technical Report (TR): *Card-Not-Present (CNP) Fraud Mitigation in the United States: Strategies for Preventing, Detecting, and Responding to a Growing Threat* (X9 CNP Fraud TR), to educate industry stakeholders on the risks presented by criminal activity and how to more effectively prevent, detect, and manage CNP fraud. This report provides a brief explanation of X9 and the importance of technical standards for financial services, and then describes key elements included in the X9 CNP Fraud TR.

[1] Card-not-present: A purchase made with a payment card, where the cardholder/card is not physically present to allow the merchant to validate the cardholder at the time of purchase (e.g., by U.S. postal mail, telephone, internet, or mobile)

[2] Europay, Mastercard, Visa.

[3] U.S. Federal Reserve Board of Governors. (2016). *Federal Reserve payments study 2016*. Retrieved from https://www.federalreserve.gov/paymentsystems/2016-payment-study.htm.

[4] Aite (2014, June). *Card-not-present fraud in a Post-EMV environment: Combating the fraud spike*. Retrieved from https://www.emc.com/collateral/white-papers/card-not-present-fraud-post-emv-env-wp.pdf. As of 2014, U.S. CNP Fraud was 45 percent. See also Nilson (2016, Oct). *Card fraud losses reach $21.94 billion*. The Nilson Report, Issue 1096. Retrieved from https://www.nilsonreport.com/upload/content_promo/The_Nilson_Report_10-17-2016.pdf.

[5] U.S. online retail sales nearly quadrupled between 2005 and 2015, and in 2016 accounted for $394.9 Billion and 8.1 percent of total retail sales. U.S. Census Bureau (2017, Feb. 17) *Quarterly Retail E-Commerce Sales 4th Quarter 2016*. Retrieved from https://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf and comScore (2017, Feb.) *M-Commerce data*. In 4Q 2016, mobile commerce spending was 21 percent of total e-commerce retail sales. Retrieved from http://www.comscore.com/Insights/Press-Releases/2017/2/comScore-Reports-109-Billion-in-Q4-2016-Total-Digital-US-Retail-E-Commerce-Spending-Up-18-Percent-vs-Year-Ago?

[6] For more information, see https://x9.org.

[7] The X9A Retail Payments Subcommittee develops and supports standards focused on retail card and mobile-based payments affecting consumers, including electronic benefits. Presently, ASC X9 operates five technical subcommittees and 20-30 technical working groups that develop financial industry technical standards and guidelines.

The views expressed in this paper are those of the author and do not necessarily represent those of the Federal Reserve Bank of Boston or the Federal Reserve System. Mention or display of a trademark, proprietary product, or firm in this paper does not constitute an endorsement or criticism by the Federal Reserve Bank of Boston or the Federal Reserve System and does not imply approval to the exclusion of other suitable products or firms

Understanding Accredited Standards Committee (ASC) X9 and the Value of Standards

ASC X9 leads efforts to develop and promote the open consensus technical financial industry standards needed to act efficiently and competitively in the marketplace.[8] These technical standards are widely recognized and used in the U.S. in financial procedures and transactions. Although X9's primary focus is national standards, X9 standards are adopted in countries around the globe.[9]

Standards make a significant contribution to the financial services industry. For example, standards determine the size of a paper check, create protocols for transaction messaging, electronic security systems, paperless contracts, and more. Standards are designed to simplify existing processes and support interoperability. The lack of standards or their misapplication makes their value more apparent. For example, when transactions or payment-related technology results in negative consumer or stakeholder experiences, the standards community may intervene to help enhance the reliability, efficiency, and interoperability.

X9 promotes an open consensus development process, where members can directly influence the development of technical standards by participating in its formulating groups. In addition to standards, X9 also develops Technical Reports (TRs), which are intended to provide education and industry best practices. Because CNP transactions can be initiated from multiple payment channels, flexibility is needed to apply best practices or recommendations to different environments, which is best supported by a TR. Therefore, the goal of the X9 CNP Fraud TR is to educate the payments industry about the existing threat environment and available strategies, tools, and approaches for mitigating fraud, and provide recommendations to key industry stakeholders to help prevent anticipated increases in CNP fraud.

CNP Fraud and Relevant Mitigation Tools and Strategies

Technical Reports establish consensus-driven definitions that support the document, as well as a framework for delivering the content. The X9 CNP Fraud TR framework maps the "lifecycle" of CNP fraud, which begins with the theft of data, followed by fraudulent testing of that data, the fraudulent purchase of goods, and then monetization of those stolen goods. The TR outlines the primary types of attacks used to steal data and commit fraud and focuses on how key industry stakeholders – merchants, merchant acquirers and payment gateways, issuers and issuer processors, and payment card networks –can develop strategies, tools, and approaches to mitigate CNP fraud.

Merchants tend to be more affected by fraud (losses, customer problems, etc.), which makes it critical for them to understand: (1) the broad range of available fraud solutions; (2) fraud tools used by their peers; (3) primary types of CNP fraud attacks; and (4) how to structure their organizations to strategically address CNP fraud across all channels (e.g., e-commerce, mobile, telephone and mail order, call center, etc.). CNP merchants need to ensure that their CNP channels are adequately protected from increasingly sophisticated criminal attacks.

[8] ASC X9 operates under its own procedures as well as those prescribed and approved by the American National Standards Institute (ANSI). Because X9 standards carry the ANSI designation, it shows they are in accord with ANSI rules and specifications for standards development and management. ANSI does not develop standards, rather accredits industry bodies like X9 to do so and calls such bodies accredited standards developers or ASDs.

[9] ASC X9 also holds the U.S. vote on all International Standards Organization (ISO) standards of TC 68 or its subcommittees; therefore, X9 participates in the develop of many international standards used in facilitating global commerce.

Primary Types of CNP Fraud Attacks

The X9 CNP Fraud TR focuses on how stolen credentials are used in certain types of CNP attacks. This section of the report highlights the primary attacks described in the TR: botnet and scripted attacks; identity testing or velocity attacks; account takeover (ATO) attacks; and new account or application fraud.

Botnet attacks. A basic bot[10] attack can perform velocity-based function and account validation attacks (as described in the next section). Complex botnet attacks use more advanced methods to spoof IP addresses, emulate browsers, or spoof applications. Bots pretend to be legitimate traffic by masking their true context. These types of attacks are often directed toward large and well-known retailers. Digital goods, given the immediacy of the transaction, are often prime targets.

Identity testing or velocity attacks.[11] Fraudsters initially test stolen payment credentials with transactions on vulnerable e-commerce and m-commerce sites that do not invest adequate resources in security, such as non-profits and charitable organizations, or other businesses where low dollar transactions can be processed undetected. Fraudsters conduct these low dollar tests before using the stolen credentials to make high value purchases. Fraudsters also try to use stolen customer login credentials to access customer accounts with online merchants or payment service providers (PSPs),[12] often inputting these credentials into automated bot attacks that target a large number of online merchants to access the related accounts.

Account takeover (ATO) fraud attacks. A CNP ATO attack[13] occurs when fraudsters use stolen login credentials to access consumer accounts with online merchants or other types of PSPs, steal personally identifiable information (PII) to change account settings, and take over the account to make purchases using the consumer's payment information stored on file. ATO is increasingly committed at scale by bots or scripts that test combinations of stolen usernames and passwords across multiple websites and applications until they are successful. To mitigate ATO fraud, businesses need to quickly and accurately detect fraudulent logins to protect their customers and their brand reputation, using methods that minimize friction with legitimate users.

New account or application fraud attack. A 2016 Javelin Strategy & Research study reported that new account fraud more than doubled in 2015 with PII stolen from 1.5 million consumers used to create fraudulent checking, credit card, loan, and other accounts.[14] This type of fraud occurs when a consumer's stolen or compromised PII, synthetic identities, or compromised primary account numbers (PANs)[15] are used with malware, phishing, or bots, to open new accounts or to obtain lines of credit without the consumer's consent. The nature of the stolen information can vary – the fraudster may use a real person's name, address, payment card, or other information in order to mask his identity or location.

[10] An automated program that operates as an agent for a user or another program or simulates a human activity.

[11] Also referred to as card testing, card probing, or account validation attacks.

[12] A company that serves as an intermediary between the merchant and the payment network, such as a payment processor, merchant acquirer, gateway, wallet provider, or other type of third party service provider.

[13] This type of ATO attack differs from ATO attacks that target consumer financial accounts through online or mobile banking.

[14] Javelin Strategy & Research. (2016, April). *Mitigating application fraud from synthetic identities*. Retrieved from https://www.javelinstrategy.com/coverage-area/mitigating-application-fraud-synthetic-identities.

[15] The 15-16-digit number that appears on the primary accountholder's payment card.

Primary Types of CNP Fraud Mitigation Tools and Approaches

This brief references several primary tools and approaches used to mitigate CNP fraud, including strong consumer authentication, behavioral analytics, device fingerprinting and geolocation, transaction monitoring, and machine learning and artificial intelligence.

Strong consumer authentication. Strong consumer authentication is a critical component to prevent CNP fraud. Industry best practices support a risk-based approach to authentication. Stakeholders should consider the level of risk posed by a transaction or consumer and align that risk with the appropriate level of authentication. Low risk transactions with repeat customers or low dollar items should use frictionless consumer authentication and higher risk transactions should employ additional layers, e.g., step-up, authentication[16] in certain circumstances.

Many authentication solutions are active or customer-facing, requiring a particular action by the user (e.g., username and password, knowledge-based authentication (KBA), one-time passwords (OTPs), out-of-band authentication (OOBA), and biometrics (e.g., fingerprint)). Passive authentication methods are performed in the background (e.g., device fingerprinting, voice recognition, geolocation, IP address, behavioral or biometric analytics, transaction and login analytics, and risk-based authentication).

Payment authentication is performed at the point of a transaction or when a payment card is authenticated before it is stored on file. 3-Domain Secure version 2.0 (3DS 2.0) is the latest authentication tool developed by the card networks (via EMVCo)[17] that is worth noting.[18] 3DS 2.0 is a messaging protocol that enables consumers to be authenticated with their card issuer when making CNP e-commerce and m-commerce purchases. 3DS 2.0 requests that enhanced data be included for transmission to the issuer, including information on the devices being used by the customer, IP address associated with the transaction, geolocation information, and more.

Behavioral analytics. Behavioral analytics solutions examine user actions and compare legitimate versus fraudulent patterns on a website, mobile browser, or mobile app and across third party provider networks. This tool considers the normal behavior of individual account holders, calculates the risk of each new activity, and then applies intervention methods commensurate with the risk in real-time. This allows detection of anomalous activity before a transaction is initiated (e.g., changing contact information prior to initiating a CNP transaction).

Device fingerprinting and geolocation. Device fingerprinting analyzes a computer device (e.g., desktop or mobile) and its characteristics (e.g., installed plug-ins, software, time zone) to confirm that the device being used for a transaction is the same device used for previous legitimate transactions. A "fingerprint" of a user's computer or other access device is established to track activity and determine links with other devices. Device fingerprinting is primarily used to track velocities on devices associated with

[16] The process of using additional authentication methods to verify the identity of a cardholder based on the risk level of the transaction. Step-up authentication can be used for suspicious or atypical transactions, such as a consumer logging into an account from an unknown device. For further verification a merchant can use out-of-band authentication (OOBA) by sending a passcode via SMS text or email to the customer.

[17] EMVCo developed the EMV standard for chip and tokenization specifications. It is jointly owned by American Express, Discover, Visa, MasterCard, JCB, and Union Pay.

[18] For more information about 3DS 2.0, see Pandy, S. (2017). *Why 3-Domain Secure should be adopted in the U.S.* Retrieved from https://www.bostonfed.org/publications/payment-strategies/why-3-domain-secure-should-be-adopted-in-the-us.aspx.

an account and the number of accounts associated with a device. It can also be used to prevent any device associated with fraud from making future purchases/payments.

The growing inclusion of GPS functionality in mobile devices for mapping, navigation, and marketing applications is also being used for security applications. It is often combined with other authentication methods to validate the user's location rather than as a standalone authentication solution, since it only has information about the device. This helps identify potential CNP fraud, particularly if the mapping shows a "high fraud" location or a location distant from the customer's normal location. Depending on the user agreement for a particular mobile application, the consumer may be able to disable this capability within the mobile app or in the mobile device settings. Even if tracking is disabled on the phone, some software can provide an approximate location based on cell tower triangulation.

Transaction monitoring. Transaction monitoring minimizes customer friction by tracking the number of unique accounts, payment cards, geolocations, or email addresses used on each device. While legitimate customers may submit an abnormal number of transactions in a short time period, they are not likely to create new accounts or use new payment methods for each transaction. Therefore, each customer's device or true IP address and history should be individually reviewed to flush out criminals. This can be aided by leveraging a global intelligence network among industry peers. Several fraud prevention and mitigation tools provide customizable fraud management filters to monitor a broad range of information, such as email address, device ID, billing address, shipping address, phone number, IP address, geolocation, and PAN.

Machine learning and artificial intelligence. Machine learning uses artificial intelligence to autonomously "learn" the types of card transactions that are at higher risk of fraud. It applies complex data analysis, rules, and predictive modeling to payment card transactions and combines the results with human insight to flag transactions as valid or fraudulent. With these findings, risk factors and thresholds can then be created and applied to transactions in real time, allowing businesses to accept or reject individual transactions. Because card transactions are always being added to the historical dataset, machine learning can continually revise and update its rules based on new transactions. Traditionally, human-generated rule sets were the most prevalent approach to fraud management and continue to be in practice today. However, the expansive computing power and availability of big data have enhanced how data is used to identify and prevent fraud.

CNP Fraud Mitigation Tools and Approaches for Industry Stakeholders

The X9 CNP Fraud TR discusses mitigation tools and approaches merchants, acquirers, payment gateways, issuers and issuer processors, and payment card networks should consider, some of which are highlighted below.

Merchants. A strong and efficient merchant defense against CNP fraud begins with a comprehensive assessment of customer and transaction history data followed by robust analysis to fully understand their customer base vulnerabilities to certain types of fraud. Merchants can use insights from this data to develop a comprehensive fraud detection strategy, based on their overall risk tolerance. This will depend on the merchant's industry segment, transaction and dollar volumes, and other factors. The fraud strategy should create flexible rules and models to differentiate legitimate transactions from potentially fraudulent ones. It should consider multiple layers of data elements, such as IP geolocation, multi-merchant transaction histories, global delivery address, and phone number verification. Many fraud detection strategies include automated and manual processes for monitoring and reviewing transactions. Merchants should also continually adjust and refine existing strategies by analyzing previous transactions to identify the most useful fraud management settings. In this way, merchants can develop a fraud model that automatically validates legitimate transactions and directs suspicious transactions to the manual review process.

Issuers. Payment card issuers seek to optimize transaction acceptance while minimizing fraud risk. This requires a balance between acceptance rates and security controls to identify and eliminate potentially fraudulent transactions. Overly restrictive security controls may increase false positives (i.e., erroneously identifying legitimate transactions as fraud attempts) leading to lost revenue, customer dissatisfaction, and potential loss of top-of-wallet position. Less restrictive security controls may result in reduced customer inconvenience and increased transaction revenue, but increase the risk of undetected fraudulent transactions resulting in higher losses. While customers typically do not bear any financial loss from fraudulent transactions on their accounts, they experience inconvenience waiting for replacement cards or completing forms to dispute fraudulent transactions. Fraud mitigation strategies for issuers vary substantially based on their customer base, customer service and risk management policies and objectives.

Issuers perform cardholder, payment card, and transaction authentication steps based on the information provided in the transaction authorization message, whereas merchants begin applying customer authentication steps during the customer login and authentication process. The authorization message received by an issuer undergoes a multi-step assessment in milliseconds and the issuer returns an “accept” or “decline” authorization message to the merchant. The assessment includes cardholder authentication, payment card authentication, fraud risk analysis, and final transaction authorization based on the account status and funds or credit availability.

Payment card networks. Payment card networks (networks) see all the transaction data from their individual brands, enabling them to recognize fraud patterns across wide geographies, product categories, and stakeholder groups. This data provides a robust view of cardholder behavior based on historical usage, allowing networks to develop detailed profiles of normal account usage over time, across channels (CNP, CP, recurring, etc.), and by transaction type. In addition, networks are well-positioned to detect and respond to fraud attacks at an early stage, before they impact all of the intended targets. Most networks offer tools to industry stakeholders to help prevent, detect, and manage CNP fraud, and many offer intelligent authorization tools that integrate advanced machine learning across all transactions to monitor for elevated risk and provide automatic responses to network-level security threats.

Key Takeaways

The X9 CNP Fraud TR included several takeaways for mitigating CNP fraud.

Use data more effectively to assess and manage transaction risk and enhance decision-making. Merchants, in particular, need to know what data they have across the organization and collaborate across departments to gather and analyze that data.

Apply stronger customer authentication methods balanced with customer convenience to avoid creating additional friction in the customer journey.

Understand organizational fraud rates. Merchants, in particular, must understand their fraud rates and determine an acceptable and manageable fraud rate for their business. This will help merchants identify pain points that need to be managed and decide what fraud solutions are most appropriate. Understanding fraud rates will help merchants know how much attempted fraud they are stopping and how many orders they are reviewing.

Deploy a data security solution. Merchants need to deploy a data security solution combined with fraud mitigation tools. Both are needed to effectively address CNP fraud. Tokenization and encryption tools are critical considerations to include as part of a data security strategy.

Enhance industry collaboration. Stakeholders should seek collaborative solutions, particularly those that enhance the coordination between merchants and issuers.

Implement adaptive CNP fraud mitigation models. Issuers and merchants need to keep pace with the evolving nature of CNP fraud attacks. Stakeholders need to shift from a reactive to an adaptive approach, striving for continual improvement in the efficiency and effectiveness of fraud mitigation strategies, policies, procedures, and tools.

Monitor industry fraud trends. Stakeholders should stay current on industry-wide CNP fraud intelligence to identify new fraud trends, attacks, and corresponding fraud mitigation strategies. Industry groups can be leveraged to identify best practices and other opportunities for improvement and to provide advice regarding effective fraud mitigation tools and techniques.

Review and adjust the CNP fraud mitigation plan and models. Regardless of the frequency of fraud rule updates, the full CNP fraud mitigation strategy should be reviewed at least annually. This periodic review allows for updating the fraud rules and risk scores assigned to the data elements in the current fraud screening model; and identifying and addressing any gaps in the data elements of the fraud model.

Status of X9 CNP Fraud TR

The X9 CNP Fraud TR was balloted to the X9 Voting Members on October 31, 2017 and closed on December 2, 2017 with the required number of affirmative votes to move forward (two-thirds affirmative vote). Participants can vote “yes or no” both “with or without comments” or they can abstain. The ballot included submission of comments, which the workgroup reviewed to develop a revised TR. The final TR was balloted to the X9 Board Category A organizations, which closes on February 23, 2018. If fully approved, the TR is anticipated to be published by X9 in mid- to late 2018.