FEDERAL
RESERVE
BANK
of ATLANTA

Getting Ahead of the Curve: Assessing Card-Not-Present Fraud in the Mobile Payments Environment

Marianne Crowe and Susan Pandy, Federal Reserve Bank of Boston
David Lott, Federal Reserve Bank of Atlanta

November 10, 2016

Marianne Crowe is Vice President and Susan Pandy is Director in the Payments Strategies Group at the Federal Reserve Bank of Boston. David Lott is a Payments Risk Expert in the Retail Payments Risk Forum at the Federal Reserve Bank of Atlanta. The views expressed in this paper are solely those of the authors and do not reflect official positions of the Federal Reserve Banks of Atlanta or Boston or the Federal Reserve System.

Mention or display of a trademark, proprietary product, or firm in this report 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.

The authors would like to thank members of the MPIW and other industry stakeholders for their engagement and contributions to this report.

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

The U.S. retail payments industry is undergoing significant change to secure card payments by migrating to EMV chip cards for card-present or point-of-sale (POS) transactions. Effective October 1, 2015, card network operating rules changed to shift fraud liability to the merchant if it was not enabled to accept EMV chip credit or debit cards. As a result, merchants have been upgrading their terminals to comply. Enabling EMV chip card acceptance at POS reduces card-present counterfeit fraud by removing the opportunity for fraudsters to compromise payment card credentials. However, this is driving fraudsters to attack the more vulnerable online and mobile card-not-present (CNP)[1] channels with weaker authentication protocols, at a time when consumers are increasing their use of mobile phones to make CNP purchases. According to a 2016 Javelin study, consumer use of the mobile browser to make online purchases doubled from 2011 to 2016, and the availability of mobile apps to make online purchases is adding to that trend.[2]

Recognizing that these trends are predictors of future CNP growth, industry stakeholders are closely monitoring the CNP landscape and assessing existing security controls for gaps to understand what is needed to protect against new risks and threats. This whitepaper describes the work of the MPIW[3] to identify and analyze potential areas where mobile commerce is vulnerable to fraud and other threats. The analysis was conducted within a framework of four use cases to which existing wallet models were mapped. The group identified potential risks and threats for each model and then compared risks across models. They completed the analysis by outlining key controls and tools to enhance security for the wallet models within the use cases.

The whitepaper first provides an overview of the current CNP landscape (Section III). Context is based on the impact of CNP fraud in European countries and Canada after they migrated to EMV chip cards, and also shows the growth trends for e-commerce and m-commerce transaction volume. It then describes the framework used to analyze the four mobile CNP use cases and the subsequent comparative analysis across functions and risk factors (Section IV). The paper concludes by describing several gaps and issues associated with security approaches, as well as recommendations for industry stakeholders to consider for improving CNP payment security.

[1] Card-not-present payment occurs when a cardholder/card is not physically present when making a purchase, preventing the merchant from validating the cardholder as the card owner. Examples of CNP payments include internet (via mobile or PC/laptop), telephone, or mail order.

[2] Javelin Strategy & Research. (2016, October.) *Mobile Online Retail Payments 2016*.

[3] The Mobile Payments Industry Workgroup (MPIW), convened by the Federal Reserve Bank of Boston Payment Strategies group and the Federal Reserve Bank of Atlanta Retail Payments Risk Forum, meets several times per year to discuss trends, developments, and barriers to adoption of mobile and digital retail payments, with a shared goal of building an efficient, secure, and ubiquitous mobile/digital payments environment in the U.S. For more information, see https://www.bostonfed.org/payment-studies-and-strategies/digital-mobile-payments-innovation-and-applied-research/mobile-payments-industry-workgroup.aspx.

II. INTRODUCTION

The convergence of physical and online channels increases the complexity of retail payments. Multiple stakeholders, including financial institutions (FIs) and non-banks, are developing alternative payment methods that leverage existing payment systems in different ways. Many are mobile and digital wallet solutions that support CNP payments. These solutions are creating new opportunities, but also challenges for merchants, issuers, and security vendors to manage risk across channels and payment types. The MPIW has been following the expansion of mobile payments beyond the POS to the CNP/e-commerce channel to evaluate the associated risks.

It is important for the payments industry to understand how the migration from magstripe to EMV chip card at POS and the ensuing shift in fraud to the CNP channel will impact m-commerce.[4] Methods used to combat fraud in the traditional e-commerce channel may not necessarily apply to m-commerce, and there are new controls and security methods for mobile of which the payments industry should be advised, which are addressed in this paper.

In July 2015, the MPIW formed a subgroup to develop a set of mobile CNP use cases and conduct an assessment of their fraud risks.[5] The four use cases covered mobile models with and without card-on-file (CoF)[6] (credit or debit only, not prepaid), and models using a mobile browser or mobile app.[7] The project objectives were to:

1. Review relevant industry research on CNP fraud;
2. Define specific m-commerce use cases and analyze the functions that are vulnerable to known types of attacks;
3. Conduct a comparative analysis of the risks, security gaps, mitigations, and controls across the defined use cases;
4. Provide an overview of available authentication solutions and security controls;
5. Identify best practices and recommendations for mitigating m-commerce CNP fraud.

The four use cases are:

1. Guest checkout via merchant mobile app or mobile browser, no payment CoF.

2. Mobile in-app purchase using an EMV payment token and identification and verification (ID&V), as defined in the *EMV Payment Tokenization Specification* (EMV spec).[8] These models are mobile

[4] CNP fraud involves the unauthorized use of payment credentials (stolen credit/debit card number) to purchase products or services in a non-face-to-face environment between the customer and the merchant, such as an e-commerce transaction via a call center, computer, mobile device, or mail order. Smart Card Alliance (2014, Feb.) *Card-Not-Present Fraud: A Primer on Trends and Authentication Processes*. Retrieved from http://www.emv-connection.com/downloads/2014/01/CNP-WP-012414.pdf.
[5] We recognize the existence of other use cases and the emergence of new ones in the market, but it was necessary to maintain a narrow focus to complete this analysis. The MPIW will assess emerging models in future research.
[6] Card-on-file (CoF) is the authorized storage of a consumer's payment credentials by a merchant or payment service provider that allows the consumer to make repeat or automatic payments, including money transfers, without the need to re-enter payment credentials each time.
[7] Other payments, such as prepaid, gift cards and branded open loop cards are out of scope for this study.
[8] The EMV Spec describes payment tokens and an ID&V process that validates the cardholder and cardholder's account (PAN) to establish a confidence level for binding the payment token to the PAN/cardholder. EMVCo (2014, March). *EMV Payment Tokenization Specification – Technical Framework*. Available at http://www.emvco.com/specifications.aspx?id=263.

wallets offered by wallet service providers (WSPs) that use near-field communication (NFC)[9] technology and store the payment token in a secure element (SE) on the mobile phone;[10] or that use host card emulation (HCE),[11], storing the token in a secure trusted zone in the mobile OS or in a trusted execution environment (TEE) in the mobile phone.[12] The industry has labeled these as the "Pay" wallets.[13] While Pay wallets are expanding into the mobile browser environment, this paper does not address that use case.

3. Mobile browser or mobile app CoF wallets provided by online merchants[14] or payment service providers (PSPs)[15] (e.g., PayPal, Pay with Amazon) that use other authentication processes that are not "EMV ID&V." The consumer authenticates via login through the PSP, if the PSP processes on behalf of the merchant,[16] or via login directly on the merchant's website.[17]

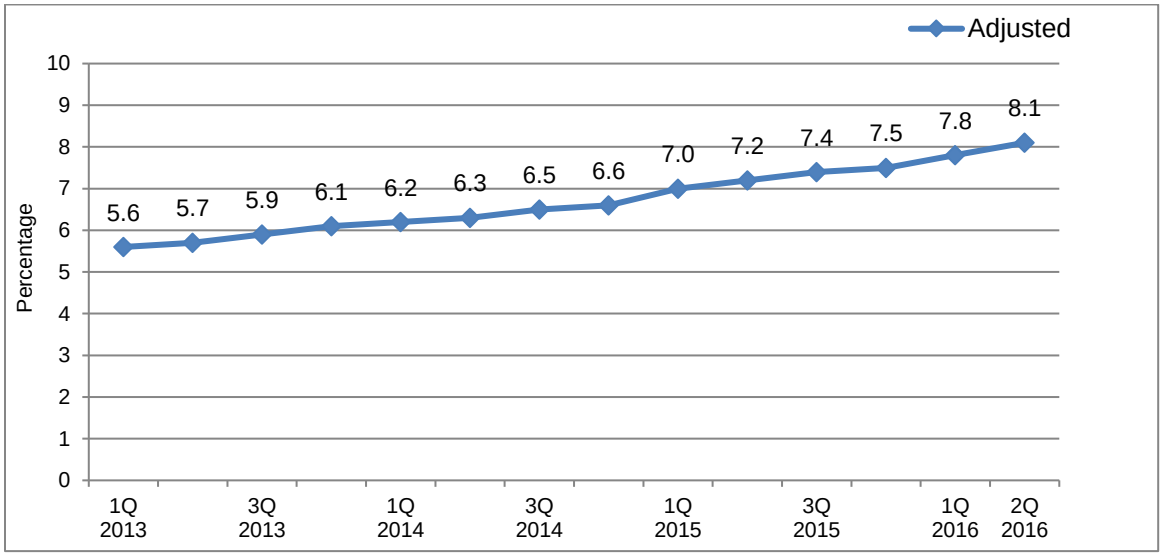
4. Card network digital wallet (e.g., American Express (AmEx) Checkout, Masterpass, and Visa Checkout).

[9] Near-field communication (NFC) is a standards-based wireless communication technology that allows data to be exchanged between devices that are a few centimeters apart. While NFC only applies to the POS transactions and not CNP, these wallets are grouped into one use case because of their support of NFC and EMV payment tokens.
[10] GlobalPlatform defines a secure element (SE) as a tamper-resistant one-chip secure microcontroller capable of securely hosting applications and their cryptographic data (e.g., key management) in accordance with the rules and security requirements set forth by trusted authorities.
[11] Host card emulation (HCE) allows NFC card emulation without using the secure element (SE) in mobile handsets by enabling NFC card emulation communications to be routed through the mobile phone's host processor versus from the POS terminal through the NFC controller to the SE.
[12] The trusted execution environment (TEE) is a secure area of the main processor of a smart phone (or other connected device). It guarantees code and data loaded inside (e.g., payment tokens) to be protected with respect to confidentiality and integrity.
[13] Apple Pay, Android Pay, and Samsung Pay are *currently* the only mobile wallet models in the marketplace that follow the EMV spec that requires payment tokenization and issuer ID&V. Other mobile wallets, such as Chase Pay and Walmart Pay, are not defined as "Pay" wallets in this study because they are proprietary, and use QR codes instead of NFC.
[14] This paper assumes that the merchants referenced are all "online" merchants that operate in a CNP environment, in addition to or instead of POS, enabling purchases via the mobile browser or mobile app.
[15] A payment service provider (PSP) may be a payment processor, merchant acquirer, gateway, wallet provider, or other type of third party that serves as an intermediary between the merchant and the payment network.
[16] PSPs provide payment acceptance services for online merchants that allow consumers to authenticate to their PSP account to initiate purchases, and the PSP processes the payment on behalf of the merchant (i.e., merchant of record).
[17] Merchant mobile website or mobile app allows a customer to create an account and store a payment card on file for future purchases. Consumer authenticates to the merchant with login credentials to initiate purchases.

III. CNP LANDSCAPE OVERVIEW

The e-commerce and m-commerce channels are experiencing strong growth, driving up CNP transaction volume and associated dollar value. E-commerce sales as a percentage of overall retail sales has been steadily increasing since 2006, and was 8.1 percent in Q2 2016, as illustrated in Figure 1. In terms of dollars, the U.S. Department of Commerce estimated retail e-commerce sales[18] for Q2 2016 at $97.3 billion, marking a 4.5 percent increase over Q1 2016.[19] At the same time, global payments fraud is growing rapidly across all channels and significant data breaches have become commonplace, which is driving concerns about increased e-commerce fraud in the U.S.

Figure 1. Estimated Quarterly U.S. E-Commerce Sales as Percent of Total Retail Sales (2013-2016)



Source: U.S. Department of Commerce. (2016, Aug. 16). *Quarterly Retail E-Commerce Sales 2nd Quarter* 2016

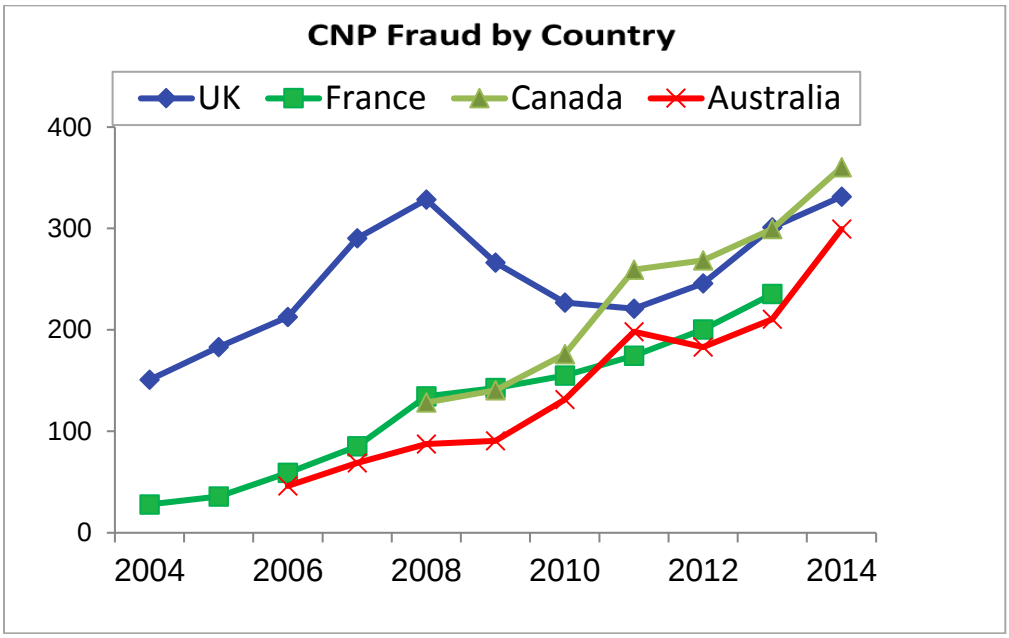
In 2012, card networks announced a liability shift for issuers and merchants that did not migrate from magstripe payment cards to EMV chip cards to combat POS counterfeit card fraud by October 1, 2015. While EMV chip cards protect against counterfeit fraud for POS card present transactions, they do not provide added protection for the CNP environment, since the chip is not used in the transaction. Fraudsters are taking advantage of this gap in security by shifting their focus to CNP activity, supported by the experiences of other developed countries which have shown that EMV chip card implementations led to the migration of fraud to other types of transactions. In Europe, fraud shifted to CNP card payments with weaker authentication controls (e.g., e-commerce/m-commerce, mail order, and telephone order).

[18] The U.S. Department of Commerce defines e-commerce sales as the sale of goods and services where the buyer places an order, or negotiates the price over an Internet, mobile device (m-commerce), extranet, electronic data interchange (EDI) network, electronic mail, or other comparable online system. Payment may or may not be made online.

[19] U.S. Department of Commerce (2016, Aug. 16) *Quarterly Retail E-Commerce Sales 2nd Quarter* 2016. CB16-18, Retrieved from https://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf.

Figure 2 shows how CNP fraud increased between 2004 and 2014 in the U.K., France, Canada, and Australia after these countries migrated to EMV chip cards.[20] In the U.K., card-present counterfeit fraud decreased 56 percent from 2005 to 2013. However, CNP fraud losses (primarily e-commerce fraud) increased 79 percent from 2005 to a peak in 2008.

Figure 2. EMV Card Migration does not Address CNP Fraud (Values shown in local currencies)



Sources: Data compiled from Financial Fraud Action UK, The Observatory for Payment Card Security, Canadian Bankers Association, and Australian Payments Clearing Association

E-commerce merchants and issuers were able to reduce their fraud losses in subsequent years after implementing 3-Domain Secure (3DS),[21] a stronger authentication protocol for e-commerce transactions, and improved fraud analytics.[22] Many European merchant locations also stopped accepting magstripe cards, which limited the ability for fraudsters to use compromised counterfeit magstripe card data in the CNP environment.

[20] Figure 2 shows the currency value of CNP fraud losses for each country, not the transaction volume. It should be noted that while the value of fraud losses has increased, total e-commerce spending has increased as well.
[21] 3-Domain Secure (3DS) is a secure communication protocol used to enable real-time cardholder authentication directly from the card issuer during an online transaction to improve online transaction security and support the growth of e-commerce payments.
[22] Rippleshot (2015, April). *EMV Adoption in the U.S.* Retrieved from http://info.rippleshot.com/hubfs/Mktg_Offers/EMV_Whitepaper.pdf?t=1470846395564.

Remote channels have experienced a sharper rise in the cost per dollar of fraud losses. Figure 3 shows that although physical POS-only merchants have cost/dollar fraud levels similar to remote channel merchants, their year-over-year increase of 3 percent is significantly smaller than the 9-12 percent experienced by online and mobile commerce merchants, respectively.[23]

Figure 3. Cost per Dollar of Fraud Losses by Year by Channel (2015-2016)

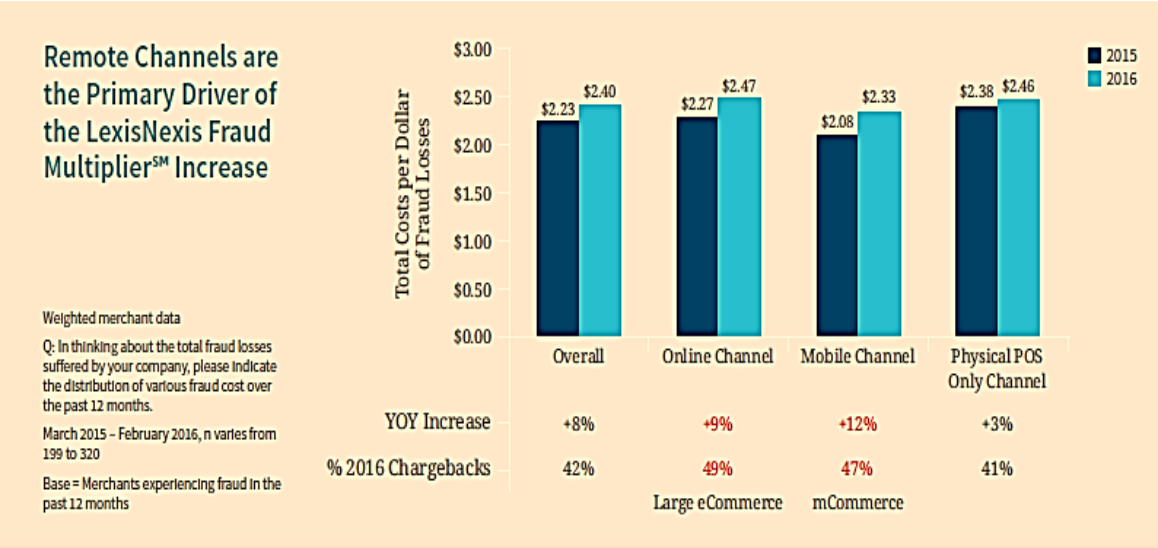


Figure 4: Cost per dollar of fraud losses by year by channel (2015 – 2016)

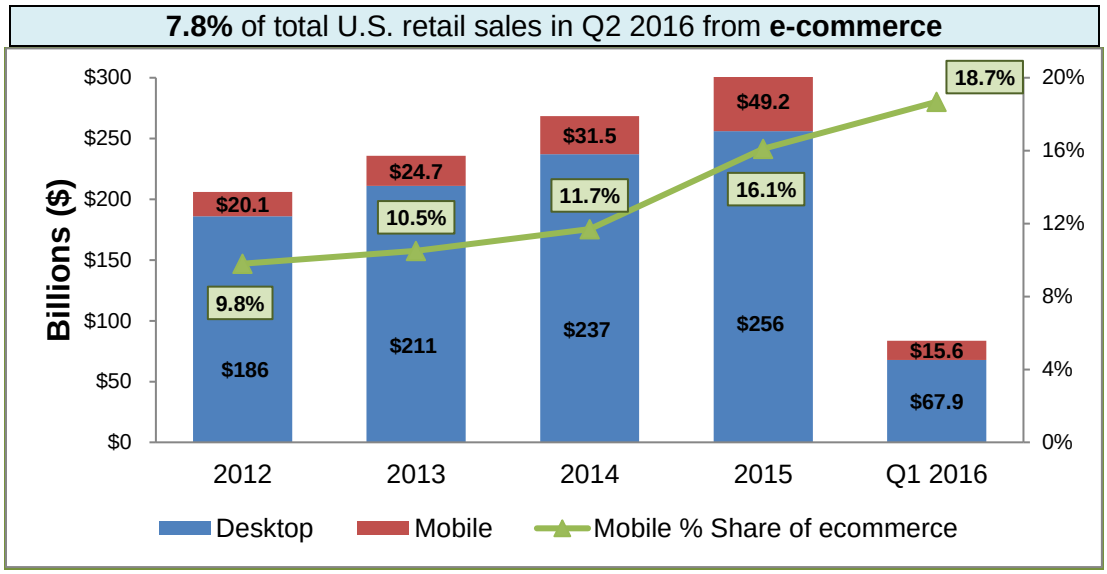
Source: LexisNexis (2016). *2016 LexisNexis True Cost of Fraud Study*

Mobile fraud is an even bigger issue because it is expected to grow at a faster rate than total e-commerce. Fraud cost as a percentage of revenue is higher among m-commerce merchants, and is expected to increase as more transactions are processed through the m-commerce channel over the next 1-2 years (2017-2018). Therefore, the payments industry must prioritize actions to improve the security of CNP transactions overall, including the mobile space.

[23] LexisNexis (2016, May). *2016 LexisNexis True Cost of Fraud Study*. Retrieved from https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2016.pdf.

E-commerce sales have been growing for the last several years, but m-commerce sales, as a component of total U.S. retail e-commerce sales, have been increasing at a higher percentage each year since 2012. Figure 4 shows that m-commerce is currently 19 percent of total retail e-commerce dollars, while desktop e-commerce sales have also been growing but at a declining rate, averaging 11.2 percent since 2012.

Figure 4. M-commerce as Percentage of E-commerce



Source: U.S. Census Bureau (2016); comScore M-commerce Measurement (2016)

Merchants can offer multiple approaches for consumers to make m-commerce purchases and help drive up overall e-commerce volume: (1) by directly accessing a merchant's mobile website using the mobile browser on the mobile phone; (2) by downloading a merchant's native mobile app[24] from the merchant's website or from one of the mobile app stores (e.g., Apple Store or Google Play); (3) by using a mobile "Pay" wallet (e.g., Apple Pay, Android Pay, or Samsung Pay) to make digital purchases directly from within a merchant's native mobile app or via a mobile browser, using payment credentials stored securely with the Pay wallet; or (4) by using a digital wallet offered by a PSP (e.g., PayPal, Amazon, card network) that works with multiple participating retailers. It will be important for the industry to monitor trends in merchant acceptance of various types of mobile payments and wallets, as well as consumer preferences for shopping with different mobile wallet options (browser, merchant app, in-app wallet, or digital wallet) to understand behavior as well as the related risk mitigation requirements.

More online merchants are enabling purchases through the m-commerce channel according to a Kount 2016 mobile payments and fraud survey.[25] This survey shows that 82 percent of merchant respondents support the mobile channel, up from 69 percent in 2014. Fifty-eight percent of merchants have a dedicated mobile website, 55 percent have a mobile app, and 34 percent accept at least one mobile wallet to support m-commerce. Despite this support for the mobile channel, when asked how important it was to have the ability to detect mobile devices in the inaugural 2012 study, more than 55 percent of merchants could not tell if a mobile device was used to complete an online transaction. This number dropped to 35 percent in

[24] Merchant native mobile apps are covered in *Use Case No. 3 – Cloud-based Wallets provided by online merchants or PSP that use other authentication processes*.
[25] Kount (2016). *Mobile Payments & Fraud: 2016 Report*. Available for download at http://info.kount.com/mobile-payments-report-2016. A survey of merchants, acquirers, and other organizations.

the 2016 survey. Kount concluded that perhaps the decline is because merchants now take this ability for granted, and are focusing on how to collect quality information from the consumer's mobile (or other connected) device, such as device type, to analyze transactions.

The Kount study also reported that nearly half (43 percent) of merchants indicated they did not know the value of fraud losses from the mobile channel.[26] This makes it difficult to determine the impact of mobile fraud on adoption. In a separate set of fraud and risk-focused questions, when respondents (card networks and merchants) were asked whether or not they considered the mobile channel to be riskier than the traditional e-commerce channel, 41 percent of merchants considered the mobile channel to be "somewhat riskier" or "far riskier" than PC-based e-commerce. Kount qualified this question by measuring how many organizations actually track and differentiate fraud in the mobile channel from fraud in the traditional e-commerce channel. Fifty-six percent of merchants reported that they track m-commerce fraud attempts or losses separately from e-commerce fraud.

Several barriers exist to mitigating fraud in the mobile/e-commerce space. First, because the customer cannot be physically identified by the merchant, more robust tools are needed to perform authentication. Second, smaller and mid-sized merchants may be unaware of available security tools and their value (e.g., multifactor authentication,[27] encryption, tokenization), or the tools may not be easily accessible or affordable. Third, merchants must balance the need to reduce fraud with the risk of creating consumer friction that results in shopping cart abandonment or rejecting legitimate customers. More effective identity management to improve consumer authentication is needed and has been highlighted as a major industry gap, particularly for e-commerce where transactions are more vulnerable to fraud because the consumer is not present. An analysis of how the m-commerce use cases address these issues is discussed in the next section.

[26] This percentage is based on a response to a new question on the survey asking merchants, "What share of their total fraud losses are occurring in the mobile channel?"

[27] Multifactor authentication (MFA) combines two or more independent credentials or factors: what the user knows (password), what the user has (token) and what the user is (biometric verification).

IV. COMPARATIVE USE CASE ANALYSIS

The subgroup created a matrix framework to compare use cases and provide a qualitative analysis of the potential risks associated with different wallet models in order to discuss risks in a relative manner. The objective of the assessment was to assist industry stakeholders when developing their wallet strategies. Multiple factors informed the risk analysis, including input from subject matter experts within the MPIW, industry research, and personal experiences using some of the wallets, which together represent our interpretation of the wallet models.

The matrix describes five functions of a mobile CNP transaction: (1) account creation,[28] (2) EMV identification and verification (ID&V),[29] (3) authentication, (4) integration of mobile device and operating system (OS), and (5) use of third party providers, which are vulnerable to known types of attacks. The applicability of several risk types (identity theft, data breach, account takeover fraud (ATO),[30] new account fraud,[31] man-in-the-middle (MiTM)[32] or man-in-the-browser (MiTB)[33] attacks, fingerprint spoofing, malware/virus, and social engineering) were considered for each function.

The result is a qualitative determination (high, medium, or low) of the probability of risk of an attack and the magnitude of risk of impact to the stakeholder(s) (typically the consumer/device, merchants, or the broader payments industry) for each function within the use case.

Magnitude of risk is defined as the level of impact to the affected stakeholders, based on our interpretation of the analysis. A high magnitude of risk could have a greater impact on a consumer (e.g., financial loss), impact to multiple consumers, or multiple merchants, etc., with greater associated expense. A medium magnitude of risk would have some broader impact and expense; and a low magnitude of risk would have minimal impact to the consumer, merchant, or payments industry.

Probability of risk is defined as the likelihood of the risk occurring for the specific wallet use case, as it is currently configured. A high probability of risk indicates that a specific attack is very likely to occur. Medium probability indicates that the risk of attack is little or somewhat likely to occur, and low probability of risk represents the unlikelihood of an attack.

Each function and the associated types of attacks are described below. Risk matrix details are included in Appendix B.

---

[28] Account creation is the consumer process of opening a new online account and establishing a user profile with a merchant, PSP, WSP, financial institution, or other business during which consumer PII and payment credentials are collected and can be a potential point of vulnerability.

[29] In this analysis, EMV ID&V only applies to Use Case 2 – Mobile In-App, although it is now used to provision payment tokens to the Masterpass digital wallet and other emerging models.

[30] Account takeover fraud occurs when a fraudster obtains an individual's bank or payment card number and other PII, such as email, password, username, or social security number. The fraudster changes the contact information or adds another user to an existing account, which he can then use to conduct transactions. Fraudsters can buy login details from the black market, use malware and phishing to steal, or refer to a list of the most common passwords to attempt to hack a customer's online shopping account.

[31] New account fraud occurs when a fraudster creates a new account (with PII or payment information obtained from a breach) using a customer's real name, and commits fraud usually within the first 90 days after an account is opened.

[32] A man-in-the-middle (MiTM) attack intercepts a communication between two systems. For example, an attacker within reception range of an unencrypted Wi-Fi wireless access point can insert himself in the communication between the two points.

[33] Man-in-the-browser (MiTB) is a type of MiTM attack that uses a proxy Trojan horse to infect a web/mobile browser by taking advantage of vulnerabilities in browser security to modify web pages or transaction content.

A. FUNCTIONS VULNERABLE TO ATTACKS IN THE CNP ENVIRONMENT

1. ACCOUNT CREATION

For these use cases, account creation occurs when a consumer creates an account with an online merchant, PSP, or WSP[34] and links the eligible credit or debit payment card credentials to that account. Fraudsters attack the account creation process to obtain account login credentials and PII,[35] which is becoming an alternative attack option to the prevalent method of stealing payment credentials by data breach during the transaction process. This shift is being driven by a combination of the tightened security of EMV chip card transactions and POS terminals, and increasing online transaction volume as consumers make more purchases electronically.

[34] A payment service provider (PSP) includes Amazon and PayPal. A wallet service provider (WSP) includes companies that offer specific wallet solutions (e.g. Apple (Apple Pay), Google (Android Pay), etc.)

[35] NIST Special Publication 800-122 defines personally identifiable information (PII) as "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."

Attacks that impact account creation include data breach, malware or virus, account takeover fraud, new account fraud, and mobile device-porting fraud. The attacks are described in the following chart.

ATTACKS THAT CAN IMPACT ACCOUNT CREATION IN THE CNP CHANNEL	
Data breach	• Fraudsters obtain PANs and PII to access accounts consumers have with online merchants, PSPs, or WSPs; or to create new accounts. • Data breaches usually manifest into other types of attacks noted in this chart.
Malware or virus[36]	• Malicious software that disrupts a mobile device/OS to steal PANs and PII, used by a fraudster to create accounts with online/mobile merchants, PSPs, or WSPs. • Malware attacks on smartphone users more than tripled in 2015 compared to 2014,[37] and will continue because of the vulnerability of legitimate mobile apps that can lead to data breaches.[38] • 97% of malware attacks target the open Android OS, due to the tightly controlled Apple iOS.[39]
Account takeover fraud (ATO)	• Fraudsters use stolen consumer login credentials to access online accounts and steal PII to change account settings and take over the account, assuming there are no other layered controls are in place (e.g., OTP to tenured channel on file with issuer for each transaction).[40] • After gaining control of an account, fraudsters can make high-value purchases or mask fraudulent transactions. • This type of attack underscores the importance of protecting the PAN and related data because fraudsters have access to much more data via the CNP channel.[41] • ATO fraud has increased significantly in the e-commerce channel, resulting from increased stolen identities obtained through data breaches.[42]
New account fraud	• Fraudsters use compromised PANs and PII to create new CNP accounts because online account enrollment is easier to complete with valid information. • New account fraud is growing rapidly and more than doubled in 2015 with PII stolen from 1.5 million consumers used to create fraudulent checking, credit card, loan, and other accounts.[43]
Mobile device-porting fraud	• Fraudster obtains PII through a compromise, calls the consumer's mobile carrier and impersonates the consumer to request transferring his mobile phone number to the fraudster's new phone. • Fraudster then uses the stolen PII and PAN to enroll a wallet on his new mobile phone and conduct fraudulent transactions.

[36] Examples of malware include Trojans, worms, virus, spyware, and ransomware.

[37] Kaspersky Lab (2016, Feb. 23). *The Volume of New Mobile Malware Tripled in 2015*. Retrieved from http://www.kaspersky.com/about/news/virus/2016/The_Volume_of_New_Mobile_Malware_Tripled_in_2015 and Gostav, A., et. al. (2016). *IT Threat Evolution in Q1 2016*. Kaspersky Lab. Retrieved from https://securelist.com/files/2016/05/Q1_2016_MW_report_FINAL_eng.pdf.

[38] Security News Desk (2016, Jan 5.) *2016: Networks And Mobile Devices Come Under Attack*. Retrieved from http://www.securitynewsdesk.com/2016-networks-and-mobile-devices-come-under-attack/

[39] Although Android has been the primary target for attacks, iOS attacks are growing since non-jailbroken iOS devices were infected by the WireLurker Trojan in November 2015. Millman, R. (2016, June 26). Updated: 97% of malicious mobile malware targets Android. *SC Magazine*. Retrieved from http://www.scmagazineuk.com/updated-97-of-malicious-mobile-malware-targets-android/article/422783/.

[40] Once fraudsters obtain consumer usernames and passwords, they attempt fraud across multiple online accounts since consumers tend to use the same password for many accounts. Fraudsters may also alter account details (e.g., personal and contact information) to block consumers from regaining control of their accounts.

[41] Research shows that fraudster demand for PANs is decreasing because payment companies (and cardholders) quickly identify anomalous spending patterns, limiting the shelf life of stolen payment card data.

[42] The mobile attacks may stem from unsecured WiFi networks that can intercept consumer credentials, spoofed mobile apps downloaded by consumers that deliver malware to a user's mobile device, and interception of PII inadvertently leaked by a legitimate mobile app or intercepted by malware, MiTB, or bots. Threat Metrix (2016). *Cybercrime Report: Q1 2016*. Retrieved from https://www.threatmetrix.com/whitepapers/ThreatMetrix-Cybercrime-Report-Q12016.pdf?_ga=%201.97586775.%20934060937.1453926672.

[43] Javelin Strategy & Research (2016, April). *Mitigating Application Fraud from Synthetic Identities*. Available at https://www.javelinstrategy.com/coverage-area/mitigating-application-fraud-synthetic-identities.

2. EMV ID&V

EMV ID&V refers to the issuer process of risk management decisioning to authenticate a consumer and validate the payment card primary account number (PAN) *before provisioning a payment token to a Pay wallet*. EMV ID&V plays a key role in determining if the consumer is the legitimate owner of the account credentials linked to a Pay wallet; therefore, it is a critical point of vulnerability if not performed effectively. Tokenized payment credentials will not be provisioned to the secure area of a mobile phone for a Pay wallet until the issuer has vetted the cardholder and account. During the provisioning process, the Pay wallet provider may send the issuer a risk score based on a review of data that the Pay wallet providers collect, such as device ID, device fraud scoring (i.e., history of fraud on the device), geolocation, phone model, type of mobile OS (e.g., iOS or Android), and history of iTunes or Google account, to improve the risk decisioning process.

3. AUTHENTICATION

During the transaction process, a customer is also authenticated to the online merchant, PSP, or WSP. Several well-known authentication solutions for mobile CNP transactions are customer-facing, such as username and password, knowledge-based authentication (KBA), one-time passwords or tokens (OTPs), and out-of-band authentication (OOBA). Other authentication methods include: device and location-based authentication, such as device ID, geolocation, and biometrics (e.g., fingerprint); data verification; risk-based authentication (RBA); and behavioral analytics. Strong authentication practices do not rely on one method of authentication, but employ multi-layered or multifactor authentication (MFA), which are both recommended best practices. Layered authentication employs multiple methods of single-factor authentication (e.g., username and password plus KBA). The goal of MFA is to create a layered defense and make it more difficult for an unauthorized person to access the physical location, computing device, network, or database. If one factor is compromised or broken, the attacker still has at least one more barrier to breach before successfully breaking into the target. Furthermore, the level or strength of the authentication method should match the risk being mitigated. Despite the broad range of solutions available, authentication is the most serious fraud challenge merchants and issuers face for both e-commerce and m-commerce.

The following chart describes different authentication methods.

TYPES OF AUTHENTICATION METHODS	
Username and password	• Most common and inexpensive method, but also the most vulnerable method used to access accounts via the online or mobile channel. Data breaches often target usernames and passwords, so to strengthen its use requires additional layers or types of authentication.
Knowledge-based authentication (KBA)	• Requires user to answer secret questions that cannot be found easily in a physical wallet or online (e.g., mortgage amount, prior residences, high school mascot, favorite book, etc.).
Out-of-band-authentication (OOBA)	• Type of two-factor authentication that requires a second verification method through a separate communication channel (e.g., SMS or email) along with customer's username and password. A one-time password (OTP) is a form of OOBA sent via SMS for the customer to verify.
Risk-based authentication (RBA)	• Examines a variety of contextual information (e.g., IP address, geolocation), which device is being used (e.g., device type), and whether or not the user's behavior is consistent (e.g., login frequency and attempts) to verify the consumer's identity.[44] • RBA can be performed in the background by using more cardholder and transaction data for risk-decisioning and only proactively involving the consumer if the risk exceeds a predetermined level.
Device ID/fingerprinting	• Analyzes the mobile device and its characteristics (e.g., installed plug-ins, software, time zone, etc.) to confirm that the mobile device being used for a transaction is the same device used for previous legitimate transactions.
Device type	• Each mobile device has unique attributes and characteristics that provide information about how it works with a particular transaction.
Geolocation	• Uses digital information via the internet to identify the geographical location of the user/mobile device.
Biometrics	• Current solutions include fingerprint, facial or iris recognition, and voice print. • Fingerprint is currently the most common method for mobile CNP payments, particularly with the increased installation of fingerprint sensors on newer smartphone models, but use of voice and iris recognition is growing. • Consumer surveys show favorable comfort levels using certain biometrics in lieu of usernames and passwords.[45]
Behavioral analytics	• Leverages information about a user's normal online activity patterns to detect good users from bad ones and determine if additional authentication is required.[46] • For m-commerce, both the login and browsing processes should be monitored for anomalous activity to determine if certain transactions do not align with the user's typical patterns of transacting.[47]

[44] CA Technologies (2014). *Why Strong Authentication is a Must for All Users.* [Presentation] Retrieved from http://www.ca.com/content/dam/ca/us/files/ebook/why-strong-authentication-is-a-must-for-users.pdf.

[45] Accenture (2015, July). *2015 North America Consumer Digital Payments Survey: When It Comes to Payments Today, the Customer Rules*. Available at https://www.accenture.com/us-en/insight-digital-payments-survey.

[46] For instance, consumer shopping habits reveal information about their behavior such as where and when they shop, how much they typically spend, etc. A user who initially fails login and then changes the shipping address before confirming an online purchase might raise a red flag. Other identifiable behaviors include how long a user spends browsing, browsing history, and browsing patterns.

[47] Behavioral analytics should not be confused with behavioral biometrics which may track patterns related to how a user interacts with his mobile device.

The use cases assess some types of attacks on authentication, including MiTM/MiTB and spoofed authentication, described below.

TYPES OF AUTHENTICATION ATTACKS	
Mobile man-in-the-middle/browser attack	• Perpetrator installs Trojan horse malware on the victim's mobile device that can modify the user's online transactions in real time. • Perpetrator installs malware to fool a user into downloading a fake mobile app that can intercept SMS traffic such as authorization codes used for OOBA.
Spoofed authentication	• Uses a fake mobile app to capture sensitive data and/or authentication factors. • Some factors that can be spoofed include biometric fingerprint, mobile device, and IP address. A spoofed device can make other features, such as SMS, susceptible to redirection, hijacking, and spoofing. • Faked or cloned mobile apps can also capture consumer authentication credentials.

4. INTEGRATION OF MOBILE DEVICE AND OPERATING SYSTEM

Mobile devices and operating systems are addressed jointly because most mobile operating systems support specific hardware, with little flexibility.[48] There are three levels of security for a mobile device: 1) hardware, 2) hardware and software, and 3) software. Differences in hardware and software may affect the security level of a mobile device. For example, Apple Pay relies on hardware embedded in the mobile phone (i.e., a tamper-resistant SE that is impenetrable by malware or virus) that securely stores the payment token and payment applets, protecting them from attacks on the mobile OS. Samsung Pay uses a hybrid approach that relies on an integrated security environment (i.e., TEE), and Android Pay relies on software that creates isolated secure "zones" stored in the mobile OS memory. Use Cases 1, 3 and 4 (non-Pay wallet models) are device-agnostic and can be accessed using a mobile app or mobile browser. Online merchants and PSPs that support or offer device-agnostic mobile wallet models must be cognizant of the existing vulnerabilities posed by mobile devices and operating systems which they cannot control.

Mobile Device versus Mobile Operating System Risks

Several risks can impact a mobile device or OS: jailbreaking or rooting a mobile phone, lost or stolen device, and malware or virus. Many of these risks occur because of the inability to change consumer behavior to protect the device (e.g., PIN to unlock phone, anti-virus software, not downloading unapproved apps, etc.). Jailbreaking and rooting are considered a larger problem than most might consider as research shows that more than 27 percent of users root their phones.[49] A jailbroken or rooted device diminishes the existing security controls in the mobile OS, exposing the mobile browser or mobile app to malware or spyware that could potentially capture sensitive data. A lost or stolen device can increase the risk of consumer accounts being compromised if fraudsters are able to access sensitive account information and PII. Other concerns stem from the vulnerabilities specific to a particular mobile OS. The most well-known mobile device operating systems in the U.S. include: Apple iOS, Google Android, RIM BlackBerry, Nokia

[48] Users can jailbreak or root some mobile devices, which allows them to install another mobile OS or unlock restricted applications.
[49] Data from Tencent Study as cited in Lucic, K. (2014, Nov. 13). Over 27.44% users root their phone(s) in order to remove built-in apps, are you one of them? *AH Android Headlines.* Retrieved from http://www.androidheadlines.com/2014/11/50-users-root-phones-order-remove-built-apps-one.html.

Symbian, and Microsoft Windows; although iOS and Android represent over 90 percent of the market.[50] The level of vulnerability to jailbreaking or rooting, malware or virus, MiTB, or mobile app compromise depends on how these OS environments are controlled.

Mobile Apps versus Mobile Browsers

Differences in how security controls are applied for mobile apps and mobile browsers can create additional risks.

Mobile apps can incorporate more security features and collect more information about the mobile device to supplement the payment transaction data than mobile browsers are able to do. The data required from a consumer when downloading an app varies depending on the mobile device OS and the merchant app requirements.[51] For example, before a merchant app is installed on an Android mobile phone, Android requests user permissions to collect information such as identity, location, phone log, photo files, camera, WiFi connection, device ID, and call information. Apple does not request these permissions from consumers when they install iOS. Instead, the iOS app requests permissions when it is first used or when a particular permission is first required (e.g., GPS, photos, calendars, contacts, microphone, etc.).

Google and Apple also manage their Android and iOS app stores (Google Play and Apple App Store) differently. Apple closely controls its app store, fully vetting new apps before making them available to customers, not providing APIs to developers[52] (to prevent widespread malware infection of iOS users), and immediately suspending a suspicious app. Conversely, Android is a more open and flexible system that allows installed mobile apps from third party sources, but bears the risk that they may be fraudulent or contain malware.[53]

To prevent consumers from downloading spoofed mobile apps, the app stores and owners of the mobile operating systems issue guidelines and developer frameworks that leverage industry security standards, as well as requirements that app developers must follow to test the security of their mobile apps. However, issuing guidelines does not guarantee compliance; this activity is self-regulated, particularly with the Android platform. Mobile payment apps that collect sensitive information (e.g., name, address, payment credentials) must have the appropriate level of security (e.g., encryption and tokenization) to store and transmit that information.

Mobile browsers generally offer a more ubiquitous consumer experience than mobile apps because consumers can use the default browser on a mobile device. Mobile browsers do not require users to apply updates to the browser to use new mobile devices and OS versions, unlike mobile apps, which prompt the user to initiate app updates.[54] However, mobile-enabled websites rely on internet security protocols which expose websites to the same vulnerabilities as desktop/PC-based browsers – malware attacks, spoofing, eavesdropping. These attacks can lead to malware penetration of the mobile device and instances where a

---

[50] Microsoft's Windows 8 functions as a traditional PC OS and a mobile OS.
[51] While an OS will require consumer permissions, an app may also require permissions, such as geolocation for a taxi service.
[52] In June 2016, Apple announced that it would open just its Siri platform to third party developers.
[53] While Google has installed automated malware/virus scanners and conducts random reviews of submitted applications to its app store, evidence suggests that Android is the most vulnerable mobile platform, targeted by 96 percent of mobile malware attacks. Verizon. (2016). *2015 Data Breach Investigations Report*. Retrieved from http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report_2015_en_xg.pdf.
[54] Iovation (2015). *Fighting Mobile Fraud: Protecting Businesses and Consumers from Cybercrime.* Retrieved from https://s3.amazonaws.com/content.iovation.com/white-papers/PDF/iovation-mobile-fraud-white-paper.pdf.

consumer's login and PAN could be compromised, as noted earlier. Therefore, strong security controls must be applied to these mobile websites to minimize risk.

Several types of risk are assessed for the integration of mobile device/OS across the use cases: mobile device jailbreaking or rooting, lost or stolen device, and malware or virus. The possible impact of mobile device and OS integration on each of the use cases varies in terms of whether the mobile wallet solution is cloud-based or device-dependent as with the Pay wallet models.

5. USE OF THIRD PARTY PROVIDERS

While there are many types of third party providers in the payments industry, this whitepaper includes only those that access data needed to provide operations and technical support, processing, and other functions specifically for the mobile wallets included in the use cases.[55] Mobile wallet providers interact with device manufacturers, MNOs, technology solution providers, card networks, OS providers, developers, and app stores. Not all third party providers address vulnerabilities consistently or effectively, and those that handle consumer payment credentials or PII may pose risks to merchants, PSPs, and WSPs, as evidenced by numerous data breaches in recent years – some through third party providers. A 2014 Ponemon Institute study shows that third party error has the greatest impact on the capital cost of a data breach, with 65 percent of companies that reported sharing customer data with a partner also reporting a subsequent breach through that partner.[56] This underscores the importance of closely monitoring and managing third party providers.

To the extent that third parties contribute to data breaches that impact payment data, some best practices for CNP payments may be gleaned from available guidelines and requirements, such as the Federal Financial Institutions Examination Council *FFIEC IT Examination Handbook*[57] and the Office of the Comptroller of the Currency (OCC) guidance on third party risk.[58] The Payment Card Industry Security Standards Council (PCI SSC)[59] also issued the *Information Supplement: Third-Party Security Assurance for Standards Version 3.2*[60] and the *PCI Data Security Standard (DSS) E-commerce Guidelines*,[61] which includes a section that addresses risk associated with outsourcing to third party providers. This extensive guidance highlights the importance of having a strong third party risk management program.

---

[55]Some stakeholders may have interdependencies. For example, a PSP or merchant may rely on another business to provide authentication, fraud management, cloud storage, or token management services.

[56]Ponemon Institute. (2014, May). *2014 Cost of a Data Breach Study.* Retrieved from http://www-935.ibm.com/services/multimedia/SEL03027USEN_Poneman_2014_Cost_of_Data_Breach_Study.pdf.

[57] Federal Financial Institutions Examination Council (2016, April 29). *FFIEC Examination Handbook: Appendix J: Strengthening the Resilience of Outsourced Technology Services*, pp. J-16. Retrieved from http://www.ffiec.gov/press/PDF/FFIEC_Appendix_J.pdf and *Appendix E: Mobile Financial Services* https://www.ffiec.gov/press/PDF/FFIEC_booklet_Appendix_E_Mobile_Financial_Services.PDF.

[58] U.S. Office of the Comptroller of the Currency. (2016, Spring). *Semiannual Risk Perspective from the National Risk Committee.* Retrieved from http://www2.occ.gov/publications/publications-by-type/other-publications-reports/semiannual-risk-perspective/semiannual-risk-perspective-spring-2016.pdf and (2013, Oct. 30). *Bulletin 2013-29: Third-Party Relationships.* Retrieved from *http://occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html*.

[59] The Payment Card Industry Security Standards Council (PCI SSC) is an open global forum responsible for the development, management, education, and awareness of the PCI security standards including the Data Security Standard (PCI DSS), Payment Application Data Security Standard (PA-DSS), and PIN Transaction Security (PTS) requirements. For more information, see https://www.pcisecuritystandards.org.

[60] PCI SSC (2014). *Information Supplement: Third-Party Security Assurance*. Retrieved from https://www.pcisecuritystandards.org/documents/PCI_DSS_V3.0_Third_Party_Security_Assurance.pdf.

[61] PCI SSC (2013, Jan.) *Information Supplement: PCI DSS E-commerce Guidelines*. Retrieved from https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_eCommerce_Guidelines.pdf.

It is the responsibility of the merchant, PSP, and WSP to know which third party providers have access to customer data and how that data is secured.

B. USE CASE COMPARATIVE ANALYSIS

This section briefly describes each use case, followed by an assessment of the risks associated with account creation, EMV ID&V, authentication, mobile device and OS integration, and use of third party providers.

USE CASE 1: GUEST CHECKOUT WITH NO CARD ON FILE[62]

MoovWeb found that the majority (66 percent) of the top 100 retailers offer guest checkout, which does not require a consumer to create an account with an online merchant to complete a purchase; while the other one-third (34 percent) of retailers require their customers to create an account.[63] The Moovweb analysis also found that guest checkout is preferred by many shoppers not only for the convenience and speed, but also because it does not require the consumer to login, or store payment credentials or PII with the merchant for future use or to track shopping behavior. Furthermore, smartphone shoppers are 1.2 times as likely to select guest checkout rather than opting to log in.

The mobile browser and mobile app guest checkout processes are similar. However, to checkout using a merchant's mobile app, the consumer must first download the app to his mobile phone. Both methods request similar information from the consumer to complete a purchase: name, billing address, shipping address (if different), phone number, rewards information, and the payment method. For credit card purchases, a consumer must enter the PAN, expiration date, and card verification code (CVC)[64] (not always required depending on merchant site configuration). During the transaction process, the merchant may use tools such as an address verification service (AVS)[65] to confirm that the address matches an address on file with the issuer.

Account Creation. Fraud resulting from account creation is not applicable to guest checkout because the consumer does not create an online account or establish login credentials with the merchant and no PANs or PII are stored on file. If the PAN remains in the clear (i.e., not encrypted) while the consumer enters it into the mobile app or browser during guest checkout, it could be intercepted. Most large merchants[66] encrypt the payment data during the transaction process and some replace the PAN with a security token on the backend for storage, either via a merchant acquirer or using a proprietary system. Merchants have an incentive to implement the most reasonably secure methods possible in the context of

---

[62] See Appendix B – Use Case 1: Guest Checkout with No Card-on-File.

[63] Based on MoovWeb's analysis of the Internet Retailer Top 500 database. Salvesen, A. (2016, March 31). *The Truth about Guest Checkout*. [blog]. Moovweb. Retrieved from http://www.moovweb.com/blog/the-truth-about-guest-checkout/.

[64] Card networks vary in their definitions of the card verification code depending on whether it refers to the static magnetic stripe data, the static data on the back of a credit/debit card, or the dynamic code generated by an EMV chip (AmEX–Card Security Code/CSC; Discover–Card Identification Data/CID; MasterCard–Card Verification Code/CVC/CVC2; and Visa–Card Verification Value/CVV/CVV2). This paper collectively refers to this value as the card verification code (CVC).

[65] Address verification services (AVS) verify a consumer's billing address with data on file with the issuing bank. Only the house number and zip code of the billing address entered are compared to the billing address on file for the card. A U.S. Postal Service database and verification services by other technology providers can be used to confirm the authenticity of the complete address.

[66] PCI SSC outlines four tiers of merchants and this study considers tiers 1 and 2 to be "large" merchants. Tier 1 merchants process over 6 million credit/debit card transactions annually through all channels (CP, CNP, e-commerce). Tier 2 merchants process 1–6 million credit/debit card transactions annually through all channels (CP, CNP, e-commerce).

their business as they are responsible for all fraud related chargebacks. Although encryption of payment card data over open, public networks is a PCI DSS requirement, not all merchants comply.[67]

Merchants are exploring tools (e.g., software development kits (SDKs)) that tag the customer and capture the device ID to give them more visibility into the guest checkout. Alternatively, some industry experts recommend that merchants eliminate the guest checkout option and require customers to register and create accounts in order to collect more fraud prevention data. However, merchants worry that not offering guest checkout could result in lost sales, since as noted earlier consumers currently have a strong preference for the guest checkout option.

Guest checkout is vulnerable to data breach and malware/virus when a consumer enters a PAN and PII to pay for a transaction. The probability of risk for each attack, via mobile browser or mobile app, is medium because a fraudster could capture the PAN and PII if the data being entered by the consumer is not encrypted. Also, the first attempted fraudulent transaction with a stolen PAN may go undetected by merchant fraud systems. However, the magnitude of risk is low for both types of risk because: (1) no account or login credentials are created with the merchant and no PANs or PII are stored with the merchant; (2) malware or virus would need to penetrate many consumers' mobile phones and individual merchants to carry out a large scale attack; and (3) the PAN becomes less valuable to fraudsters with EMV chip card issuance, which limits the shelf life of a magnetic stripe issued PAN. The probability and magnitude of risk may increase for smaller merchants that lack the proper tools or resources to respond to these types of attacks.

Authentication for Guest Checkout is more difficult for merchants to perform than authentication of customers who have established online accounts and login credentials. Therefore, the merchant must use other risk management methods, such as AVS, check digit,[68] and any data about the purchase to verify the customer before processing the transaction. More large merchants are beginning to use device ID for additional authentication, which help track specific details about the phone to check for any previous association with fraud. Larger merchants may create a security token for the first guest transaction and use it with other information (e.g., basket items, IP address), to identify a returning guest and distinguish between legitimate and suspicious customers. The associated risks from mobile MiTM/browser or spoofed authentication do not apply to the authentication function for this use case, since merchants employ other risk management methods to help identify a legitimate customer.

Integration of the Mobile Device/OS exposes Guest Checkout to several risks. The risk of rooting/jailbreaking is medium to high. A rooted/jailbroken device diminishes existing mobile OS security controls, which could allow malware to compromise PAN/PII entered through a mobile browser or mobile app. However, across all the use cases, most merchants, PSPs, and WSPs use certificate validation of mobile browsers and mobile apps to ensure that the browser session or app is authentic and has not been hijacked. If the person using the mobile device is not the owner (device was lost or stolen), the risk of gaining access to consumer data and making a successful guest checkout purchase is high. Malware or

[67] PCI DSS Requirement 4.1 specifically requires merchants to use encryption to protect stored data and the transmission of cardholder data and sensitive information across public networks (this includes Internet). PCI SSC recently issued new requirements for stronger encryption to transport layer security (TLS) versus secure socket layer (SSL) based on the number of security vulnerabilities associated with SSL encryption. Some browsers and servers are still using old, outdated versions of these standards.

[68] Check digit uses a pop-up window to notify a customer of the incorrect entry of a PAN. It does not validate the legitimacy of the PAN, only that the account number structure is correct.

virus could direct a consumer to a spoofed mobile website or app and capture the consumer PAN and PII entered during the checkout process. The magnitude of risk is low for all of these attacks for the same reasons described for account creation and authentication.

Use of Third Party Providers for Guest Checkout may help merchants integrate the guest checkout function into their mobile browser or mobile app, or operate the mobile browser or mobile app interface that captures consumer payment data. The probability of data breach is medium because of reliance on a third party to protect the consumer PAN and PII. The magnitude of risk is high because the third party provider for a guest checkout service may have broad reach in the industry (e.g., support multiple merchants) and a breach could impact many devices and customers.

USE CASE 2: MOBILE IN-APP WITH EMV ID&V[69]

This use case represents the Pay wallet models that leverage EMV ID&V for e-commerce payments. Use of EMV payment tokenization distinguishes these "in-app" payments from purchases made directly from a merchant's native mobile app or PSP mobile app.

Account Creation for Mobile In-App with EMV ID&V requires consumers to enroll a PAN with the Pay wallet prior to conducting a transaction. The WSP passes this information to the card issuer to perform EMV ID&V before provisioning[70] a payment token in lieu of the PAN to the wallet. During creation of the wallet account, the PAN is encrypted and transmitted to the token service provider (TSP).[71] Whether a consumer is prompted to create a WSP account when he purchases and activates the mobile device, or he activates the wallet later, the process remains the same. However, industry stakeholders that support the Pay wallets generally trust an aged device more than a new one. A mobile device owned by the user for a while provides an account history with an issuer, and is considered a "tenured channel."

The probability and magnitude of risk from malware/virus, account takeover, or mobile device-porting fraud compromising the Pay wallet account creation process are all low because the PAN is encrypted and not captured or stored with the wallet provider. If malware or a virus resides on a mobile device when the account is created and is able to penetrate the secure area where the token is stored, it still cannot access the PAN. Also, the subsequent EMV ID&V and token provisioning process will ensure that only payment tokens are stored on the mobile device. If compromised, payment tokens have no value without the accompanying dynamic cryptogram generated for each transaction.

EMV ID&V for Mobile In-App is subject to social engineering. Fraudsters attempt to create a mobile wallet with stolen payment card credentials by manipulating an issuer's call center customer service representative (CSR) to inadvertently divulge enough confidential customer information that enables the fraudster to convince the CSR that he is the legitimate cardholder and can make changes to the account.[72]

---

[69] See Appendix B – Use Case 2: Mobile In-App with EMV ID&V.

[70] See Crowe et al. (2015, June). *Is Payment Tokenization Ready for Primetime: Perspectives from Industry Stakeholders on the Tokenization Landscape?*

[71] The EMV spec defines a token service provider (TSP) as an entity that provides a token service comprised of the token vault and related processing.

[72] Early implementations of Apple Pay resulted in some instances of call center fraud during the ID&V process. Fraudsters were able to provision stolen payment credentials to Passbook Wallets. The largest issuers were targeted but the vulnerability has since been addressed by the FIs putting stronger ID&V processes into place.

To address this risk, the card networks require issuers to use at least two of the following step-up authentication methods as part of the EMV ID&V process:

> **(1) Call centers**. Consumers are directed to an issuer's call center to provide additional information when stepped-up authentication is required because the payment card being provisioned appears suspicious or cannot be verified without additional information.
>
> **(2) One-time password (OTP)**. To use OTP for stepped-up authentication requires the issuer to know the consumer's email address or mobile phone number. Concerns exist that fraudsters could use malware to intercept OTPs sent via text or email.
>
> **(3) App-to-app authentication**. This method requires the consumer to log in to his mobile banking app for verification and link payment credentials to a mobile wallet.[73]

To provide an additional layer of security and ensure that the legitimate cardholder requested provisioning the card to the wallet, the issuer will notify him via email, text, or regular U.S. mail. If the consumer did not initiate or is unaware that provisioning occurred, he can contact the issuer to have the token suspended or deleted.

Authentication for Mobile In-App with EMV ID&V with a Pay wallet requires the consumer to use a fingerprint or passcode/PIN to authenticate to the mobile device. A fingerprint could be spoofed or a PIN/passcode compromised, but both the probability and magnitude of risk are very low because of the complexity involved to make this attack successful. The fraudster must steal the user's phone (versus having access to a file of payment credentials), unlock the phone (if locked), have knowledge of the PIN/passcode or create a spoofed fingerprint, and make transactions before the phone is reported lost or stolen. Also, as part of the authentication process, issuers can leverage their existing fraud engines to detect changes in customer behavior patterns to block suspicious transactions (e.g., transactions from opposite sides of the U.S.). Mobile authentication tools such as device ID and geolocation (used by the issuer) provide data to recognize and decline suspicious transactions, while other tools such as remote wipe (requested by the consumer after discovering his phone is lost or stolen) can limit the loss.

Integration of Mobile Device/Operating System for Mobile In-App with EMV ID&V has both a low probability and magnitude of risk because the mobile wallet applet is stored in a secure location in the mobile device and protected from any breach to the device or OS.

Use of Third Party Providers for Mobile In-App with EMV ID&V also has a low probability and magnitude of risk because these models operate within a tightly controlled environment under the EMV spec, which governs the relationship between various stakeholders (e.g., token requestors,[74] TSPs, issuers, acquirers, other networks, etc.). The technical interfaces between these parties are based on common rules and specifications. For the mobile in-app solution, the Pay WSPs offer APIs to the e-commerce merchants that want to accept "Pay" wallet solution via their shopping carts.

---

[73] The transaction is identified as a network credit and reversal. The user may be instructed to find a code in her mobile banking app (e.g., a pending authorization for $.04) and verify the amount. The card network, acting as the merchant, sends the authorization to the issuer and then reverses the transaction within a specific timeframe.

[74] For example, Apple Pay, Android Pay, and Samsung Pay.

USE CASE 3: CLOUD-BASED WALLET USING OTHER AUTHENTICATION APPROACHES[75]

This use case includes two cloud-based wallet models. In the first model, the consumer creates a PSP wallet account (e.g., Pay with Amazon or PayPal) and enrolls a payment method. To make a purchase through a PSP, the consumer selects that wallet option on the participating merchant's mobile website or mobile app and then logs in to the PSP to complete the purchase. In the second model, the consumer creates an account with a merchant and enrolls a payment CoF for future purchases.

Most PSPs and large merchants require the consumer to create a username (e.g., email) and password (which is encrypted) to initially establish and subsequently login to the account. The PSP may also ask the consumer to select and create responses to knowledge-based security (challenge) questions that can be referenced when additional authentication is needed because of a forgotten password, suspicious transaction, or unrecognized device, for example. The first time the cardholder uses either wallet, he authenticates with the login credentials. The PSP or merchant matches the accountholder's name to the payment card on file to ensure it belongs to the cardholder and to verify that the transaction is legitimate. The PSP or merchant may also ask for the CVC to determine if the cardholder has the physical credit or debit card, and perform AVS for further authentication.

The PSP or merchant acquirer sends the PAN, expiration date, and purchase amount in an encrypted format to the card network/issuer to process a payment. The issuer validates the information and returns the authorization response (approval or decline) to the PSP or merchant acquirer via the card network.

Account Creation for Cloud-based Wallets Using Other Authentication Approaches requires the consumer to provide payment credentials, PII, and a username and password. The probability of risk is high for data breach, malware or virus, account takeover (ATO) and new account fraud. The probability of data breach or malware/virus occurring could be high because the data valuable to fraudsters is concentrated (e.g., PANs, PII, login credentials), unless this data is encrypted. The probability of ATO and new account fraud are high because fraudsters can leverage previously compromised account usernames and passwords to log in to consumers' online merchant or PSP accounts and use the PAN stored in the wallet account on file (i.e., CoF) to make purchases. Alternatively, fraudsters can open new PSP or online merchant wallet accounts with stolen PANs and PII and make fraudulent purchases. The magnitude of risk is medium across these types of attacks because, in most cases, the data is encrypted, and the attack is limited to the single merchant or PSP website or mobile app where the consumer account was created.

Authentication for Cloud-based Wallets Using Other Authentication Approaches requires a consumer to log in with a username/email and password to authenticate to the merchant or PSP for the first time, which then creates a tenured channel through which the PSP or merchant can determine the level of risk for each subsequent transaction. The PSP or merchant will perform risk modelling using customer profile information, behavioral analytics, and transaction monitoring (including IP address, device ID, and geolocation) and other authentication methods. If additional authentication is needed for future

[75] See Appendix B – Use Case 3: Cloud-based Wallets Using Other Authentication Approaches.

transactions, the PSP or merchant can perform the authentication without issuing an explicit challenge to the customer.

Well-established PSPs and larger merchants may use proprietary risk engines to analyze data, building on successive customer interactions in the CNP environment to develop an internal risk score that determines the level of risk and whether to allow, challenge, or decline a transaction.[76] Using sophisticated risk management and fraud prevention tools, these PSPs and merchants can track a broad range of proprietary and transaction data, such as what a typical transaction for that customer looks like, average shopping cart size/items, historical purchase data, and login behavior. If the transaction is identified as high risk, the PSP, merchant, or issuer can present a security challenge question to the customer, or use historical transaction data, or other authentication methods (e.g., 3DS), to verify the cardholder. Using 3DS 2.0, a PSP or merchant with insufficient data to challenge the customer can ask the issuer to perform additional risk analysis based on previous customer behavior and determine whether the transaction is low or high risk, and if high, offer the merchant an issuer-based challenge to the consumer.

This model is vulnerable to both MiTM and spoofed authentication attacks because the consumer must use login credentials or another form of authentication (fingerprint) to authenticate himself to his account and the merchant or PSP before completing a transaction. The probability and magnitude of risk for these attacks are low if the PSP or merchant encrypts and tokenizes the payment credentials. Out-of-band authentication can also be used to thwart an attack by confirming the identity of the customer. Spoofing is also a low probability because PSPs and larger merchants can use their risk management tools to authenticate the consumer. Malware used to perform a spoofing attack would need to penetrate a large number of mobile devices with stolen login credentials and PANs from many PSPs and merchants. However, the probability and magnitude of risk would be high for PSPs and merchants that only rely on username and password for customer authentication.

Integration of Mobile Device/Operating System for Cloud-based Wallets Using Other Authentication Approaches has the same risks as Use Case 1: Guest Checkout.

The probability of jailbreaking or rooting a mobile device is medium because a jailbroken device diminishes the existing security controls in the mobile OS, which could allow malware to compromise the wallet account. However, the magnitude of risk is low because sophisticated PSPs and larger merchants have tools to help recognize and prevent the use of a rooted or jailbroken device and no payment credentials or PII are stored on the device.

The probability of fraud occurring from a lost or stolen device is high if the mobile device and payment applications are not well-protected (i.e., weak passwords increase the risk that a fraudster can access the wallet and make purchases with the payment credentials already stored on file in the wallet). However, the magnitude of risk is low because the consumer can remotely wipe the device or disable or close an account with a PSP or merchant. A PSP or merchant can also disable or freeze activity on a consumer's account if a device is reported lost or stolen.

[76] These risk management practices are proprietary, although their terms and conditions or user agreements may describe how the PSP/merchant collects the data to help with authentication and identification.

The probability of risk for malware or virus penetration is high because it can potentially locate PANs and PII when a consumer logs in to a PSP or merchant account. However, wallet providers in this use case encrypt the data, making this a low probability of risk. The magnitude of risk is low because a successful compromise would require a large-scale attack on mobile phones and access to consumer login credentials, PANs, and PII.

Use of Third Party Providers for Cloud-based Wallets Using Other Authentication Approaches is similar to other cloud-based wallet models. These wallets may also depend on third-party relationships to manage various aspects of the payment transaction (e.g., shopping cart interface), requiring the wallet provider to grant access to payment credentials and other sensitive information. However, not all cloud-based wallet providers have strong third party risk management practices in place, exposing them to potential compromises. The probability of risk from a third party breach is low for PSP or large merchant cloud-based wallets (e.g., Amazon, PayPal) because they have sophisticated third party management and compliance programs, as well as legal agreements that govern relationships with app developers and merchants that accept their wallets. The magnitude of risk is high because a third party breach could compromise a significant amount of customer data and impact a large number of mobile devices.

USE CASE 4: CARD NETWORK DIGITAL WALLET (THE "CHECKOUTS")

AmEx, MasterCard, and Visa offer digital wallet or digital acceptance services to merchants and issuers. Merchants can add these digital wallet payment options to their mobile browser or mobile app checkout carts. Consumers enroll in a digital wallet service so they do not need to enter their payment credentials on a participating merchant's mobile website or app to make a purchase. The card networks request similar information from consumers to enroll in a digital wallet, with one exception. AmEx Express Checkout is only available to customers with an online account issued on americanexpress.com.[77]

Account Creation for Card Network Digital Wallets varies by card brand. These wallets take slightly different approaches to consumer account creation and enrollment.

The Express Checkout account creation process is automatic for customers who opt-in. It uses the same login credentials the customers established for their online accounts with americanexpress.com, which adds more security from prior issuance, vetting, and verification. Prior to the customer's first Express Checkout transaction, AmEx sends an OTP to the customer via email or SMS.

Consumers can enroll in Visa Checkout or Masterpass directly on the wallet website or mobile app, or through a merchant, issuer, or partner service provider directing them to the wallet during the checkout process. Both wallets are also integrated with some issuers that allow their customers to enroll using their online/mobile banking platform. Because these wallets are card brand-agnostic, consumers can add any eligible credit or debit card associated with a major card brand. Enrollment requires the consumer to provide his first and last name, email address or mobile phone number, and a password. Once the consumer has been verified, he adds other personal information and payment credentials to the account, either manually or by using the mobile device camera to scan the payment card, although the CVC must be entered manually. During enrollment and purchase, the wallet providers verify the email and billing address and

[77] Customers with AmEx cards issued by other financial institutions are not eligible to enroll in Express Checkout.

collect mobile device data, such as device ID or IP data checks.[78] Other risk management tools include velocity checks, issuer CVC verification, account monitoring or enrollment attributes, transaction history, and proprietary fraud tools. The consumer may also be asked to select security questions and answers. Enrollment is confirmed with an email.

Masterpass provisions a payment token to the wallet through the issuer, so the token is passed in lieu of the PAN for these wallet purchases. The issuer decides whether stepped-up authentication (e.g., OTP) is necessary before provisioning the token to the Masterpass wallet. Visa Checkout plans to add this feature in the near future, and currently passes the encrypted PAN with the transaction. Both networks also have robust risk management systems to monitor cardholder and account behavior for anomalies to prevent fraud.

The probability of risk is "medium to low" for attacks resulting from data breach, malware or virus, and account takeover fraud during account creation. The actual risk of data breach occurring is low because these files are built on a rigorous architecture supported by the major card payment networks with high standards for data protection. However, some industry stakeholders consider data breach risk to be high because of the concentration of valuable data, and fraudsters continue to search for weak links to breach the files. Therefore, assigning a "medium to low" probability of risk acknowledges that card network wallet providers must be vigilant about maintaining high standards of data protection.

The probability of malware or virus risk is also "medium to low." The card networks use multi-layered security and malware controls to prevent the compromise of login credentials and encrypt the payment credentials during account creation. However, if the card networks do not also tokenize the PAN, the risk increases.

The magnitude of risk for data breach and malware or virus is low because payment credentials are encrypted, tokenized, and not stored on a mobile device.

Account takeover fraud risk is "medium to low" because while passwords may be vulnerable to compromise from an ATO attack, these wallet models perform additional validation at the mobile device level to limit this risk. The magnitude of risk for ATO fraud is low because this attack affects only one consumer account and card networks have step-up authentication mechanisms in place.

The probability of new account fraud occurring is medium because fraudsters can use payment credentials obtained from a previous data breach to create new digital wallet accounts. However, the magnitude of risk is low because of card network controls to manage higher risk transactions, robust controls integrated with issuer systems to limit new account fraud, and limited merchant acceptance of these wallets today.

[78] Internet Protocol (IP) data checks identify an Internet user's geographical information, including: country, region, city, latitude and longitude, zip Code, internet service provider, and domain name.

Authentication for Card Network Digital Wallets also varies slightly by card brand in the approach.

A consumer authenticates to the Express Checkout wallet using the same login credentials established for his americanexpress.com account. If additional authentication is needed, AmEx will send an OTP to a tenured channel (email or SMS) for each purchase, and may also use device information to match the device being used for the transaction to a tenured device already linked to americanexpress.com or the AmEx app.

Visa Checkout first authenticates the consumer when he enrolls payment credentials in the digital wallet (e.g., with an OTP sent to email or SMS). When making a purchase the consumer authenticates to the wallet with a username/email and password, but layered authentication methods such as device ID, geolocation, or behavioral analytics are also applied without involving the customer. Prior to approving each purchase, Visa Checkout uses device fingerprinting and proprietary dynamic network analytics scoring to authenticate the customer and reduce the risk of fraudulent transactions. Masterpass follows a similar process but authenticates the payment token in the consumer's wallet. One benefit of authentication with a card network digital wallet is that the consumer has already been vetted via the card network and the issuer.

The probability and magnitude of risk associated with a MiTM/MiTB or spoofed authentication attack are both low for the digital wallets because card networks use robust risk management systems to monitor cardholder and account behavior for anomalies to prevent fraudulent attacks.

Integration of Mobile Device/ Operating System for Card Network Digital Wallets is subject to the same risks of jailbreaking or rooting, lost or stolen device, and malware or virus as with Use Cases 1 and 3 because these wallets function within a cloud-based environment, which has a higher probability of risk than a device- or hardware-based environment as with Use Case 2. However, the probability of these types of risks occurring is low. They can be mitigated by the card networks with tools to: (1) recognize and restrict the use of a jailbroken or rooted device; (2) collect information about the mobile device type and OS; and (3) detect a lost or stolen device because it is quickly reported by a consumer or by detecting anomalies of device behavior. Risk is also mitigated because payment credentials are not stored on the mobile device.

Use of Third Party Providers for Card Network Digital Wallets has a different risk profile than other models because the card network is the sole provider of the wallet service and controls the integration with merchants and issuers. A card network may have a third party relationship with developers that provide SDKs and open APIs that request open access to a card network's underlying payment capabilities. These models may also use a combination of proprietary and third party solutions to implement transaction fraud checks. For these reasons, the probability and magnitude of risk from the use of third party providers are both low.

V. MOBILE CNP SECURITY CONTROLS AND METHODS

Several security controls and methods are prevalent for managing fraud in the mobile CNP fraud. While many of these controls exist in the traditional e-commerce CNP environment, the industry is still adapting the necessary controls to manage the m-commerce channel.

Authentication

Authentication in the CNP channel has always been a challenge and the industry continuously seeks stronger solutions. While MFA is promoted as a best practice in the industry, merchants have shown reluctance to impose additional layers of security for fear of inconveniencing the customer and increasing transaction abandonment. Examples of MFA include push notification to the user, OOBA verification code (email, SMS), one-time password (OTP), and responding to dynamic KBA questions. Payment service providers, WSPs, merchants, and issuers may send alerts via text or email to notify customers of suspicious transactions or respond to parameters established by the customer following completion of a transaction.

The use of fingerprint authentication for mobile payments is a recent development that has gained traction through the Pay wallets. Globally, approximately 50 percent of smartphones sold by 2019 are expected to integrate an embedded fingerprint sensor, and the number of fingerprint sensors embedded in devices is projected to grow from 499 million in 2015 to 1.6 billion units in 2020, according to market research firm IHS.[79] The near future may provide more opportunities to use voice, iris, and facial recognition authentication.

Information gleaned from a mobile device is the most popular choice for layered authentication of mobile payments. Knowing the device ID is important for analyzing device attributes and anomalies. Out-of-band authentication uses the consumer's mobile phone number (obtained during registration) for additional verification via another channel (e.g., text, voice call); and strong KBA is an effective method to layer onto device ID techniques. One common practice among PSPs and merchants is to authenticate CNP consumers with AVS and CVC, although such information can be easily obtained by a fraudster.

Dynamic Cryptograms

A dynamic cryptogram is generated using a symmetric key that is validated by the party that shares the key with the cardholder's device for each mobile CNP transaction. *Mobile in-app* wallets that use an EMV payment token pair the token with a dynamic cryptogram that is passed with each mobile transaction. Each Pay wallet has a customized approach for generating the cryptogram and managing the keys. The iOS model generates a dynamic cryptogram using keys stored on the SE in the mobile device. The Android model employs limited use and single-use keys[80] stored either in a secure area of the OS or in the TEE on the mobile phone. Because HCE does not use an SE, AmEx, Visa and MasterCard HCE specifications require the use of additional software security tools such as white-box cryptography to prevent hackers from trying to identify keys stored in the mobile OS or TEE.

[79] Boustany, M. and Fox, J. (2015, Dec. 18). *Fingerprint Sensors in Mobile Devices Report – 2016.* Available for purchase at https://technology.ihs.com/523369/fingerprint-sensors-in-mobile-devices-report-2016?utm_campaign=PR_fingerprint_sensors_mobile_dev-001&utm_medium=press_release&utm_source=Newsroom.

[80] Visa uses limited use keys (LUKs) and MasterCard uses single-use keys (SUKs).

The types of cryptograms used to support mobile payment apps for cloud-based digital wallets (vs. mobile in-app with EMV ID&V) are not dynamic and are primarily used to encrypt data and ensure secure communications between the mobile app and the back-end server handling the transaction.

Encryption

Encryption is the process of encoding data using algorithmic schemes (keys) to transform plain text information (i.e., the PAN) into a non-readable form, rendering transaction information useless if intercepted by fraudsters because the data cannot be decoded.[81] Nowhere is the value of encryption more apparent for payment transactions than with online merchants because a secure encryption protocol protects customer data in-transit during the payment process.

In a 2014 Ponemon Institute study, 4,800 IT managers were interviewed in ten countries, half of which stated that they invested in encryption to lessen the impact of data breaches.[82] The study noted that the use of encryption has doubled, with 34 percent of organizations now utilizing it extensively, and FIs representing 43 percent of those respondents. A key observation from the study was the recognition that encryption use should be much higher than it is, but the complexity and expense to implement encryption key management is the main barrier to more widespread adoption.

PCI DSS requires merchants to encrypt cardholder data and sensitive information during transmission across public networks and when stored. Because of the number of security vulnerabilities associated with Secure Socket Layer (SSL) encryption in recent years, PCI SSC recently issued new requirements for stronger encryption to Transport Layer Security (TLS). However, some browsers and servers still use outdated versions of these standards.

Payment and Security Tokenization

Tokenization removes payment credentials from the clear by replacing the actual payment account number with a randomly generated value, known as a token, in the same format as the 16-digit PAN.

Payment tokenization replaces the PAN with a token when the consumer enrolls in a wallet solution. When the consumer initiates a mobile payment (at POS or CNP) using a Pay wallet or other CNP wallet (e.g., Masterpass, and PayPal in the near future), the payment token is used in lieu of the PAN in the transaction message. The payment token represents the PAN during the entire transaction, except when it is passed between the TSP (e.g., card network) and the issuer for authorization and can only be de-tokenized and re-tokenized by the TSP.

The use of payment tokenization is considered a strong security solution because it eliminates the need for the PAN to be transmitted in the clear to the merchant acquirer during the transaction and follows standard formats and practices established in the proprietary EMV spec. PCI SSC also has issued *Additional Security*

[81] Many types of encryption processes are available, including Format Preserving Encryption (FPE), Triple Data Encryption Standard (3DES) and End-to-End Encryption (E2EE), that all work to thwart data breaches. (Verifi, 2015).

[82] The Ponemon Institute. (2015, April) *2015 Global Encryption and Key Management Trends Study*. Sponsored by e-Thales Security. Available for download at https://www.thales-esecurity.com/company/press/news/2015/april/2015-global-encryption-and-key-management-trends-study-release (registration required).

Requirements and Assessment Procedures for Token Service Providers (EMV Payment Tokens), Version 1.0.

Security tokenization is a proprietary process developed by the merchant, processor, or PSP to protect data stored (data-at-rest) or used post-authorization. Security tokens are substitute values that replace the underlying sensitive data (i.e., PAN).[83] Merchants and PSPs use security tokens instead of PANs to reduce cardholder data stored in their systems, decrease fraud exposure, and reduce their PCI DSS compliance burden. Security token schemes are not consistent, but there are some industry efforts to move them closer to uniformity. PCI SSC has issued *Tokenization Product Security Guidelines* for evaluating tokenization products that replace the PAN with a security token.[84] ANSI X9 is developing standards to support implementation and security requirements for post-authorization security tokenization systems.

3D–Secure 2.0

3-D Secure is a messaging protocol that enables consumers to authenticate themselves with their card issuer when making an online purchase. It was initially created to accelerate the growth of e-commerce by reducing fraudulent use of cards online and to protect the merchant from exposure to fraud-related chargebacks. It is built on a three domain structure that includes the merchant/acquirer domain, issuer domain, and interoperability domain.

Although available for several years, 3DS adoption in the U.S. has been very low. The original 3DS 1.0 version required the merchant, issuer, and consumer to subscribe to the service and required the consumer to authenticate for each transaction invoked by a merchant. This process created customer friction and increased shopping cart abandonment. Despite adoption of 3DS 1.0 in other countries (some mandated), there was a need for improvement. The original 3DS 1.0 only supports cardholder authentication for online browser-based transactions. It does not support newer CNP channels, including in-app, mobile and digital wallets.

The new 3DS 2.0 specification[85] updates the risk management approach by incorporating risk-based elements and delivering expanded capabilities in terms of technology, security (e.g., tokenization), performance, user experience, and flexibility. Unlike the original version, 3DS 2.0 automatically registers all customers with participating issuers, so consumers do not need to enroll to use the service.

3DS 2.0 applies KBA and a risk-based authentication (RBA) approach that allows issuers and merchants to exchange additional risk data, such as device ID and geolocation, at both ID&V and transactional levels. Merchants decide when stepped-up authentication is needed for a higher risk transaction and can invoke 3DS.[86] For example, when a consumer checks out on a merchant's mobile website, the purchase

[83] Security token models for POS and e-commerce have existed since the mid-2000s, driven primarily by the issuance of the PCI DSS in 2004, which defines business requirements for protecting cardholder data. The intent of the PCI SSC *2011 Tokenization Guidelines* and proposed X9 requirements are to use tokens to secure and protect sensitive information (i.e., low value token), not to create a token to replace a payment credential used during a financial transaction (i.e., high value token) and processed over a payment network.

[84] PCI SSC (2015, April). *Tokenization Product Security Guidelines Version 1.0.* Retrieved from https://www.pcisecuritystandards.org/documents/Tokenization_Product_Security_Guidelines.pdf.

[85] *EMV 3-D Secure–Protocol and Core Functions Specification v2.0.0* is available for download at https://www.emvco.com/specifications.aspx?id=299.

[86] 3DS 2.0 risk engine will only challenge transactions that merchants deem medium to high risk.

information, along with device data and other details, is sent to the issuer to authenticate the cardholder and confirm the purchase. The issuer can use RBA to passively authenticate the cardholder or, based on the risk profile, use stepped-up authentication by asking the cardholder to enter an OTP to authenticate himself or respond to a CSR call. A transaction may be considered high risk if the mobile device or laptop does not match one that the customer has used before.

3DS 2.0 will be customizable for issuers as well as merchants. The goal is to enable merchants to have more control over when to invoke 3DS, but issuers will still control the authentication stream because they will continue to own the liability for all 3DS-initiated transactions that they approve. However, merchants will supply more data (e.g., email address, mobile phone number, shipping, billing and IP addresses) to help issuers with authorization decisions.

VI. GAPS AND ISSUES ACROSS USE CASES

The subgroup leveraged its collective expertise and industry knowledge to identify the most vulnerable points of attack across the use cases, including account creation, authentication, and ID&V. Two of these functions (authentication and ID&V) are also considered risk management methods. In addition to analyzing the key vulnerabilities, they identified several gaps and issues related to tokenization approaches, use of end-to-end encryption (E2EE), ID&V approaches, and authentication practices.

A. Tokenization Approaches

Tokenization is an important security control used to protect payment credentials end-to-end in a POS or CNP online or mobile transaction by replacing the PAN credentials with a surrogate value. Not all use cases apply tokenization, and approaches differ. Currently three of the four use cases discussed in this paper use only security tokenization, with the exception of the Pay wallets, which use payment tokens. Some browser and cloud-based CoF models are implementing payment tokens, but because this is a recent development and the subgroup did not analyze the model.

Having two major payment tokenization approaches provides value in terms of enhanced payment security. However, some issues remain before the benefits of both approaches can be fully realized. For cloud-based wallets that use a mobile browser or mobile app, the PAN may be exposed during consumer enrollment unless it is encrypted, until a security token is created to store it as a CoF with the PSP or merchant. Layering robust risk controls on top of security tokenization can prevent the PAN from being compromised. As a best practice, any token solution should ensure that payment data is never stored in clear-text in a mobile app or browser or passed with the transaction.

While some PSPs and merchants have integrated the use of both payment tokens and proprietary security tokens, the integration may not always be a seamless process and requires coordination of the two tokenization approaches. Finally, the market still lacks ubiquity in the implementation of tokenization strategies across the POS, e-commerce, and mobile channels.

B. Use of End-to-End Encryption

End-to-end encryption (E2EE) protects sensitive payment/cardholder data from the point where it is captured or entered by the consumer into the mobile app or mobile browser, through transmission to the web/application, cloud and networks, to the trusted party (e.g., merchant acquirer) that holds the decryption key. If payment data is stolen at any point during the process, E2EE renders the data useless to criminals.[87]

E2EE works in conjunction with tokenization to ensure complete security of cardholder data through the entire transaction lifecycle (whether POS or CNP). With encryption and payment tokenization the PAN is never passed or stored in the clear (unencrypted) by the merchant.

Encryption practices are not consistent across the mobile CNP use cases. For example, it is unclear how many guest checkout sites encrypt the payment credentials as they are being entered by the consumer. As fraudsters shift their focus to the CNP online and mobile channels, this puts the e-commerce merchants at greater risk of data breaches unless they implement E2EE.

Cloud-based use cases that accept payments via a mobile app or mobile browser should leverage E2EE as a best practice. Some wallet providers may be using encryption at the browser session level, which only protects data during the brief connection (or session) between two systems (e.g., merchant server to acquirer server). E2EE begins at the data level, where consumer information is initially entered.

C. EMV ID&V and Other Authentication Approaches

EMV ID&V applies to the Pay wallet models and is managed by the card issuer. Non-Pay wallet models use proprietary authentication approaches.

EMV ID&V

According to issuers and processors, lessons learned from the challenges of social engineering fraud with early implementations of the Pay wallets led to the collection of more information about a customer (e.g., mobile phone number, dynamic KBA questions) to enhance ID&V. This is often referred to as "tenured" information that provides more history about a customer's behavior (e.g., age of mobile phone, age of wallet account or email address) to aid in authenticating the customer during enrollment.

Other issues to consider include:

- Continually evaluating the EMV ID&V process to ensure that the type of information that is collected and used for risk-decisioning is valuable.
- How to balance the extent to which enhanced data is collected by issuers with the risk of managing and securing that data.
- How to ensure that large and medium-sized issuers and processors are aware of the needs and challenges of smaller issuers and evaluating opportunities to share fraud information despite the potential risks.

[87] Verifone (2014, July). *Multi-Layered Security Strengthens Payment Structures: How to Prepare a Comprehensive Strategy*. Retrieved from http://www.verifone.com/media/4041137/verifone-comprehensive-multilayered-security-white-paper.pdf.

ID&V is an evolutionary process. Issuers are continually refining their analytics based on trends in the marketplace and new information. Third parties that process for smaller FIs should also be educating and sharing security best practices with clients handling e-commerce businesses. Industry stakeholders have noted that re-training call center staff to handle wallet provisioning is a major endeavor. It involves selecting agents with the necessary skills to recognize and answer questions appropriately, while being aware of social engineering tactics used by fraudsters; in addition to being able to handle lost phones and to perform lifecycle management of payment tokens. This challenge is greater for issuers that have managed credit and debit cards, but have never managed tokens.

The card networks offer "on behalf of" services that include risk capabilities to assist issuers with implementing ID&V. They also offer portals through which issuers can perform lifecycle management, but this requires issuers to train call center representatives on how to remotely access and login to each of the network portals. As another option, the card networks offer issuers lifecycle management APIs that that they can integrate into their systems. While this also requires CSR training, it is less burdensome because the process is streamlined to a single experience. Processors also have tools available to help issuers. Lifecycle management is important because issuers and processors must update the token vault when a new PAN is issued (e.g., because of a data breach) so that the new PAN can be re-associated with the token on the mobile device.

Other Authentication Approaches

Large online merchants and PSPs recognize the need to further enhance authentication for the CNP channel. They have sophisticated risk management systems that collect and constantly analyze vast amounts of data to help strengthen the authentication of their customers. However, smaller e-commerce merchants which do not work with third party providers may not have sophisticated approaches to fraud and have less access to information needed to verify a customer, increasing their risk of fraud. Based on the use case analysis and industry research, larger PSPs and online/mobile merchants also use more authentication methods (multi-layer) and fraud mitigation tools than smaller online/mobile merchants who may only use a few tools such as username and password for login/initial authentication, AVS, phone number verification, and check digit.[88]

Other issues include: (1) the merchant's lack of visibility into fraud data across all online/mobile payment methods to provide a more holistic view of each individual customer; (2) the lack of a framework to inform CNP merchants about authentication practices and tools used by larger and more sophisticated stakeholders; and (3) the need to identify the methods, if any, used by smaller e-commerce merchants. While merchant acquirers have a wide range of authentication products to provide to the smaller merchants, it remains a challenge for all parties to disseminate and understand these options.

Whether using EMV ID&V or other authentication approaches, more and better data to help manage fraud is needed.

[88] LexisNexis (2016). *2016 LexisNexis True Cost of Fraud Study*.

D. Level and Sophistication of Customer Authentication Methods

Stakeholders use a variety of approaches to authenticate consumers during the mobile CNP transaction process. While the use case models deploy a variety of methods, including username and password, OOBA, OTP, KBA, device fingerprinting, and biometrics; continued reliance on user ID and password as the *de facto* authentication practice by many online/mobile merchants has become increasingly risky as fraudsters find new ways to steal data and use it to commit payment fraud or gain access to other consumer PII.

The FFIEC guidance has strongly encouraged FIs to implement MFA for digital and mobile banking rather than single factor (username and password) authentication since 2005 and is considered a best practice.[89] In April 2016, the FFIEC added *Appendix E: Mobile Financial Services (MFS)* to its *IT Examination Handbook*,[90] which specifically defines MFS to include "the use of a mobile device to conduct banking transactions *and to initiate retail payments*." While it does not address non-bank compliance directly, it is important that other organizations involved in mobile and digital services (e.g., wallets) review this information and consider the recommended approaches for stronger authentication.

PCI SSC also recently published new requirements for MFA in its PCI DSS version 3.2[91] The purpose of these requirements is to make sure businesses that can make changes to the cardholder data environment (CDE) systems and potentially weaken security controls or introduce vulnerabilities, are more strongly authenticated to prevent, detect, and respond to cyberattacks that can lead to payment data breaches.

SMS has been used as a tool to support MFA for several years. The National Institute of Standards & Technology (NIST) recently updated its recommendations for authentication and other security issues. One recommendation noted that SMS can be compromised and is increasingly becoming a target for criminals; therefore, NIST recommends that U.S. government agencies phase it out as an OOBA method, i.e., the delivery of an OTP for digital authentication in the U.S. government. While not specific to retail payments, SMS is an authentication method used in the retail CNP environment that needs to be reviewed and potentially replaced.[92]

While issuers and many larger merchants, PSPs, and WSPs use MFA and/or multi-layered authentication, practices vary widely based on the level of risk and the sophistication or size of the company. Even with

---

[89]Federal Financial Institutions Examination Council. (2005, Oct. 12). *Authentication in an Internet Banking Environment.* Retrieved from http://www.ffiec.gov/pdf/authentication_guidance.pdf. A supplement was published in 2011 to reinforce the Guidance's risk management framework and update the agencies' expectations regarding customer authentication, layered security, or other controls in the increasingly hostile online environment.

[90]FFIEC. (2016, April). *FFIEC IT Application Exam Handbook: Appendix E*. Retrieved from http://www.ffiec.gov/press/PDF/FFIEC_booklet_Appendix_E_Mobile_Financial_Services.PDF. Recommends that FIs have process for authenticating MFS users to protect customers against fraud. Based on a risk assessment, FIs should consider biometric (e.g., voice, fingerprint, facial recognition) or OOBA processes and FIs ***should not*** rely on less secure (e.g., single factor) methods of authentication for mobile payment applications.

[91]PCI SSC. (2016, April). *Data Security Standard: Requirements and Security Assessment Procedures Version 3.2*. Retrieved from https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf?agreement=true&time=1473436165655.
Johnson, L. (2016, June 1*). Assessor Viewpoint: Adopting PCI DSS 3.2, Multi-factor Authentication and More*. [blog]. PCI SSC. Retrieved from https://blog.pcisecuritystandards.org/adopting-pci-dss-3-2.

[92]Out-of-band verification that uses an SMS message on a public mobile phone network requires that the pre-registered telephone number being used is verified and is actually associated with a mobile network and not with a VoIP (or other software-based) service. Changing the pre-registered telephone number shall not be possible without two-factor authentication at the time of the change. Out-of-band verification using SMS is deprecated, and will no longer be allowed in future releases of this guidance. NIST (2016, Aug. 30). *Draft NIST Special Publication 800-63B Digital Authentication Guideline: Authentication and Lifecycle Management.* Retrieved from https://pages.nist.gov/800-63-3/sp800-63b.html.

guidance and industry best practices, the gap in authentication practices may be widening, leaving mid-sized and smaller e-commerce merchants behind. Advanced tools, such as biometrics, primarily fingerprint authentication for mobile CNP (and POS) payments, and enhanced risk-based authentication (i.e., 3DS 2.0) are being developed and implemented, but the challenge is persuading more m-commerce merchants and PSPs of their value to achieve broader adoption and decrease fraud. So while there are many authentication tools available to reduce fraud associated with m-commerce, not all m-commerce merchants are fully aware of the options, their value, or how many of these tools are actually used by traditional online merchants.

VII. RECOMMENDATIONS

The following recommendations are based on the comparative use case risk analysis and the identification of gaps and issues.

A. Consider Mobile Commerce a New Channel

The mobile channel should be treated separately from, rather than as an extension of, online commerce, because some risks associated with m-commerce differ from e-commerce. The mobile channel may require different or additional security approaches, particularly to prevent and manage mobile CNP fraud.

It is critical for online merchants with a mobile presence to develop appropriate methods to monitor fraud in their e-commerce and m-commerce channels and apply mobile-specific fraud management tools that leverage the unique capabilities of mobile devices. Monitoring these channels separately provides the opportunity to leverage the rich data that can be obtained from the mobile device to provide more details to help identify the customer at login and better manage risk. Merchants can integrate the fraud data into a system that looks across channels and compares data elements such as device ID and login information, addressing the need to manage fraud holistically across customer entry points. They should also consider using the data collected from fraud tools to build a profile of a legitimate versus a fraudulent customer in the mobile CNP channel.

B. Use Multi-layered and Multifactor Security Controls

Section V outlined several security controls and methods: authentication, dynamic cryptograms, encryption, tokenization, and 3DS 2.0. No one solution is a silver bullet to address mobile CNP fraud. Stakeholders should analyze available tools and utilize those that best fit their CNP fraud strategy. Reviewing the NIST and FFIEC resources will help them become more familiar with various options. They should also assess the 3DS 2.0 specifications and related network operating rules.

C. Develop a Strategy to Eliminate Magstripe Cards (Over the next 3-5 years)

As the U.S. payments system migrates from magstripe credit and debit cards to EMV chip cards, a major piece remains to be addressed – removing the magstripe. While nearly all U.S. chip cards continue to be issued with magstripes to ensure continued usability as merchants gradually migrate to EMV technology, the faster chip card acceptance expands, then the faster the use of magstripes may be reduced. Until then, inclusion of the magstripe on cards is a major vulnerability because when swiped instead of dipped, the card is susceptible to counterfeit card fraud. In the POS environment, some merchants are not waiting to

eliminate the magstripe on their private-label cards. For example, Target is planning to remove magstripes from all closed-looped debit and store-only credit cards as part of its transition to EMV chip technology.[93]

In the current CNP environment, many smaller e-commerce merchants may have weak authentication controls that provide fraudsters with the opportunity to make fraudulent purchases with stolen counterfeit card numbers. There is also the risk that a counterfeit card number will be provisioned to a mobile wallet and used to make fraudulent purchases. Overall, reducing potential vulnerabilities in other payment channels benefits the mobile channel as well, as they are all connected and used by consumers.

D. Industry Collaboration on Information Sharing and Customer Education

Many payments industry stakeholders recognize the need for more inclusive collaboration and information sharing to reduce overall payments fraud, and CNP specifically. Today, the information provided is more often shared only with industry groups (e.g., FIs/Financial Services-Information Sharing and Analysis Center (FS-ISAC), merchants/Retail Cyber Intelligence Sharing Center (R-CISC), government agencies, etc.), although there are efforts to cross industry segments where possible. In the retail payments environment, FIs often see fraud or suspicious activity faster than merchants because of the robust risk management tools and fraud monitoring systems they have to support compliance with financial services regulations (e.g., KYC, BSA, electronic funds transfer, consumer protection, etc.). Financial institutions are also the primary point of contact by cardholders when fraudulent activity occurs. Some technology providers[94] offer secure networks that connect issuers and merchants, a model that the industry should consider how to expand, while respecting the confidentiality and competitive aspects of the data.

The need for more effective information sharing expands beyond the CNP environment to the entire payments ecosystem, so while we have identified it as a recommendation for mobile and e-commerce, the broader industry needs to identify ways to improve the value and timeliness of fraud data that will also help the CNP environment.

Consumer research has consistently shown that a major barrier to adoption of mobile payments at POS or via the e-commerce channel is a belief that mobile payments are less secure than card or other forms of payment. As noted in this whitepaper, initiating payments from a mobile device can be significantly more secure due to additional authentication elements provided by the mobile device. All stakeholders have an obligation to support ongoing customer education regarding secure mobile payment practices, and should engage collaboratively in developing consistent materials and messaging.

---

[93]Kossman, S. (2015, Dec. 2). Magnetic stripe begins its farewell tour. *Creditcards.com*. Retrieved from http://www.creditcards.com/credit-card-news/magnetic-stripe-farewell-tour-1273.php.

[94]As an example, Ethoca provides collaboration-based technology that enables issuers and e-commerce merchants to stop CNP fraud, recover lost revenue, and eliminate chargebacks. The technology can quickly notify merchants of potentially fraudulent cards and allow merchants to intercept a shipment and cancel an order to avoid a chargeback. Heun, D. (2016, Feb. 26). TSYS, Ethoca partner for transaction recovery network. *PaymentsSource*. Retrieved from http://www.paymentssource.com/news/retail-acquiring/tsys-ethoca-partner-for-transaction-recovery-network-3023582-1.html.

E. Share Best Practices from M-Commerce Use Case Analysis

The best practices identified in this use case analysis should be shared with mid-sized and smaller/micro m-commerce merchants, and CNP third-party/non-bank mobile solution providers. While small m-commerce merchants were not the focus of this research, the risk analysis applies to them as well. We assume that risks associated with small businesses have indirect consequences for medium and large merchants and the broader payments ecosystem. To support this assumption, it would be helpful to understand if smaller m-commerce merchants: (1) experience different types of fraud and risks; (2) leverage information provided from consumer mobile devices; and (3) participate in relevant industry security forums.

Furthermore, non-bank technology providers and start-ups that support mobile CNP solutions and services often lack knowledge about the payments industry and security. It is difficult to assess the risk created by these companies because there is no consistency to how they evolve or operate. All third party relationships should be carefully evaluated before an agreement is executed as well as on a recurring basis.

Large e-commerce merchants and processers should recognize that sharing some of their best practices and experiences using different fraud tools for CNP payments with the smaller, less sophisticated, or newer mobile/e-commerce businesses will have a positive impact on the entire CNP environment. Distributing this knowledge can potentially reduce overall fraud and increase consumer confidence in making mobile and online purchases. The major stakeholders should coordinate efforts to develop best practices targeted at the smaller m-commerce merchants, determine effective ways to reach out to them and communicate this information.

F. Collaboration on Standards and Best Practices to Mitigate Mobile CNP Fraud

Issuers, merchants (POS and e-commerce), acquirers, card networks, processors, PSPs, and WSPs should collaborate and coordinate initiatives to identify where gaps exist in current proprietary and open standards and practices. They should provide input and expertise in the development or enhancement of technology standards, as well as guidelines and best practices, to improve the security of mobile and e-commerce CNP payments, particularly in the areas noted in this paper: authentication, and tokenization and encryption for data protection.

VIII. CONCLUSION

This comparative use case risk analysis provides rich insight into some of the primary wallet models in the U.S. payments environment from a consumer, business, and technology perspective. The evolution of these models is important because mobile commerce is a big driver of e-commerce and CNP payments. Furthermore, multiple technologies exist to support different mobile CNP use cases and the models leverage multiple fraud mitigation solutions. Consumer adoption of mobile wallets remains slow but is expected to grow significantly in the coming years as consumers become more comfortable using the wallets to pay and as their security concerns decline. Mobile wallets can offer enhanced security over traditional online e-commerce because consumers constantly carry their mobile phones, they can use a fingerprint or PIN to unlock the phone, or they can remotely wipe the phone if it is lost or stolen. The mobile device also allows

merchants, PSPs, WSPs, and issuers that offer mobile wallets to leverage new data elements about the consumer's identity and the mobile device that can enhance their fraud management strategies.

Whether a mobile browser or a mobile app is used to make a mobile payment, each has advantages and disadvantages. A mobile browser can leverage new data elements about the mobile operating system or the device type and does not require a download by the consumer. Mobile apps engage the customer with a robust mobile experience and provide richer, customized data for merchants (e.g., GPS, phone number, device ID/type). Several shortcomings of mobile browsers include a variable IP geolocation that results in accuracy problems, and the ability to spoof browsers and direct consumers to a fraudulent website. Shortcomings of mobile apps come from their proliferation. On average, consumers only regularly use about 2-3 mobile apps on their mobile phone. For merchants, mobile apps are more expensive to update and manage than mobile browsers. For consumers, mobile apps often request too many permissions to collect user data, leading to privacy concerns.

The use cases outline the range of authentication and security controls applied at different points in the transaction flow and how these controls vary by model. The guest checkout model offered by merchants is an important solution for customers that may not want to create online accounts or store payment credentials with retailers. However, it is more difficult for merchants to authenticate guest checkout customers than it is for registered customers, but *mobile* guest checkout transactions can provide merchants with more data about the device, such as device ID and device type to strengthen authentication. The wallet models vary in their use of tokenization. As noted earlier, some models use payment tokenization and others rely on proprietary security tokenization approaches. The use of payment tokenization makes the Pay wallets very secure because the payment credentials undergo strong risk analysis before a token is provisioned to a wallet and for all future wallet purchases, only a payment token (and a dynamic cryptogram) is used in the transaction, eliminating use of the PAN. Cloud-based CoF models that use other authentication processes leverage sophisticated risk modelling and behavior analysis to know their CNP customers and prevent fraud. The card network digital wallets benefit the consumer because payment credentials do not need to be shared with merchants for purchases. Also, the card networks have robust risk management systems to monitor cardholder and account behavior for anomalies to prevent fraud.

Regardless of the number or strength of the authentication and security controls used to prevent and manage fraud, there is room for improvement and more industry guidance on how to select and implement these tools. The payments industry recognizes this need and is taking action to enhance existing methods, introduce new solutions, and identify best practices to mitigate CNP mobile fraud, and overall e-commerce fraud. Issuers, merchants, processors, PSPs, and WSPs are aware of the existing gaps in security tools and approaches and equally realize the need to protect the PAN and user login credentials as these have now become a prime target for fraudsters.

In the face of rapid technology innovation and emerging alternative payment models, it will be critical to anticipate emerging and manage existing fraud threats. Collaboration and partnerships will be key relationships for targeting this fraud to ensure an advanced, but secure payments system. It is equally important to collectively track and monitor consumer adoption, behavior, and preferences for mobile wallets/models, particularly since nearly 20 percent of U.S. consumers use mobile wallets to complete a purchase currently and 12 percent of merchants generate half of their revenues via the mobile channel,

which is expected to double in the next two years.[95] Mobile wallets may support a more secure payments experience than the traditional online channel; however, the industry must work together to support and develop interoperable security controls and solutions that do not negatively impact the consumer or merchant experience. The MPIW will continue to track and monitor trends in the mobile CNP payments environment and report on relevant developments through ongoing dialogue, subgroup efforts, qualitative research and publications, industry presentations, and other educational materials.

[95] Gjerding, K. (2016, Oct. 11). How to navigate a rapidly growing payments ecosystem. *Cardnotpresent.com*. Retrieved from *http://cardnotpresent.com/how-to-navigate-a-rapidly-growing-payments-ecosystem/*.

APPENDIX A: GLOSSARY

Account Creation: Account creation is the consumer process of opening a new online account and establishing a user profile with a merchant, PSP, WSP, financial institution, or other business during which consumer PII and payment credentials are collected and can be a potential point of vulnerability.

Account Enrollment: The process of the customer registering one or more payment credentials to their account, which the customer can opt to store on file as a default payment method for future purchases.

Account Takeover Fraud (ATO): ATO fraud occurs when fraudsters use stolen consumer login credentials to access online accounts and steal PII to change account settings and take over the account to make purchases.

Address Verification System (AVS): A tool that checks that the numeric portions (i.e., street number, zip code) of a billing address provided by the consumer to see if it matches the address on file with the cardholder's issuing bank.

Authentication: The verification of the identity of a person or process. Authentication is usually supported by several factors that include something that a person knows (e.g., PIN, shared secret, image), something that a person has (e.g., card, token, phone), and something that a person is (e.g., biometrics).

Authorization: The process of giving an individual or entity permission to do or have something.

Behavioral Analytics: Data that is collected and analyzed about a user's normal online/mobile activity patterns (e.g., login and browsing processes) to detect good users from bad ones by identifying anomalous activity to determine if certain transactions do not align with the user's typical patterns of transacting.

Biometric technology: Biometric technology measures and analyzes a person's physical and behavioral characteristics. Biometrics such as fingerprints and facial, iris, or voice recognition are being used more as a form of identity to authenticate a person, replacing passwords and PINS.

Card-Not-Present (CNP): CNP is a payment made for a purchase using a payment card, where the cardholder/card are not physically present to allow the merchant to validate the cardholder at the time of purchase (e.g., by U.S. postal mail, telephone, or internet).

Card-not-Present Fraud: Involves the unauthorized use of a payment card number, card verification code (CVC) 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.

Card-on-File (CoF): Authorized storage of a consumer's payment credentials by a merchant, PSP, or WSP, that allows the consumer to conveniently make repeat or automatic purchases without the need to re-enter payment credentials each time. *(Note: CoF may include a broad range of payment types such as bill payment or P2P, but this project is focused on mobile retail CNP payments).*

Card Present: Describes a payment transaction where the cardholder is physically present and either presents the physical card or an electronic representation of it (i.e., mobile wallet).

Chip and PIN: The phrase adopted by the payments industry as an authentication option for the EMV smart card payment system for payment cards. The word "chip" refers to a computer chip embedded in the smartcard; "PIN" refers to a personal identification number that must be supplied by the consumer in lieu of their signature to authorize a transaction.

Device ID/Fingerprinting: A method that analyzes the mobile device and its characteristics (e.g., installed plug-ins, software, time zone) to confirm that the mobile device being used for a transaction is the same device used for previous legitimate transactions.

Device Rooting/Jailbreaking: The process for unlocking the operating system of an Android (rooting) or Apple iOS (jailbreaking) mobile device to gain access over various subsystems and the ability to install unauthorized applications.

Device Type: Unique attributes and characteristics about a mobile device that can be leveraged to provide information about how it works with a particular transaction.

Digital Wallet: A software-based container that allows a user to store personal information (e.g., ID, insurance, health, transportation, etc.), loyalty and couponing information, and payment information (i.e., credit card or bank account) that can be used to perform e-commerce/m-commerce transactions. The wallet application may reside on the user's mobile device or computer.

Dynamic Cryptogram: A unique value generated for each transaction using a symmetric key that is validated by the party that shares the key with the cardholder's device for each mobile CNP transaction.

EMVCo: A consortium formed in 1994 by Europay (now part of MasterCard), MasterCard, and Visa that manages, maintains and updates the specifications for chip-based payment cards and terminals.

Encryption: In cryptography, the process of converting messages or information (e.g., payment data) in such a way that only authorized parties can read it.

Geolocation: Digital information obtained to identify the geographical location of a user/mobile device.

Host Card Emulation (HCE): A software-based technology that supports the ability for a mobile wallet app running on the host processing unit of a mobile device, to communicate through the NFC controller in the mobile device to a contactless NFC-enabled POS terminal/reader to pass payment card credentials (or payment token), eliminating the need to access payment credentials or tokens stored on the physical SE chip in a mobile device.

Identification and Verification (ID&V): A process by which an entity may successfully validate the cardholder and the cardholder's account in order to establish a confidence level for linking a payment token to the cardholder's PAN.

Knowledge-based Authentication (KBA): Requires a user to answer security questions that cannot be easily found in a physical wallet or online.

Malware or Virus: Malicious software that disrupts a mobile device/operating system to steal payment credentials and PII that can be used by a fraudster to create accounts with online and mobile merchants, PSPs, and WSPs.

Machine Learning: 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 and learn from previous computations to produce reliable, repeatable decisions and results and turn background knowledge and examples (input) into knowledge (output).

Mobile Application: An application that can be downloaded to a mobile device (or tablet) from a mobile app store, such as Google Play or the Apple Store.

Mobile In-App Payment: A mobile application that allows users to purchase goods and services (including digital goods and services) directly from within a merchant native mobile app using a mobile wallet that has been provisioned with an EMV payment token (currently, Apple Pay, Android Pay, and Samsung Pay). Purchases can be made by a consumer by selecting the mobile wallet icon within the mobile app and authorizing the transaction with a fingerprint or PIN/passcode.

Mobile Browser-Based Payment: Use of a mobile phone browser to navigate to a company's mobile website to make a payment for a purchase.

Mobile Device-Porting Fraud: A type of attack that occurs when a fraudster obtains PII through a compromise and then calls the victim's mobile carrier and impersonates the victim to request to transfer his mobile phone number to the fraudster's new phone. The fraudster can then use the stolen PANs and PII to enroll in a wallet on his new mobile phone and conduct fraudulent transactions.

Mobile Man-in-the-Middle (MiTM) or Man-in-the-Browser (MiTB): A MiTM attack intercepts a communication between two systems. A MiTB is a type of MiTM attack that uses a proxy Trojan horse to infect a web/mobile browser by taking advantage of vulnerabilities in browser security to modify web pages or transaction content.

Mobile Payment: Using a mobile phone to make proximity or remote purchases, including point-of-sale (POS), transit, online goods and services, digital content and person-to-person (P2P) money transfers. Payment can be funded with a payment card, prepaid account, bank account (ACH) or charged to a phone bill.

Mobile Wallet: An application in a mobile device that controls access to payment credentials and other personal information (e.g., payment cards, bank accounts, coupons, loyalty rewards, transit tickets) to allow the individual to perform electronic proximity or remote transactions.

Multifactor Authentication (MFA): A security control that requires more than one method of consumer authentication from independent categories of credentials to verify the user's identity for a login or other transaction, such as something the user knows (password), something the user has (security token), and something the user is (biometric verification).

Near-Field Communication (NFC): A standards-based wireless communication technology that allows data to be exchanged between devices that are a few centimeters apart.

New Account Fraud: A type of attack where fraudsters use compromised PANs and PII to create new CNP accounts because online account enrollment is easier to complete with valid consumer information.

Out-of-Band Authentication (OOBA): A type of two-factor authentication that requires a second verification method through a separate communication channel (e.g., SMS or email).

PC Browser-Based Payment: Use of a PC/laptop browser to navigate to a company website to make a purchase.

Payment Service Provider (PSP): 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.

Payment Tokenization: The process of replacing sensitive payment credential data (i.e., account number) with a surrogate value that has no exploitable value. Payment tokenization is currently only used in models that follow the *EMV Payment Tokenization Specification* with payment tokens issued by card networks.

Personally Identifiable Information (PII): PII, as used in U.S. privacy law and information security, is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

Primary Account Number (PAN): The 16 digit number that appears on the primary accountholder's credit or debit card.

Proximity Payment: Payments made at both attended POS locations (such as stores) and unattended locations (such as vending machines) between a mobile device and a payment receiving device.

Quick Response (QR) Code: A machine-readable, two-dimensional barcode that contains information (e.g., payment account data) which can be scanned and decoded quickly.

Remote Mobile Payment: Uses a variety of mobile device data channels to conduct a transaction, such as a mobile browser or mobile app.

Risk-based Authentication (RBA): Examines a variety of contextual information to verify the consumer's identity (e.g., IP address, geolocation), which device is being used (e.g., device type), and whether or not the user's behavior is consistent (e.g., login frequency and attempts).

Sandboxing: Sandboxing improves application security by isolating an application to prevent outside malware, intruders, system resources or other applications from interacting with the protected app.

Secure Element (SE): A secure element resides in highly secure cryptographic chips (usually a smart card chip) for which there are three types: UICC/SIM card, microSD, and embedded SE. The SE chip provides a dynamic, tamper-resistant environment in which application code and application data can be securely stored and administered and in which secure execution of applications occur.

Security Tokenization: A method for protecting payment card data post-authorization or for data-at-rest by substitution of a sensitive payment credential information (i.e., PAN) with a unique, randomly generated sequence of numeric and/or alphabetical characters. Security tokenization is often also referred to as acquirer tokenization because it is supplied by acquirers to merchants, or can be supplied by third party technology providers and payment gateways. Some merchants may develop their own proprietary systems.

Spoofed Authentication: A spoofing attack occurs when a malicious party impersonates another device or user on a network in order to launch attacks against network hosts. A spoofed authentication attack seeks to mimic existing user authentication methods (fingerprint, mobile device, IP address) to gain access to an account or use a fake mobile app to capture sensitive consumer data and/or authentication factors.

Three-Domain Secure (3DS): A risk-based authentication messaging protocol to enable consumers to authenticate themselves with their card issuer when making online purchases. The three domains consist of the merchant / acquirer domain, issuer domain, and the interoperability domain (i.e., payment systems).

Token Provisioning: The process of delivering an *EMV payment token* and its related values to the token storage location. A token storage location could be on a secure element of a mobile device, secured software environment of a mobile device, or a remote server.

Token Service Provider (TSP): An entity providing the generation, issuance, maintenance, and other processing support for payment tokens and operation of the token vault.

Token Vault: A repository operated by the token service provider that maintains the linkage of a payment token to the cardholder's PAN.

Trusted Execution Environment (TEE): Secure processing area that stores the payment token in the mobile phone.

Wallet Service Provider (WSP): WSPs support mobile wallets that use various communications technology for mobile payments.

White-box Cryptography: A method that prevents the cryptographic key from being retrieved even if the original source code is available and could be used to hide payment credentials in a host card emulation application.

APPENDIX B: USE CASE ANALYSIS MATRICES

Use Case 1: Guest Checkout via Mobile Browser or Mobile App with No Card-on-File			
FUNCTIONS OF CNP TRANSACTION		**Probability of Risk**	**Magnitude of Risk**
ACCOUNT CREATION[96]			
1. Data breach risk	• Consumer data may be exposed as it is entered on merchant's website via browser or in a mobile app. o Low risk if encrypted. • Consumer data stored in merchant system is not adequately protected (e.g., encrypted, tokenized). o Probability of risk is MEDIUM. • Fraudster may complete successful transaction before the risk is detected. Larger merchants usually can detect risk for subsequent transactions. • Risk may be high for smaller merchants lacking proper tools or resources to respond to attacks. o Magnitude of risk is LOW. (1) No account is created with the merchant. (2) No account login credentials are created. (3) No PANs or PII stored with merchant. (4) PAN alone is less valuable to fraudsters because of EMV chip card issuance and limited shelf life.	MEDIUM[97]	LOW[98]
2. Malware/virus	• Consumer data may be exposed as it is entered (or auto-populated) on merchant's website via browser or in a mobile app. o Low risk if encrypted. • Probability of risk is MEDIUM. o Fraudster may complete a successful transaction before risk is detected. Larger merchants usually can detect risk for subsequent transactions. o Risk may be high for smaller merchants lacking proper tools or resources to respond to attacks. • Magnitude of risk is LOW. (1) No account is created with the merchant. (2) No account login credentials are created. (3) No PANs or PII stored with the merchant. (4) PAN alone is less valuable to fraudsters because of EMV chip cards and limited shelf life. (5) Malware would need to penetrate each mobile device, reducing likelihood of large-scale attack.	MEDIUM	LOW

[96] Fraud associated with account takeover, new account creation, and mobile device-porting are not applicable to Use Case 1.
[97] Low risk of capturing PANs; higher risk of capturing login credentials and PII.
[98] Would have to attack individual phones making large-scale attack difficult.

AUTHENTICATION			
1. Mobile man-in-the-middle (MiTM) attack 2. Mobile man-in-the-browser (MiTB) attack 3. Malware • Most MiTB attacks are intended to install malware on a device. • Fraudsters can eavesdrop on a mobile device's via a rogue hotspot and can intercept data flowing to and from the device's browser and apps to capture sensitive information.	• Probability of risk is MEDIUM. o Fraudster could intercept PAN or PII when being entered by consumer. o Risk may be lower for mobile app because more information can be collected about device and user behavior (e.g., device ID, geolocation, transaction history). o Risk lowered if data is encrypted during entry and mobile app is protected from penetration attacks. • Magnitude of risk is LOW. (1) No account is created with merchant. (2) No account login credentials are created. (3) No PAN or PII stored with merchant. (4) PAN alone is less valuable to fraudsters because of EMV chip card issuance and limited shelf life. (5) Larger merchants are likely to use strong fraud detection techniques; however, smaller merchants may not have proper tools or resources to respond effectively to these attacks. (6) Malware would need to penetrate each mobile device reducing likelihood of large-scale attack. (7) Prior to transaction occurring, larger merchants perform several consumer authentication and verification checks (e.g., AVS, device ID, IP address, bill to ship to match, maybe 3DS) on guest checkouts and may be more stringent since the user is unknown.	MEDIUM	LOW
MOBILE DEVICE / OS INTEGRATION			
1. Mobile device rooting/jailbreaking	• A rooted/jailbroken device diminishes existing security controls in mobile OS, which could allow malware to compromise PAN/PII that is entered using a mobile browser or mobile app. • Probability of risk is MEDIUM to HIGH. o Security of mobile device/OS cannot be controlled if device is rooted/jailbroken. o Device becomes vulnerable to malware and other attacks to access sensitive information. • Magnitude of damage is LOW. o Fraudster would need to steal and compromise many mobile phones, PANs, and PII for a large-scale attack.	MEDIUM - HIGH	LOW
2. Lost/stolen device	• Probability of risk is HIGH. o Fraudster with a stolen device may gain access to consumer information to make a guest checkout purchase. • Magnitude of risk is LOW. (1) Guest checkout only occurs on mobile browser or mobile app and PANs and PII are not stored with merchant. (2) Consumers quickly report a lost or stolen device and can remotely wipe the device of data and mobile apps. (3) Larger merchant detection programs can turn off the mobile device to prevent the ability to complete transactions. (4) Fraudster would need to steal and compromise many mobile phones, PANs, and PII for a large-scale attack.	HIGH	LOW

3. Malware/virus	• Probability of risk is HIGH. o Malware or virus could direct a consumer to a spoofed mobile browser site or mobile app that appears legitimate and captures consumer PAN and PII. • Magnitude of risk is LOW. o Fraudster would need to steal and compromise many mobile phones, PANs, and PII for a large-scale attack.	HIGH	LOW
USE OF THIRD-PARTY PROVIDERS			
1. Data breach risk	• Probability of risk is MEDIUM. o If merchant uses third party provider to host the shopping cart interface to accept PANs/PII consumer enters, the information could be breached if not adequately protected by the third party provider. o Risk is lowered based on strength of the fraud detection methods used by the third party provider. • Magnitude of risk is HIGH. o Third party provider may have broad reach in the industry (e.g., support multiple merchants) and data breach could impact many devices and consumer accounts.	MEDIUM	HIGH

Use Case No. 2-Mobile In-App with EMV ID&V and Card-on-File (the Pay wallets – Apple, Android & Samsung Pay)			
FUNCTIONS OF CNP TRANSACTION		**Probability of Risk**	**Magnitude of Risk**
ACCOUNT CREATION	• Pay wallets are pre-installed on a mobile device, which lowers potential risk of installing a fraudulent mobile app. • User required to create or sign in to an account with the WSP. Usually prompted when mobile phone is purchased and activated. • User enrolls eligible payment cards (credit/debit PAN) by manual entry, scanning, or default card-on-file (e.g., iTunes). • If person physically present to activate mobile phone, more secure. However, risk is not any greater if user sets up the mobile wallet at a later time after activation because the process is still the same. The risk to the issuer may be lower if the user waits to set up the mobile wallet because the issuer will have more tenured information about the customer and the device.		
1. Data breach risk	• PAN is intercepted when user enters it into wallet app. • Consumer unknowingly uses a fraudulent "Pay" wallet app to enter PAN/PII, which is captured during account creation. o Probability data breach LOW. (1) Account information is encrypted during enrollment and remains encrypted during the transmission. (2) While a breach is conceptually feasible, EMV spec requires all token requestors (TRs) (e.g., Apple, Android, and Samsung) to register with TSPs and implement token service APIs. TSP assigns unique IDs to each TR domain (e.g., NFC POS, mobile in-app, etc.), allowing TR to request tokens from TSP for specific domains. TR domains provide additional control to ensure that tokens are used as TR intended. o Magnitude of risk LOW.	LOW	LOW
2. Malware/virus	• Probability of risk LOW. o Payment applets are stored in a protected environment in the mobile phone, either in SE chip, TEE, or a secure area of OS memory protected by sandboxing[99] and white-box cryptography.[100] While mobile phone may be vulnerable to malware or viruses, attack cannot penetrate mobile wallet applet. • Magnitude of risk LOW. o No PANs are stored on the mobile device. o Only payment tokens, cryptographic keys, and/or single- or limited-used keys reside in the mobile device.	LOW	LOW

[99] Sandboxing isolates an application to prevent outside malware, intruders, system resources or other applications from interacting with the protected app.

[100] White-box cryptography prevents the key from being retrieved even if the original source code is available and could be used to hide payment credentials in the HCE application.

3. Account takeover fraud (ATO)	• Probability and magnitude of risk are both LOW. o Mobile phones that are enabled for Pay wallets have secure lock mechanisms that require the user to authenticate via fingerprint, pattern, PIN, etc. before making a payment. o This prevents ATO if a consumer loses his device.	LOW	LOW
4. New account fraud	• Probability of risk LOW to MEDIUM. (1) Fraudster could use stolen PAN to fund a mobile wallet account. However, PAN is only useful if payment token is successfully provisioned to mobile wallet. (2) Improvements to issuer ID&V have strengthened the ability to identify a stolen PAN and prevent its provisioning to the device. According to industry experts, probability of new account fraud is trending down for wallet accounts. • Magnitude of risk LOW. (1) Issuers use robust ID&V processes. (2) Stolen PAN has a limited life for fraudulent purchases before it is reported stolen and disabled. (3) Attack is limited to one consumer wallet account per incident and usable only with merchants that accept the Pay wallet. While merchant acceptance is low, this may also be a deterrent to fraudsters. (4) Several stakeholders (merchant acquirer, wallet provider, card network, and issuer) are involved in detecting potential fraud; so if a new wallet account is created with a stolen PAN, the provisioned token can be turned off as soon as the fraud is detected.	LOW – MEDIUM	LOW
5. Device porting fraud	o Fraudster calls a mobile carrier to port a stolen mobile phone number to a new device. If successful, the fraudster uses the stolen phone number to create a mobile wallet on his new phone. o Probability and magnitude of risk are both LOW. o Attack is limited to one individual consumer account and only to merchants that accept Pay wallets.	LOW	LOW
EMV (ID&V)	Issuer performs ID&V before a payment token is provisioned to a wallet per the EMV spec.		
1. Social engineering fraud	• Fraudster steals consumer PAN and poses as cardholder to induce an issuer's call center representative to provision stolen PAN to a Pay wallet. o Probability of risk LOW. • Risk was medium to high in early implementations because of weak ID&V practices in issuer call centers, but ID&V practices have since been enhanced. o Magnitude of risk LOW. • This type of attack is difficult to scale across multiple consumer accounts.	LOW	LOW

AUTHENTICATION[101]	Consumer authenticates to mobile device with fingerprint, PIN or passcode to initiate a transaction.		
1. Fingerprint spoofing 2. Fingerprint sensor spying attack	• Fingerprint spoofing attacks attempt to use materials such as modeling clay to make a replica of a fingertip, or to make copies of a fingerprint image, to use it to unlock a smartphone that is biometric-enabled. • Fingerprint sensor spying attack occurs when a hacker acquires a user's fingerprint sensor from a device where the sensor was not fully locked down by the manufacturer. The hacker will harvest stolen fingerprint sensors and use them over and over again where fingerprints are required since they cannot be replaced. o Probability of risk LOW for both types of attacks. (1) Stealing fingerprints is highly complex because storage is local to the mobile device and isolated within mobile device hardware. (2) Device manufacturers have recognized and corrected the lockdown exposure in the mobile device. (3) Fingerprint data for Pay wallets is encrypted and stored in secure areas of the mobile OS and not transferred to the wallet servers. One wallet requires users to re-enroll fingerprints when an account is setup on a new phone. (4) If the fingerprint data were acquired by a fraudster, he would also need the cryptographic key to access it. o Magnitude of risk HIGH for both types of attacks. • If fingerprint images and/or data are stolen and used, the consumer cannot replace his fingerprint with a new one, as with a password.	LOW	HIGH
MOBILE DEVICE/ OS INTEGRATION			
1. Mobile device rooting/jailbreaking	• Jailbreaking (iOS) or rooting (Android) removes restrictions and security checks imposed by the OS and permits root access, allowing users to download apps from non-certified app stores. o Probability and magnitude of risk are both LOW. (1) Mobile OS (Android and Apple) prohibits access to Pay wallets if the device has been rooted or jailbroken. (2) Wallets use tools to detect incompatible software that may be running on the device. (3) Rooted phone cannot penetrate the SE on an Apple phone.	LOW	LOW
2. Lost/stolen device	• Probability and magnitude of risk are both LOW. (1) No payment credentials are stored on the mobile device. (2) Issuer can delete token on device if cardholder reports device stolen or uses "Find My Phone" function.	LOW	LOW

[101] Fraud associated with MiTM and MiTB are not applicable to Use Case 2 because the models do not use a mobile browser and there is no middle point in the transaction that is susceptible to attack.

3. Malware/virus	• Depending on the model, the payment token is protected because it is stored either in the tamper-resistant SE, the TEE, or by the mobile OS's use of sandboxing and white-box cryptography.	LOW	LOW
USE OF THIRD-PARTY PROVIDERS			
1. Data breach risk	• Fraudster breaches third party provider and captures sensitive account information that third party stores or manages on behalf of a WSP or can access for other services. o Probability and magnitude of risk are both LOW. (1) Pay wallet participants (TSPs, TRs, issuers) operate within a tightly controlled environment under the EMV spec, which governs their relationships and determines which parties can participate.	LOW	LOW

Use Case 3: Mobile Browser or Mobile App Using Other Authentication Processes with Card-on-File (e.g., Large Online Merchant Mobile Wallets, Amazon, PayPal)

FUNCTIONS OF CNP TRANSACTION		Probability of Risk	Magnitude of Risk
ACCOUNT CREATION[102]	• Consumers are required to create an account username (email) and password and link eligible payment credential (debit/credit PAN) to the account to create a CoF. • Most PSPs and large merchants collect consumer name, email address, mobile phone number. o Additional information collected may include shipping/billing address and setting account preferences, browser IP address, device ID, geolocation, etc.		
1. Data breach and malware/virus	• If PSP or merchant website or mobile app is breached and penetrated by malware/virus, consumer PAN, PII, and login credentials can be compromised when entered by the consumer during account creation, unless encrypted. o Probability of risk HIGH. ▪ Data valuable to fraudster is concentrated in one location. o Magnitude of risk MEDIUM. ▪ Data is encrypted.	HIGH	MEDIUM[103]
2. Account takeover fraud (ATO)	• Stolen login credentials used to access a PSP or merchant wallet account via mobile browser or mobile app, change the account settings, and make fraudulent purchases using the victim's PAN that is stored on file. o Probability of risk HIGH. ▪ Account login credentials are a main target for fraudsters. o Magnitude of risk MEDIUM. ▪ Fraud is limited to a single merchant or PSP website or mobile app.	HIGH	MEDIUM
3. New account fraud	• Stolen PANs and PII from a previous data breach could be used in an attempt to create a new fraudulent account with the PSP or merchant. o Probability of risk HIGH. ▪ Credentials are exposed, unless encrypted. o Magnitude of risk MEDIUM. ▪ Fraud is limited to a single merchant or PSP's mobile website or app that the account was created on.	HIGH	MEDIUM

[102] Mobile device-porting fraud and EMV ID&V are not applicable to Use Case 3. EMV ID&V only applies to EMV models that use payment tokenization.
[103] Assumes larger, well-established PSPs and merchants have robust risk management practices in place to know their customers in the CNP environment.

AUTHENTICATION	• Two types of models: (1) Consumer authenticates to a PSP wallet with login credentials to pay for a purchase on a merchant mobile website/mobile app and PSP processes transaction on behalf of the merchant. (2) Consumer authenticates to a merchant account with login credentials and authorizes a transaction with the payment method that is stored on file (CoF). • PSP, merchant, or third party provider performs risk assessment on back-end before payment credentials are stored on file. • PSP, merchant, or merchant acquirer may create a proprietary security token to store (post-authorization of transaction) in databases rather than store the actual payment credential.		
1. Spoofed authentication	• Probability and magnitude of risk are both LOW. o Most large merchants/PSPs have authentication methods and risk management tools in place such as device ID, IP address, geolocation, behavioral analytics, fraud scoring, data analysis, etc.	LOW	LOW
2. Mobile man-in-the-browser (MiTB) attack and malware	• MiTB can create a fake WiFi or cell tower access point and hijack a browser session between a consumer and a merchant or PSP to steal PANs, PII, login credentials and also intercept OOBA via SMS. • All sensitive information shared over an open network should be encrypted and not transmitted in the clear. • Probability and magnitude of risk are both LOW because of the variety of risk management tools available and typically present on the browser or rich device information for a mobile app. Therefore, low risk can be maintained if: (1) Tokenized information is passed. (2) OOBA is used to thwart an attack. (3) If consumer has anti-virus software installed on device; (4) Cryptographic protocols are used that are designed to provide communications security over a computer network are a part of TLS required by PCI DSS. (5) Certificate validation of websites and mobile apps is used to ensure that it has not been hijacked and a server is what it says it is.	LOW	LOW
MOBILE DEVICE/ OS INTEGRATION			
1. Mobile device rooting/jailbreaking	• Probability of risk MEDIUM. o A jailbroken device diminishes the existing security controls in the mobile OS, which could allow malware to be introduced to the mobile device to compromise the wallet account. • Magnitude of risk LOW. (1) Tools are used to recognize rooted/jailbroken devices and restrict use of mobile apps. (2) Collection of information about device type/OS. (3) No payment credentials are stored on the device. (4) Impact is limited to a single mobile device.	MEDIUM	LOW

2. Lost/stolen device	• Probability of risk HIGH. o Fraudster accesses PSP/merchant website or mobile app via stolen mobile device and attempts to make a purchase with the payment credentials stored on file. • Magnitude of risk LOW. o PSPs/larger merchants have fraud detection tools to disable access to the stolen device. o Consumers notice and report lost or stolen devices quickly to remotely wipe the device.	HIGH	LOW
3. Malware/virus	• Probability of risk is HIGH whether mobile browser/app. o Malware/virus can potentially locate PANs/PII when consumer logs in to PSP/merchant account. Risk can be lowered if data is encrypted. • Magnitude of risk LOW. o Successful compromise would require large-scale attack on mobile phones and access to consumer login credentials, PANs, and PII. o **Mobile apps have other controls** not available with mobile browsers: (1) Apps are vetted by OS app store. App may receive random reviews and automated malware/virus scans. App store can suspend suspicious mobile apps; (2) App store issues guidelines to developers that leverage industry-recognized security standards and mobile app testing requirements; (3) Mobile apps that collect PANs/PII must have adequate level of security to store and transmit that information; (4) Mobile apps collect more information about the consumer and the transaction; and (5) Mobile apps may require user permissions before installing an app on a mobile device (e.g., geolocation, phone log, WiFi connection, device ID, etc.).	HIGH	LOW
USE OF THIRD-PARTY PROVIDERS			
1. Data breach risk	• If a merchant or a PSP uses a third party provider to host a mobile website or app shopping cart interface where PANs/PII are entered, the information could be compromised if not adequately protected. o Probability of risk LOW. ▪ PSPs and large merchants have strong third party risk management practices and compliance programs, but risk may higher for companies without these safeguards. o Magnitude of risk HIGH. ▪ Third party provider breach could compromise a significant amount of customer data and impact a large number of mobile devices.	LOW	HIGH

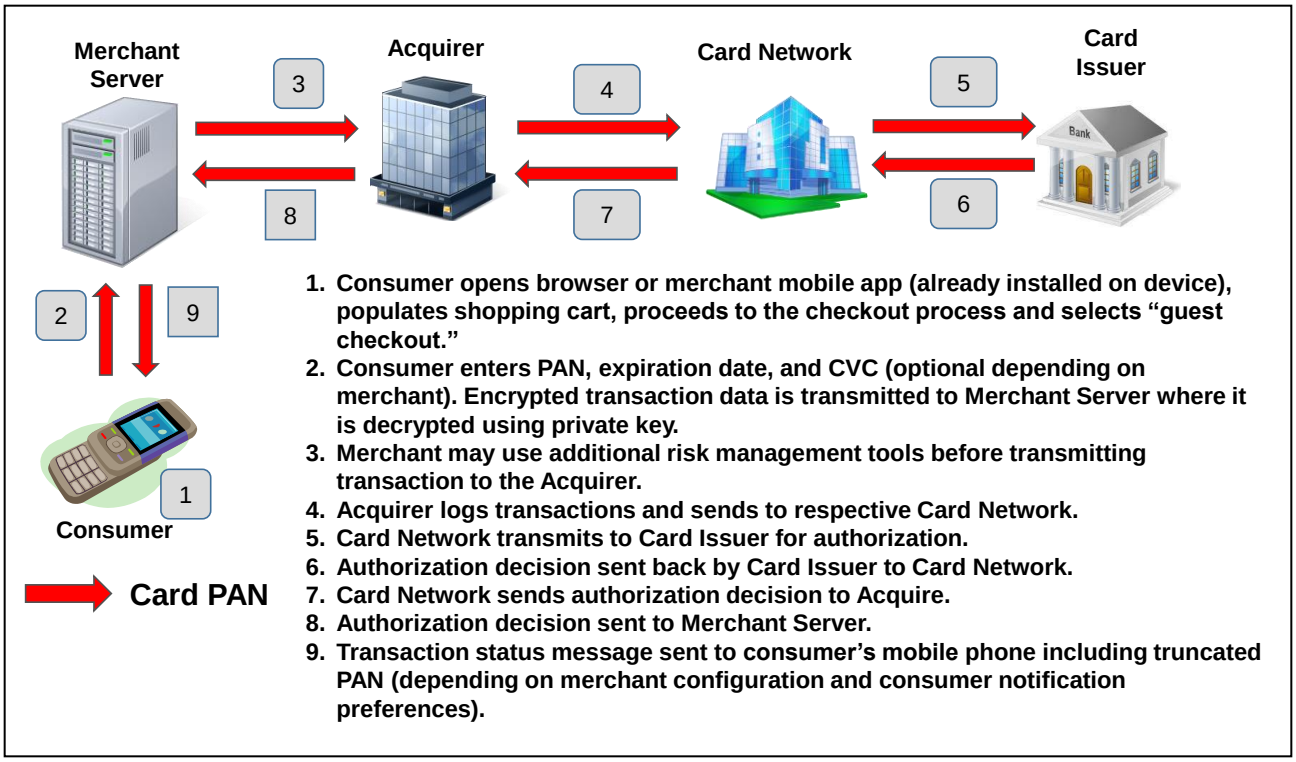
Use Case 4: Card Network Digital Wallet (Checkouts) with or without EMV ID&V with CoF or with EMV Payment Token Provisioning

FUNCTIONS OF CNP TRANSACTION		Probability of Risk	Magnitude of Risk
ACCOUNT CREATION			
1. Data breach 2. Malware/virus 3. Account takeover fraud (ATO)	• Probability of risk is MEDIUM to LOW and the magnitude of risk is LOW for these three types of attacks. **(1) Data breach**: would need to attack card network/issuer servers that store consumer payment credentials. • Very low probability because of rigorous system architecture built on foundation of core payment networks that meet high standards of data protection, as well as issuer KYC and other security compliance requirements. **(2) Malware/virus**: multi-layered security and malware controls help prevent compromise of login credentials. • If payment token provisioned to wallet in lieu of PAN, fraudster would only gain access to token, not PAN. • However, if card network only encrypts consumer data without also using tokenization, probability of risk is MEDIUM. **(3) ATO**: while passwords may be vulnerable to compromise via ATO, these models perform additional validation at a device level to limit risk. • Magnitude of risk is also low because it affects one account and because of step-up authentication mechanisms in place.	MEDIUM to LOW MEDIUM to LOW MEDIUM to LOW	LOW LOW LOW
4. New account fraud	• Probability of risk MEDIUM. o Fraudsters can use previously breached credentials to create new wallet accounts. Wallets created without issuer integration are more at risk of new account fraud. • Magnitude of risk LOW. (1) Few merchants currently use this wallet model. (2) Controls exist to manage higher risk (e.g., high value or unusual) transactions. (3) Card networks have robust controls connected to issuer systems to limit new account fraud when adding accounts into the wallet to prevent the core account from being compromised.	MEDIUM	LOW

EMV ID&V	Masterpass is currently the only card network digital wallet that uses EMV ID&V processes to authenticate the consumer and provision a payment token to the wallet, so a payment token is stored on file rather than a PAN.		
1. Social engineering fraud	See explanation for Use Case 2 – Mobile In-app with EMV ID&V.		
AUTHENTICATION	• Card network wallets collect customer information such as name, email address, mobile phone number, device ID, and IP address. • Visa Checkout authenticates a customer for a transaction with an email address and password for the login. Masterpass customers can use their online banking credentials for authentication and to authorize purchases. • AmEx customers use their login credentials created for their americanexpress.com online account.		
1. Mobile man-in-the-browser (MiTB) attack 2. Spoofed authentication	• Fraudster uses card network digital wallet login credentials obtained from a data breach and attempts to make purchases using that wallet. • Probability and magnitude of risk are both LOW for a MiTB attack or other attacks on the authentication process, such as spoofing because: (1) Card networks use MFA, limiting the possibility of a MiTB attack. (2) If a high risk transaction is detected, the networks can use stepped-up authentication (e.g., OTP to an email address to via text to mobile phone). (3) Card networks use robust risk management systems to monitor cardholder and account behavior for anomalies to prevent fraudulent attacks.	LOW	LOW
MOBILE DEVICE/ OS INTEGRATION			
1. Mobile device rooting/jail breaking 2. Lost/stolen device 3. Malware/virus	• Probability and magnitude of risk are both LOW. (1) Tools are used to recognize rooted/jailbroken and lost/stolen devices and restrict access to the wallet (lost/stolen devices can be detected by analyzing device behavior). (2) No payment credentials stored on mobile device but stored on secure server (and risk is lower if a token is used in lieu of a PAN). (3) Card networks collect information about mobile device type and OS.	LOW	LOW
USE OF THIRD-PARTY PROVIDERS			
1. Data breach risk	• Probability of risk is MEDIUM. ○ Fraudster uses stolen online banking login credentials to gain access to a customer's bank account linked to digital wallet through participating issuer and uses wallet to pay for purchases. • Magnitude of risk LOW. ○ Issuer vets customers before CoF is activated in wallet.	MEDIUM	LOW

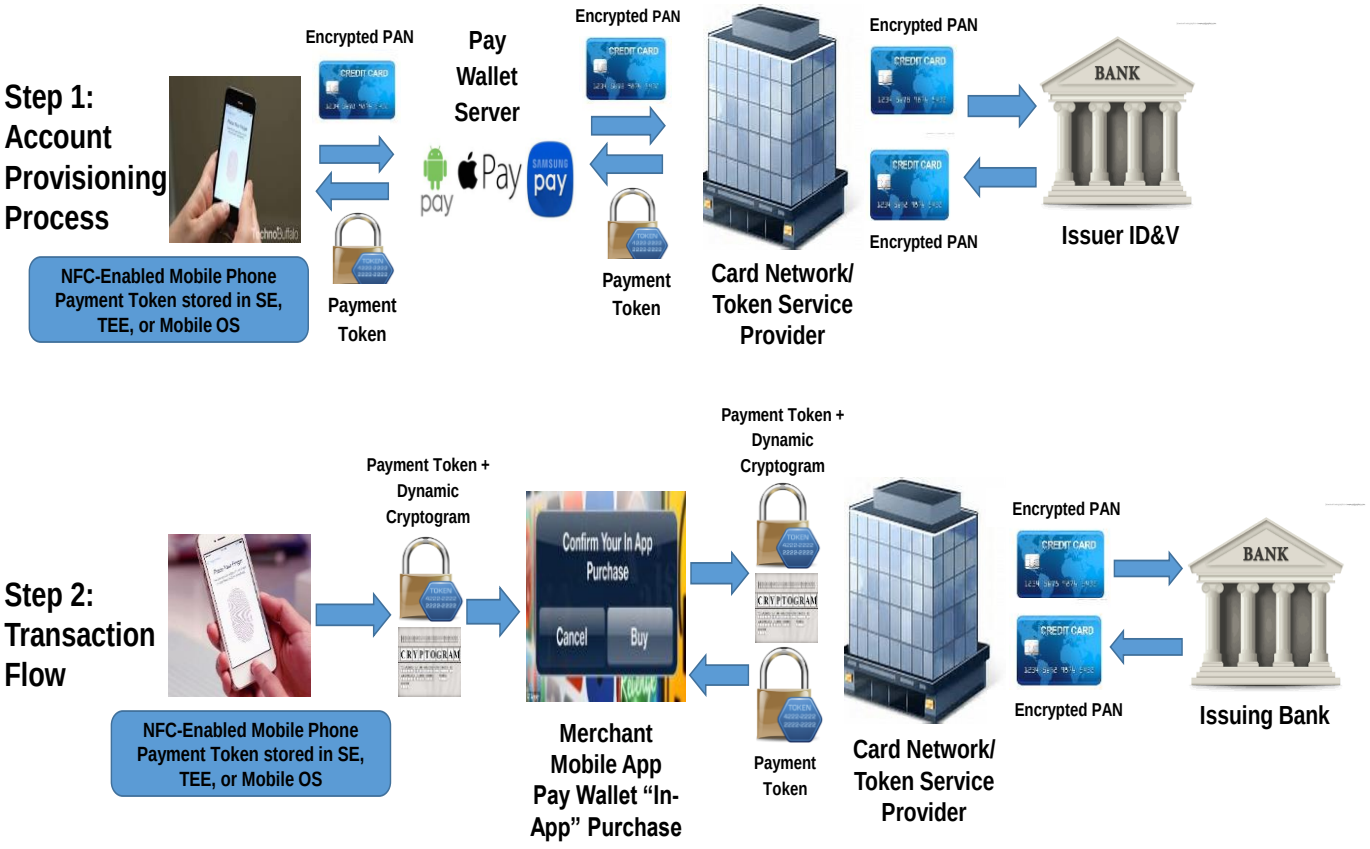
APPENDIX C: USE CASE TRANSACTION FLOWS

USE CASE 1: GUEST CHECKOUT WITH NO CARD-ON-FILE VIA MOBILE BROWSER OR MOBILE APP

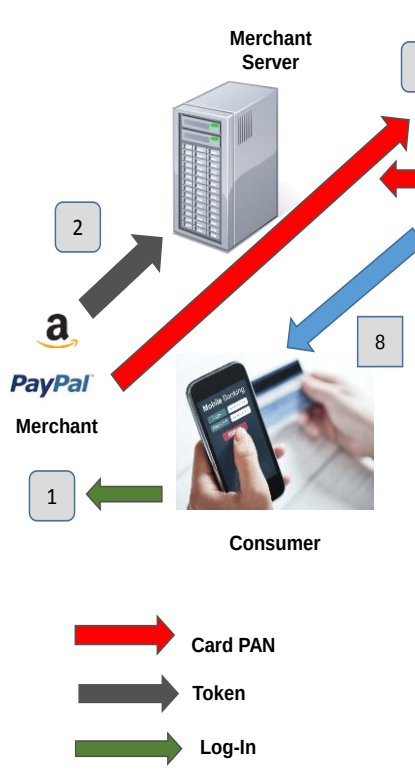


1. Consumer opens browser or merchant mobile app (already installed on device), populates shopping cart, proceeds to the checkout process and selects "guest checkout."
2. Consumer enters PAN, expiration date, and CVC (optional depending on merchant). Encrypted transaction data is transmitted to Merchant Server where it is decrypted using private key.
3. Merchant may use additional risk management tools before transmitting transaction to the Acquirer.
4. Acquirer logs transactions and sends to respective Card Network.
5. Card Network transmits to Card Issuer for authorization.
6. Authorization decision sent back by Card Issuer to Card Network.
7. Card Network sends authorization decision to Acquire.
8. Authorization decision sent to Merchant Server.
9. Transaction status message sent to consumer's mobile phone including truncated PAN (depending on merchant configuration and consumer notification preferences).

USE CASE 2: MOBILE IN-APP WITH EMV ID&V



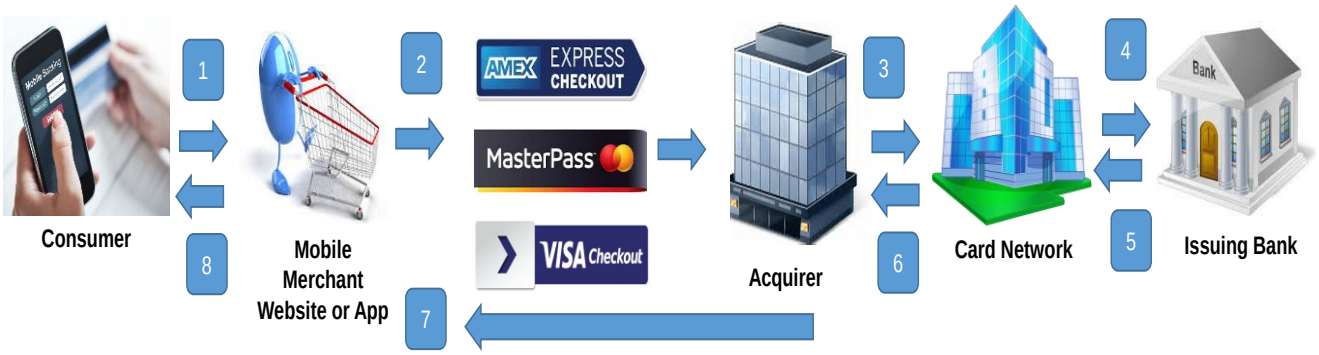
USE CASE 3: CLOUD-BASED WALLETS USING OTHER AUTHENTICATION APPROACHES



- Assumes consumer has previously created a wallet and login credentials with the PSP or merchant and has enrolled payment credential(s)/designated the default payment method for future purchases.
- Once an account has been created with a PSP or merchant, the payment credential is stored in an encrypted form or through a security tokenization process as a "card-on-file."

1. To make a purchase, consumer logins in to the PSP or merchant's mobile website or app to authenticate himself, selects goods and proceeds to checkout.
2. If Consumer uses a PSP for payment to the merchant, then the PSP recreates the original PAN from a security token stored on file and creates a transaction message that is sent to the Acquirer.
    - If the Consumer is using the CoF stored with the merchant, the authorization request is sent from the Merchant Server to the Acquirer.
3. Acquirer sends the request to the Card Network.
4. Card Network sends the request to the Card Issuer for authorization.
5. Card Issuer sends authorization decision back to the Card Network.
6. Card Network sends response to back to the Acquirer or the PSP.
7. Acquirer or PSP sends response back to Merchant.
8. PSP or Merchant sends confirmation/decline message to Consumer.

USE CASE 4: CARD NEWTORK DIGITAL WALLETS



- Assumes consumer has previously enrolled for a digital wallet with a card network.

1. To make a purchase (1): (a) Consumer logins in to the PSP or merchant's mobile website or mobile app to authenticate himself; or (b) Consumer proceeds with purchase using "guest checkout' on a PSP or merchant website/app. Consumer selects goods, proceeds to checkout, and selects preferred card network digital wallet. Assumes merchant integration with wallet to display "Wallet Checkout" logo on its website/app.
2. Consumer logs in to card network digital wallet to confirm shipping information and authorize payment. Some models may invoke 3DS if determined that stepped-up authentication is needed by the Bank Issuer (e.g., sending a OTP to the consumer for verification).
3. Acquirer sends the authorization request to the Card Network via API or ISO messaging (not all networks may offer an API).
4. Card Network sends the authorization request to Issuing Bank for a decision.
5. Issuing Bank sends authorization decision back to the Card Network.
6. Card Network sends authorization message to Acquirer.
7. Acquirer/Merchant sends confirmation message to Consumer based on consumer preferences and merchant system configuration.