SECURE PAYMENTS TASK FORCE

PAYMENT LIFECYCLE AND SECURITY PROFILE: Card Not Present (CNP)

INTRODUCTION TO THE PAYMENT LIFECYCLES AND SECURITY PROFILES

Consumers and organizations have a variety of options for making and receiving payments. While these payment types share the ultimate goal of transferring funds from payer to payee, the path those funds travel and the approaches employed for safely and securely completing transactions vary. The Secure Payments Task Force developed the Payment Lifecycles and Security Profiles as an educational resource and to provide perspectives related to:

- The lifecycles of the most common payment types, covering enrollment, transaction flow and reconciliation
- Security methods, identity management controls and sensitive data occurring at each step in the payment lifecycles
- Relevant laws and regulations, and other references, as well as challenges and improvement opportunities related to each payment type

The profiles employ a consistent format for describing the lifecycle of each payment type. The lifecycle template is not designed to represent the nuances of specific payment transaction flows, but as a broad taxonomy that can be applied across different payment types for understanding and comparing controls and risks. The profiles are not all-encompassing in describing the layered security strategies that may be employed by specific networks, providers or businesses and shouldn't be considered an assessment of overall security of different payment types. The improvement opportunities noted in the profiles highlight areas for further industry exploration and are not intended as guidance or specific solutions to be implemented.

These valuable resources were developed through the collaborative efforts of more than 200 task force participants with diverse payments and security expertise and perspectives. It is the hope of the task force that by helping industry stakeholders better understand these payments processes, the security and risks associated with these processes, and potential improvement opportunities, they will be well positioned to take action to strengthen their payment security practices.

The Card Not Present Payment Lifecycle and Security Profile maps out the lifecycle of a card not present payment to establish a common understanding of the payment journey and serves as an educational reference guide for payments and security stakeholders.

Payment Lifecycle and Security Profile information includes:

1) Payment Flow Overview
2) Payment Type Operation
3) Overview of Security Methods and Associated Risks
4) Inventory of Sensitive Payment Data and Associated Risks
5) Overview of Laws, Regulations and References on Payment Security (including Challenges and Improvement Opportunities)

CARD NOT PRESENT (CNP)

Definition: A payment card (e.g. credit or debit) funded transaction whereby the cardholder does not physically present the card for a merchant's visual examination at the time that an order is given and payment effected. This transaction may involve the cardholder typing his/her name, primary account number (PAN), one time use card number, virtual card number, account number, token, billing/shipping address, card verification code, biometric, pin, and/or expiration date into a payment access device which may include web or mobile based forms (e.g. internet browser, mobile browser, mobile application inclusive of in-app usage), or providing a portion of this information over the phone (mail order/telephone order – MOTO) to complete the purchase.

Note: These materials have been created by the Secure Payments Task Force and are intended to be used as educational resources. The information provided in the Payment Lifecycles and Security Profiles does not necessarily reflect the views of any particular individual or organization participating in the Secure Payments Task Force. The document is not intended to provide business or legal advice and is not regulatory guidance. Readers should consult with their own business and legal advisors.

PAYMENT FLOW OVERVIEW AND PAYMENT TYPE OPERATION

			GENERIC FUNCTIONAL STEP	CREDIT OPERATION	DEBIT OPERATION
ENROLLMENT			**Payer ID / Enrollment** Enrollment of a payer includes identity (ID) proofing, management of users (enrollment, de-enrollment, and changes) and determination of authority based on role	Individual or organization requests credit account with issuer. Issuer verifies customer information in accordance with their Know Your Customer (KYC) program. The Personal Identification Number (PIN) associated with the account may be communicated to the cardholder via direct outreach, email, or physical mail. For card not present authentication, merchant identifies required information based on relationship with customer; enrollment could mean the cardholder establishes an account or profile with the merchant.	Individual or organization requests debit account with issuer. Issuer verifies customer information in accordance with their KYC program. The PIN associated with the account may be communicated to the cardholder via direct outreach, email, or physical mail. For card not present authentication exercise, merchant identifies required information based on relationship with customer; enrollment could mean the cardholder establishes an account or profile with the merchant.
			Payee ID / Enrollment Enrollment of a payee includes identity (ID) proofing, management of users (enrollment, de-enrollment and changes) and determination of authority based on role	Acquirer approves merchant Merchant is registered in advance and identification data is attributed when registered by the acquirer.	Acquirer approves merchant
TRANSACTION	Payer Authentication	PAYMENTS/TRANSFERS FLOW IN BOTH DIRECTIONS	**Payer Authentication** Verification of payer when originating payments	Cardholder and card verification methods include Primary Account Number (PAN) or PAN alternative (Virtual PAN, Token) expiration date, Card Verification Values (CVV)[1], Address Verification Service (AVS), Card Holder Name, Mod 10 check, out-of-band authentication/verification. Payer authentication is ongoing (as merchants may perform some payer authentication controls pre-authorization and/or post-authorization and pre-shipment vs. post-shipment (pre-delivery).	Cardholder and card verification methods include PIN, PAN or PAN alternative (Virtual PAN, Token) expiration date, Card Verification Values[1], Address Verification (AVS), Card Holder Name, Mod 10 check, out-of-band authentication/verification. Payer authentication is ongoing (as merchants may perform some payer authentication controls pre-authorization and/or post-authorization and pre-shipment vs. post-shipment (pre-delivery).
	Initiation		**Access Mode / Network** Environment in which the payment origination is requested	Telephone, online, mobile, mail order	Telephone, online, mobile, mail order, cardless ATM transaction originated via a mobile device
			Device/Method Used to Initiate Payment Type of interaction or device used to enter payment account information	Online transactions: Internet-connected device (PC, smart phone, tablet) Telephone purchases: Phone and Point of Sale (POS) where merchant manually enters card information Mail order: paper form and POS where merchant manually enters card information Card on file payments: Card information held at the merchant Cloud wallet payments: App holds card information	Online transactions: Internet-connected device (PC, smart phone, tablet) Telephone purchases: Phone and POS where merchant manually enters card information Mail order: Paper form and POS where merchant manually enters card information Card on file payments: Card information held at the merchant. PIN entry via eCommerce (e.g. with a virtual PIN pad) Cloud wallet payments: App holds card information
			Funding Account for Payment Entry and/or identification of the funding account (with format checks)	Credit account	Demand Deposit Account (DDA)
			Payment Initiation Mechanism Payment network, system and/or third-party accessed	Merchant, acquirer, association or network, processor	Merchant, acquirer, association or network, processor
	Payer Authorization		**Payment Network Traversed** "Rails" used to route authorization requests to the holder of the funding account	Authorization occurs through payment networks (e.g. credit networks).	Authorization occurs through payment networks (e.g. debit networks)
			Transaction Authorization Determination of whether to approve or decline a transaction including authorization time-frame, obligations, and any recourse decisions	Transaction is confirmed but fulfillment may be delayed by merchant until fraud/ risk screening is complete and/or until guarantee of funds.	Transactions are approved or declined by the issuer within payment network service-level agreements (SLAs) (includes "stand-in" transactions)
	Format Exchange		**Format Exchange** Payment instructions, rules, and formatting	Acquirer authenticates merchant	As data is transferred, any conversion from one format to another, depending on payment network and brands. Payment network rules dictate format exchange rules.
	Receipt		**Acknowledgement/ Guarantee** Notification and confirmation of payment completion including terms for use		Transaction is confirmed but fulfillment may be delayed by merchant until fraud/ risk screening is complete and/or until guarantee of funds.
	Payee Authentication		**Payee Authentication** Mode of access to funds (or accounts)		Acquirer authenticates merchant
	Clearing and Settlement		**Settlement / Exchange of Funds** Actual movement of funds to settle funding arrangements and applicable fees	Settlement occurs per payment network rules (e.g. credit networks).	Settlement occurs per payment network rules (e.g. debit networks).
RECONCILIATION			**Reconciliation / Exception Handling** Process and responsibilities associated with reconciling and handling any exceptions or problems with a payment	Cardholder is required to report dispute within specified timeframe defined by payment network or card rules and regulations.	Cardholder is required to report dispute within specified timeframe defined by payment network or card rules and regulations.
			User Protection / Recourse Applicable rules, regulations, and legal means of recourse	Determined by payment network rules and applicable consumer protection laws and regulation Regulation Z's consumer protections apply to consumer credit.	Determined by payment network rules and applicable consumer protection laws and regulations. Regulation E's consumer protections apply to consumer debit.

OVERVIEW OF SECURITY METHODS AND ASSOCIATED RISKS

		SECURITY METHODS	RISKS
ENROLLMENT	PAYER ID / ENROLLMENT	Issuer verifies the individual during enrollment before issuing a card. KYC, Customer Identification Program (CIP) background checks, etc.; ID verification of a 'carbon-based life form' Employee training Issuers may utilize anomaly and fraud detection tools to help identify suspicious or fraudulent activity associated with a specific account or group of accounts.	Social engineering (e.g. call center or end user) which could include business email compromise, masquerading fraud, imposter fraud, etc. Account takeover Synthetic Identity: Use of stolen identity information combined with fraudulent information to create a new 'synthetic' identity which is used to open fraudulent accounts and make fraudulent purchases. Strong enrollment processes may help mitigate synthetic identity risk throughout the transaction process. Credential stuffing (e.g. automated injection of breached username/ password pairs in order to fraudulently gain access to user accounts) Knowledge-based questions can be compromised.
	PAYEE ID / ENROLLMENT	Acquirer (or the agent of the acquirer) verifies the individual(s) or organizations enrolling as a merchant before establishing a merchant ID (KYC, CIP, background checks, etc.) Employee training	An individual could create a fake merchant or consumer account which could lead to a 'bust-out' situation. Synthetic Identity: Use of stolen identity information combined with fraudulent information to create a new 'synthetic' identity which is used to open fraudulent accounts and make fraudulent purchases. Strong enrollment processes may help mitigate synthetic identity risk throughout the transaction process.
TRANSACTION		Mod 10 check and pre-authorization fraud prevention services offered by fraud service providers/other providers (e.g. 3D Secure authentication, device identification, finger printing, etc.) Participants in the payment transaction (e.g. merchants, acquirers/processors, payment networks, and issuers) may utilize anomaly and fraud detection tools to help identify risks and mitigate fraudulent transactions. Anomaly and fraud detection tools may include transaction risk scoring, risk-based authentication, transaction history and real-time authorization/ decline capabilities among others. Validate the integrity of the payment message. Review message format for inconsistencies. Employee training Consumer and corporate customer education Controls for device used to initiate payment merchant risk controls differ based on device/method used to initiate payment (e.g. some merchants may perform CNP in-store transactions) Some differences in controls for the above methods (e.g. 3D Secure is online only) For online, telephone, and mail order transactions merchant may conduct AVS and CVV[1] checks, and may perform identity checks. • For online transactions: may also deploy 3D Secure • For telephone transactions: may also verify phone number • For mail order transactions: may verify signature Encryption technologies can be used for card-on-file and online transactions As payments and technology continue to change, risk-based authentication is a way to continually evaluate and apply optimal security methods.	Account takeover Social engineering (e.g. call center or end user) which could include business email compromise, masquerading fraud, imposter fraud, etc. Machine takeover (payee, financial institutions, network/operator, payer) Transaction data may be altered or spoofed (e.g. counterfeit transactions, credit master attacks, brute force attacks, etc.) First party/theft/lost or stolen transactions Credential stuffing (e.g. automated injection of breached username/ password pairs in order to fraudulently gain access to user accounts) Sole reliance on a point in time compliance statement (minimal, "check the box" compliance does not equal security) Some POS systems/applications transmit and/or store card data in the clear. End-to-end encryption is not universally applied in POS systems/applications. Inadequately-controlled enrollment often poses additional risk at the time of transaction. The speed of payment processing and reconcilement may impact the ability to identify fraud in time to recover funds.
RECONCILIATION	RECONCILIATION / EXCEPTION HANDLING	Participants in the original payment transaction may utilize anomaly and fraud detection tools to identify suspicious patterns of activity that may warrant further investigation or potential modifications to transaction anomaly and fraud detection tools.	
	USER PROTECTION / RECOURSE		

INVENTORY OF SENSITIVE PAYMENT DATA AND ASSOCIATED RISKS

		SENSITIVE PAYMENT DATA (DATA THAT NEEDS TO BE PROTECTED)	RISKS ASSOCIATED WITH THE SENSITIVE PAYMENT DATA
		Sensitive payment data must be protected wherever it is processed, stored or transmitted	
ENROLLMENT	PAYER ID / ENROLLMENT	**Sensitive data used to enroll or open an account:** *Any data that is inputted by the user (e.g. email, usernames, passwords* Name | Date of Birth | Address | Social Security Number | Demand Deposit Account Number (DDA) | Signature	If compromised, this data can be used to fraudulently set up an account at a financial institution and be used for other identity theft crimes.
	PAYEE ID / ENROLLMENT	**Sensitive data used to enroll or open a merchant account:** Name | Date of Birth | Address | Social Security Number | Demand Deposit Account Number (DDA) | Signature | Business Name | Tax ID	If compromised, someone that is not a merchant could create a fake merchant account. This could also occur if the merchant account is not fully vetted / authenticated prior to setting up the merchant account.
TRANSACTION		**The following data is considered Sensitive Payment Data:** **Cardholder Data:** *Cardholder data must be protected wherever it is processed, stored or transmitted.* Primary Account Number (PAN) Cardholder Name Expiration Date **Sensitive Authentication Data:** *Sensitive Authentication Data must be protected and must not be stored after authorization of the transaction.* CVVs[1] PINs/PIN Blocks Encryption Keys PIN Offsets	Compromised cardholder data can be used by a criminal to create a fake credit/debit card for keyed, card present fraud (e.g. the magnetic stripe or chip are not properly encoded and the merchant keys in the card number at the terminal) as well as card not present fraud at merchants that do not validate CVVs[1] (or where the fraudster has already obtained the CVVs[1]) Compromised sensitive authentication data can be used in conjunction with compromised cardholder data to create counterfeit credit/debit cards that can be used as if they were the actual cardholder.
	PAYEE AUTHENTICATION	Merchant ID | Terminal ID | Terminal address | Merchant category code (MCC) | Terminal country code | Transaction currency code | Transaction type | Terminal entry capability | Merchant name	If compromised, this data may be used to submit fraudulent payments into the payments system, especially for card testing purposes. If compromised, someone that is not a merchant could spoof a legitimate merchant.
	CLEARING AND SETTLEMENT	Issuing bank ABA (routing) number | Issuing bank settlement account number | Merchant bank ABA number | Merchant settlement account number	If compromised, this data may be used to make fraudulent debits to the settlement accounts.
RECONCILIATION	RECONCILIATION / EXCEPTION HANDLING	Merchant ID **Cardholder Data:** *Cardholder data must be protected wherever it is processed, stored or transmitted* Primary Account Number (PAN) | Cardholder Name | Expiration Date	If compromised, someone that is not a merchant could spoof a legitimate merchant. Compromised cardholder data can be used by a criminal to create a fake credit/debit card for keyed, card present fraud (e.g. the magnetic stripe or chip are not properly encoded and the merchant keys in the card number at the terminal) as well as card not present fraud at merchants that do not validate CVVs[1] (or where the fraudster has already obtained the CVVs[1])
	USER PROTECTION / RECOURSE		

[1] Card Verification Values: Card Verification Values represent data elements that are (1) encoded on the magnetic stripe or the chip of a payment card; or (2) printed on the physical payment card and are used to validate the card information during the transaction authorization process. Card Verification Values encoded on the magnetic stripe (e.g. CAV, CVV, CVC, CSC) or on the chip (e.g. dCVV, iCVV) are generated via a secure cryptographic process and may be static or dynamic data used to validate the card during the authorization process. Card Verification Values printed on the physical card (e.g. CID, CAV2, CVC2, CVV2) may be three-digit or four-digit codes printed on the front or back of the physical card that are uniquely associated with the physical card and ties the primary account number to the physical card. Note: Payment network rules and the Payment Card Industry (PCI) Security Standards Council provide additional definitions of Card Verification Values.

OVERVIEW OF LAWS, REGULATIONS AND REFERENCES ON PAYMENT SECURITY
(INCLUDING CHALLENGES AND IMPROVEMENT OPPORTUNITIES)

LEGAL AND REGULATORY REFERENCES

Debit cards (consumer) – Electronic Fund Transfer Act (EFTA), 15 U.S. Code (U.S.C.) § 1693 *et seq.;* Regulation E. 12 Code of Federal Regulation (CFR) § 1005.2 *et seq.* (EFTA applies only to accounts "established primarily for personal, family, or household purposes" 15 U.S.C. § 1693a(2))

Credit cards (consumer) – Truth in Lending Act (TILA), 15 U.S.C. § 1601 *et seq.;* Regulation Z. 12 CFR § 1026.1 *et seq.* (TILA exempts "extensions of credit primarily for business, commercial, or agricultural purposes, or to governmental agencies or instrumentalities, or to organizations")

Prepaid cards (consumer) – Under Consumer Financial Protection Bureau (CFPB) Prepaid Accounts Rule (81 Fed. Reg. 83934 (November 22, 2016)) (to be codified at 12 CFR pts. 1005 and 1026), as amended on January 25, 2018, and effective April 1, 2019, Regulation E would apply to prepaid cards, with Regulation Z expanded to apply to prepaid cards with certain credit features.

Financial Crimes Enforcement Network (FinCEN) Bank Secrecy Act, 31 U.S.C. § 5311, *et seq.;* 31 CFR § 1010.100, *et seq.* (implementing regulations); Federal Financial Institutions Examination Council (FFIEC), *Bank Secrecy Act/Anti-Money Laundering Examination Manual* (2014).

Customer Identification Program (CIP), 31 CFR § 1020.220, *et seq.*

Identity Theft Red Flags Rules, 12 CFR § 41.90 (OCC); 12 CFR § 222.90 (FRB); 12 CFR § 334.90 (FDIC); 12 CFR § 717.90 (NUCA); 16 CFR § 681.1 (FTC); 17 CFR § 162.30 (CFTC); 17 CFR § 248.201 (SEC)

Board of Governors of the Federal Reserve System, Guidance on Managing Outsourcing Risk (Dec. 5, 2013) – FRB SR 13-19: Third party oversight guidance, set of cyber-risk oversight activities which includes reporting and expectations for Boards of Directors and Senior Management.

FFIEC IT Exam Handbooks: Some of the handbooks are more frequently a factor in exams, but they all contain provisions that impact payments compliance in the areas of confidentiality, availability, data integrity, privacy and third party oversight.

- **FFIEC,** *IT Examination Handbook, Information Security* (Sept. 2016)
- **FFIEC,** *IT Examination Handbook, Retail Payment Systems* (Apr. 2016)
- **FFIEC,** *IT Examination Handbook, Supervision of Technology Service Providers* (Oct. 2012)

FFIEC, *Authentication in an Internet Banking Environment* (Oct. 12, 2005); FFIEC, *Supplemental to Authentication in an Internet Banking Environment* (June 28, 2011)

Gramm-Leach-Bliley Act (1999), 15 U.S.C. § 6801 *et seq.*

Regulation P, Privacy of Consumer Financial Information 12 CFR 1016.1 *et seq.;* – enacted to control how financial institutions manage the private information of individuals. In addition, the Interagency Guidelines Establishing Standards for Safeguarding Customer Information include provisions associated with the role of risk management, boards and third party oversight.

Federal Trade Commission Act (1914), 15 U.S.C. § 45(a) (prohibiting "unfair or deceptive acts or practices in or affecting commerce"); 16 CFR § 314.3 (requiring companies to develop written information security programs to protect customer information)

Consumer Financial Protection Act of 2010, 15 U.S.C. § 5531 *et seq.* (prohibiting "unfair, deceptive, or abusive act[s] or practice[s]. . ." in consumer finance)

State-based cybersecurity and breach laws: A challenge due to the variation among those sets of regulation which include:

- All 50 States address unauthorized access, malware and viruses
- 20 States address spyware
- 23 States address phishing

Source: National Conference of State Legislatures

International cybersecurity regulations and related data-protection laws: Vary widely and continue to evolve; e.g. European Union General Data Protection Regulations (May 2018); Japan: The Act on the Protection of Information (May 2017)

Office of Foreign Assets Control (OFAC)/Sanction Screening

OTHER REFERENCES

American National Standards Institute (ANSI) X9.122 Secure Customer Authentication for Internet Payments – draft in approval stage

- Requirements for secure customer authentication for electronic payment transactions over multiple channels initiated through the interchange system (debit/credit network) via internet, mobile or voice channels
- Covers passcodes, passwords, biometrics, magnetic stripe authentication values, cryptography, small device authentication, and vendor considerations

ANSI X9-112-3 Mobile Banking and Payments – draft in approval stage

- Addresses identity verification and authentication technology standards for passcode authentication, biometrics authentication, device recognition, and single-sign-on federated identity
  - Cryptographic processes to support tokenization functions
  - Maintenance of underlying token security and related processing controls, such as domain restrictions during transaction processing. Developed out of ISO 12812-2. Published based on differences for the U.S. markets and current payment technologies

International Organization for Standardization (ISO) 12812 Core Banking – MFS – Technical Specification (TS) Part 2: Security and Data Protection for MFS

ANSI X9.8 and X9.24 and ISO 9564 PIN Management and Security Standards

- These standards prohibit online entry of a PIN. Must be an approved hardware cryptographic device (HCD)
- This eliminates online authentication models such as Randomized PIN Pad

Fast Identity Online (FIDO) Alliance specifications

- FIDO protocols are based on public key cryptography for resistance to phishing. There are two:
  - FIDO Alliance Universal Authentication Framework (UAF) specs
  - FIDO Alliance Universal 2nd Factor (U2F) specs with Bluetooth and NFC transports
- Expanding globally
- EMVCo and FIDO Alliance have recently signed a Memorandum of Understanding to determine how and when payment use cases provided by EMVCo could be incorporated into the FIDO Alliance's technical standards.

W3C Web Authentication Specifications for Secure Internet (Web API)

- Application program interface (API) specifications designed to provide a robust authentication process that mitigates the threat of phishing or man-in-the-middle fraud attacks, by implementing cryptography-based solutions for authentication of users to web applications.
- This standard also ensures consistency and interoperability with the FIDO and OAuth specifications.

W3C Web Payment Specifications – one web payment interface for all payment types

- Payment Request API
- Payment Method Identifiers
- Basic Card Payment Specifications

W3C One-Click Online Payment Model – work group effort kicked off in September 2016

- Goal is to devise a system similar to Amazon's one-click payment system

EMV Payment Tokenization Specification – Technical Framework

- Payment Tokens are surrogate values that replace the Primary Account Number (PAN) in the payments ecosystem. They may be used to originate payment transactions, while non-payment tokens may be used for ancillary processes, such as loyalty tracking. This specification does not address non-payment tokens, but does not does preclude their use.

Source: https://www.emvco.com/

EMV 3-D Secure 2.0

- To reflect current and future market requirements, the payments industry recognized the need to create a new 3-D secure specification that would support app-based authentication and integration with digital wallets, as well as traditional browser-based eCommerce transactions. This led to the development of EMV 3-D Secure – Protocol and Core Functions Specification v2.1.0. The specification takes into account these new payment channels and supports the delivery of industry leading security, performance and user experience.
- EMV 3-D Secure Software Development Kit (SDK) Specification

Source: https://www.emvco.com/emv-technologies/3d-secure/

Payment Card Industry (PCI) Data Security Standard (DSS) – Requirements and Security Assessment Procedures

- Developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. It provides a baseline of technical and operational requirements designed to protect account data and applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers. PCI DSS also applies to all other entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD).

Source: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf?agreement=true&time=1484000182971

PCI Payment Application Data Security Standard (PA-DSS) – Requirements and Security Assessment Procedures

- Define security requirements and assessment procedures for software vendors of payment applications. This document is to be used by Payment Application Qualified Security Assessors (PA-QSAs) conducting payment application assessments to validate that a payment application complies with the PA-DSS.
- Secure payment applications, when implemented in a PCI DSS-compliant environment, will minimize the potential for security breaches leading to compromises of Primary Account Number (PAN), full track data, Card Verification Values[1], PINs and PIN blocks, and the damaging fraud resulting from these breaches.

PCI Point-to-Point-Encryption (P2PE) – Solution Requirements and Testing Procedures

- Defines both requirements and testing procedures for P2PE solutions. The objective of this standard is to facilitate the development, approval, and deployment of PCI approved P2PE solutions that will increase the protection of account data by encrypting that data from the point of interaction within the encryption environment where account data is captured through to the point of decrypting that data inside the decryption environment, effectively removing clear-text account data between these two points.
- The requirements contained within this standard are intended for P2PE solution providers and other entities that provide P2PE components or P2PE applications for use in P2PE solutions, as well as P2PE assessors evaluating these entities. Additionally, merchants benefit from using P2PE solutions due to increased protection of account data and subsequent reduction in the presence of clear-text account data within their environments.

PCI P2PE – Encryption, Decryption, and Key Management within Secure Cryptographic Devices (Hardware/Hardware)

- Provides a method for providers of P2PE solutions to validate their solutions, and for merchants to reduce the scope of their PCI DSS assessments when using a validated P2PE solution for account data acceptance and processing. Specifically, this version contains validation requirements and testing procedures for hardware-based encryption and decryption solutions, also called "hardware/hardware." Hardware/hardware solutions utilize secure cryptographic devices for both encryption and decryption including at the point of merchant acceptance for encryption, and within hardware security modules (HSMs) for decryption.
- The requirements in this document are intended to apply in addition to applicable PCI DSS requirements to the token data environment (TDE). The TDE is a dedicated, secure area within the token service provider (TSP), where one or more of the following services are performed:
  - Token generation, issuing, and mapping processes
  - Assignment of token usage parameters
  - Token lifecycle management
  - Processes to map or re-map tokens, or perform de-tokenization

PCI P2PE – Encryption and Key Management within Secure Cryptographic Devices, and Decryption of Account Data in Software (Hardware/Hybrid)

- This document for hardware/hybrid point-to-point encryption solutions provides a method for providers of P2PE solutions to validate their solutions, and for merchants to reduce the scope of their PCI DSS assessments when using a validated P2PE solution for account data acceptance and processing. Specifically, this version contains validation requirements and testing procedures for hardware/hybrid solutions which utilize secure cryptographic devices at the point of merchant acceptance for encryption and for managing cryptographic keys in the decryption environment while utilizing non-SCDs for the decryption of account data.

PCI Token Service Providers (TSP) – Additional Security Requirements and Assessment Procedures for Token Service Providers (EMV Payment Tokens)

- Describes the logical security requirements required of entities that:
  - Perform cloud-based or secure element (SE) provisioning services
  - Manage over-the-air (OTA) personalization, lifecycle management, and preparation of personalization data
  - Manage associated cryptographic keys

PCI Card Production and Provisioning – Physical Security Requirements

- A comprehensive source of information for entities involved in card production and provisioning, which may include manufacturers, personalizers, pre-personalizers, chip embedders, data-preparation, and fulfillment
- The contents of this manual specify the physical security requirements and procedures that entities must follow before, during, and after the following processes:
  - Perform cloud-based or secure element (SE) provisioning services; card manufacturing, chip embedding, personalization, storage, packaging, mailing, shipping or delivery, fulfillment

PCI Card Production and Provisioning – Logical Security Requirements

- All systems and business processes associated with the logical security activities associated with card production and provisioning such as data preparation, pre-personalization, card personalization, PIN generation, PIN mailers, and card carriers and distribution must comply with the requirements in this document.
- This document describes the logical security requirements required of entities that:
  - Perform cloud-based or secure element (SE) provisioning services;
  - Manage over-the-air (OTA) personalization, lifecycle management, and preparation of personalization data; or
  - Manage associated cryptographic keys.
- Wherever the requirements specify personalization, the requirements also apply to cloud-based provisioning networks (e.g., those for host card emulation). Cloud-based systems differ from those based on requiring the use of a secure element on a mobile device.

National Institute of Standards and Technology (NIST) Cybersecurity Framework

FFIEC Cybersecurity Assessment Tool

Payment network rules
(e.g. Visa, MasterCard, American Express, Discover Network, JCB and debit card networks)

CHALLENGES AND IMPROVEMENT OPPORTUNITIES

Standards designed for card present environments may not be applicable for authentication methods used in card not present environments.

There are rules, guidance, and frameworks that address debit/credit card authentication and security in CNP environments, which could be further developed to promote innovation and enhanced security. Moreover, at the time of publication, there are industry groups working to develop standards that may address this item.

Payments stakeholders employ various methods and processes to comply with relevant state and federal regulations regarding customer onboarding as well as relevant private sector protocols. Greater focus on the development and adoption of standards related to online registration or mobile enrollment could enhance security.

ANSI X9AB currently working on a technical report which will provide CNP Fraud Mitigation Best Practice guidelines (TR48); yet to be determined if any standards will come out of this effort.

Improvements to the quality and accuracy of data collected and used to facilitate mail order, telephone order, recurring payments, one-time card on file and card present key entry payments may help further mitigate payments risk. Participants who collect, process, or authorize transactional data play an important role in ensuring the accuracy of data submitted. This includes ensuring that hardware and software are properly configured. Participants may use this information as part of their authentication decision process, making accuracy an important priority.

There are industry standards, rules, guidance, and frameworks that currently apply to digital payments for card-to-card (and account) payments and transfers which could be further developed to promote further innovation and security.

Generic card-on-file systems need to be interoperable to the extent possible.

Greater deployment of tokenization, user authentication and encryption based on open standards could enhance payment security.

Greater focus on development and adoption of risk-based cybersecurity rules, frameworks, and open standards could enhance security.

Proliferation of groups proposing to develop standards for eCommerce and commerce hold potential for incompatibilities and unneeded duplication in security protocols.