SECURE PAYMENTS TASK FORCE

PAYMENT LIFECYCLE AND SECURITY PROFILE: Check

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 Check Payment Lifecycle and Security Profile maps out the lifecycle of a check 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).

CHECK

Definition: A check payment is a negotiable instrument drawn against deposited funds and used to pay a specific entity a specific amount of funds on demand. A check is routed from the payer to the payee and deposited at the payee's financial institution. Some or all funds are made available to the payee on deposit and the item is routed to the payer's financial institution for settlement. The payer's financial institution shifts funds from the payer's account upon receipt of the item. Historically, paper checks were physically routed, but today, much of check routing is done electronically.

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

				PAPER CHECK	CHECK 21 / ELECTRONIC	ELECTRONIC FUNDS TRANSFER (EFT) CONVERSION
			GENERIC FUNCTIONAL STEP	**Note: there is potential movement between paper and Check 21/electronic check**	**(Remote Deposit Capture and Mobile Remote Deposit Capture)**	**Note: EFT transactions are addressed in the ACH Payment Lifecycle and Security Profile and treated as ACH Debit transactions.**
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	Financial Institution onboards account holder utilizing Know Your Customer (KYC) and underwriting	Financial Institution onboards account holder utilizing Know Your Customer (KYC) and underwriting	Financial Institution onboards account holder utilizing Know Your Customer (KYC) and underwriting
			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			
TRANSACTION	Payer Authentication	**PAYMENTS FLOW IN BOTH DIRECTIONS**	**Payer Authentication** Verification of payer when originating payments	Payee of check may choose to request personal identification information from the payor.	Payee of check may choose to requestw personal identification information from the payor.	Payee may choose to request personal identification information from the payor.
	Initiation		**Access Mode / Network** Environment in which the payment origination is requested	Typically, a check enters the bank to bank check collection system when the payee or a transferee deposits the check into their bank account at the Bank of First Deposit. Alternatively, the payee or transferee may present the item directly to the paying bank.	The payee or the payee's financial services provider truncates the paper check and creates an electronic image of the check to go through the clearing process to the payor's financial institution	Vendor creates ACH transaction and transmits data to vendor's financial institution.
			Device/Method Used to Initiate Payment Type of interaction or device used to enter payment account information	The device used to initiate payments is the issuance of a paper check from the drawer to the payee. Payee or transferee may deposit the check to her bank in paper form or as an image. Alternatively, the payee or transferee presents the paper check directly to the paying bank for payment The Bank of First Deposit may image the check and clear the check as an image.	The electronic image of the check is sent to the payor's financial institution, local clearing house exchange, or a collecting financial institution. Images typically are retained for purposes of record keeping laws and for reconciliation of exceptions.	Point of sale or mail check to vendor for back office conversion to ACH.
			Funding Account for Payment Entry and/or identification of the funding account (with format checks)	Typically, the Bank of First Deposit settles with its depositor by crediting the depositor's account. The depositary bank obtains credit for an item by sending it forward for collection. At each step in bank to bank collection, a credit is settled to an account of the transferring or presenting bank, and a debit is settled to the account of the subsequent collecting bank or the paying bank. The paying bank obtains credit for the item debiting the drawer's account.	Account holders can transmit check data directly to their financial institution so no physical deposit of check is necessary. Typically, the Bank of First Deposit settles with its depositor by crediting the depositor's account. The depositary bank obtains credit for an item by sending it forward for collection. At each step in bank to bank collection, a credit is settled to an account of the transferring or presenting bank, and a debit is settled to the account of the subsequent collecting bank or the paying bank. The paying bank obtains credit for the item debiting the drawer's account.	Settlement for check to ACH converted items takes place as provided by the ACH operator's agreement with its participating depository financial institutions.
			Payment Initiation Mechanism Payment network, system and/or third-party accessed	The method for initiating a check transaction is the issuance of a paper check. Each transfer or presentment of a check, whether paper or image, is legally a separate transaction that is initiated by delivering the item with the intention of giving the recipient the right to enforce the item.	The transfer of an imaged item from the payee or transferee to a Bank of First Deposit is typically initiated by secure electronic connections, using an app for remote deposit capture.	
	Payer Authorization		**Payment Network Traversed** "Rails" used to route authorization requests to the holder of the funding account			ACH Network
			Transaction Authorization Determination of whether to approve or decline a transaction including authorization time-frame, obligations, and any recourse decisions	The Bank of First Deposit may decide whether or not to accept a check deposit, as long as the account agreement provides for it.	The Bank of First Deposit may decide whether or not to accept a check deposit, as long as the account agreement provides for it. Bank of First Deposit may have additional edits for imaged items that must be met before an item will be accepted for deposit.	
	Format Exchange		**Format Exchange** Payment instructions, rules, and formatting	Banks typically accept deposits of paper checks that conform to applicable ANSI standards.	For remote deposit, all of the technical and operational standards are typically controlled by the depository bank and/or its IT service provider. In bank to bank image exchange, format exchange is determined in exchange/clearing agreement. The industry default standard is ANSI X9.100-187, but this may be varied by agreement.	NACHA rules and formats apply.
	Receipt		**Acknowledgement/ Guarantee** Notification and confirmation of payment completion including terms for use	Paper check is retained by depository financial institution and then destroyed per retention policy.	Check 21 data is captured, retained, and destroyed by depository financial institution per retention policy.	When data is captured for creation of ACH transaction, the paper check is destroyed by the vendor (typical for backroom conversions) or voided and returned to the consumer (typical for point of sale conversions).
	Payee Authentication		**Payee Authentication** Mode of access to funds (or accounts)			
	Clearing and Settlement		**Settlement / Exchange of Funds** Actual movement of funds to settle funding arrangements and applicable fees	Interbank settlement for checks may be structured by clearing house rules, Federal Reserve Operating Circular, or by bank to bank agreement. In the absence of agreement, bank to bank settlement is made by cash or transfer to the Federal Reserve account of the bank receiving settlement.	Interbank settlement for checks may be structured by clearing house rules, Federal Reserve Operating Circular, or by bank to bank agreement. In the absence of agreement, bank to bank settlement is made by cash or transfer to the Federal Reserve account of the bank receiving settlement.	ACH clearing effects interbank settlement on Federal Reserve accounts or directly between financial institutions in accordance with established agreements.
RECONCILIATION			**Reconciliation / Exception Handling** Process and responsibilities associated with reconciling and handling any exceptions or problems with a payment	The paying bank must initiate a return prior to its "midnight deadline" if it decides to dishonor a check presented by another bank. Bank to bank clearing arrangements may provide for automated means of asserting claims or requesting information related to exceptions. Warranty and indemnity claims may be asserted using requests for "adjustments" by agreement. Legal redress for breaches of warranty or for indemnity claims is available for the duration of the applicable statute of limitations. Claims based on negligence typically have a shorter time limit.	The paying bank must initiate a return prior to its "midnight deadline" if it decides to dishonor a check presented by another bank. Bank to bank clearing arrangements may provide for automated means of asserting claims or requesting information related to exceptions. Warranty and indemnity claims may be asserted using requests for "adjustments" by agreement. Legal redress for breaches of warranty or for indemnity claims is available for the duration of the applicable statute of limitations. Claims based on negligence typically have a shorter time limit.	Governed by ACH rules.
			User Protection / Recourse Applicable rules, regulations, and legal means of recourse	Checks are governed by the Uniform Commercial Code, various federal statutes (Expedited Funds Availability Act, C21 Act), and Regulation CC. These rules may be varied or expanded by clearing house rules, Federal Reserve Operating Circulars, or agreements that may be bilateral or unilateral.	Checks are governed by the Uniform Commercial Code, various federal statutes (Expedited Funds Availability Act, C21 Act), and Regulation CC. These rules may be varied or expanded by clearing house rules, Federal Reserve Operating Circulars, or agreements that may be bilateral or unilateral.	Governed by ACH rules. Consumer EFTs are subject to Regulation E.

OVERVIEW OF SECURITY METHODS AND ASSOCIATED RISKS

		SECURITY METHODS	RISKS
ENROLLMENT	PAYER ID / ENROLLMENT	Issuer verifies the individual during enrollment before issuing an account. Know Your Customer (KYC), Customer Identification Program (CIP) background checks, etc.; ID verification of a "carbon-based lifeform" Employee training	Financial institution legacy accounts may lack Know Your Customer (KYC). Social Engineering, which could include business email compromise, masquerading fraud, imposter fraud, etc. 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.
	PAYEE ID / ENROLLMENT	Know Your Customer (KYC) and Customer Identification Program (CIP) Employee training	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		Fraud mitigation services where Data From Enforcement (DFE) can verify the status of the payor's Demand Deposit Account (DDA) Employee training Consumer and corporate customer education Magnetic Ink Character Recognition (MICR), microprint and other document-related security checks to affirm the integrity of the check As payments and technology continue to change, risk-based authentication is a way to continually evaluate and apply optimal security methods.	Limited opportunity to authenticate the payor at payment initiation ABA routing gap Remote Deposit Capture (RDC) / multiple deposit risk at financial institutions Social Engineering, which could include business email compromise, masquerading fraud, imposter fraud, etc. 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		
	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: Name | Date of Birth | Address | Social Security Number	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		
TRANSACTION		Account Holder Data (must be protected wherever it is processed, stored or transmitted): Company Name (Originator) Payor Address Payor Phone Number (if provided) Payor Driver’s License Number (If provided) Payor Signature Payor Financial Institution ABA Payor Account Number Check Image Payee Account Data from Endorsement: Payee‘s Signature from Endorsement Payee’s Account Number Payee’s Financial Institution ABA	Compromised check data, such as routing transit and deposit account numbers, may be used by a criminal to create or print fraudulent/ counterfeit checks or to make payments over the phone. Additional data compromised could be used for fraudulent account set-up and account takeover (account data, invoice data, address data, signature).
	PAYEE AUTHENTICATION		
	CLEARING AND SETTLEMENT		
RECONCILIATION	RECONCILIATION / EXCEPTION HANDLING		
	USER PROTECTION / RECOURSE		

OVERVIEW OF LAWS, REGULATIONS AND REFERENCES ON PAYMENT SECURITY

(INCLUDING CHALLENGES AND IMPROVEMENT OPPORTUNITIES)

LEGAL AND REGULATORY REFERENCES

Federal Reserve Operating Circular 3 (OC 3) Collection of Cash Items and Returned Checks

Uniform Commercial Code Articles 3 (Negotiable Instruments) and 4 (Bank Deposits and Collections) (as adopted by the states)

Regulation CC: Availability of Funds and Collection of Checks, 12 CFR § 229.1 *et seq.*

Expedited Funds Available Act, 12 U.S.C. § 4001 *et seq.*

Regulation DD: Truth in Savings (maximum limits of number / amounts of deposits), 12 CFR § 1030.1 *et seq.*

Check Clearing for the 21st Century, 12 U.S.C. § 5001 *et seq.*

Regulation J: Collection of Checks and Other Items By Federal Reserve Banks, 12 CFR § 210.25 *et seq.*

Financial Crimes Enforcement Network (FinCEN) Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) compliance, 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)

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

- **FFIEC,** Authentication in an Internet Banking Environment (October 12, 2005) FFIEC, Supplemental to Authentication in an Internet Banking Environment (June 28, 2011)
- **FFIEC,** Risk Management of Remote Deposit Capture (January 14, 2009)
- Vendors/third-party processors typically provide MRDC solutions to financial institutions. Likely managed through contracts and regulations, not standards.
- See FFIEC IT Handbook: http://ithandbook.ffiec.gov/it-booklets/retail-payment-systems/payment-instruments,-clearing,-and-settlement/check-based-payments/remote-deposit-capture.aspx

Remotely Created Check (RCC)

- **FFIEC,** Authentication in an Internet Banking Environment (October 12, 2005) FFIEC, Supplemental to Authentication in an Internet Banking Environment (June 28, 2011)
- An RCC does not bear the signature of a person on whose account the check is drawn. Instead, the RCC bears the account holder's printed or typed name or a statement that the account holder authorized the check. The account holder can authorize the creation of an RCC by telephone by providing the appropriate information, including the MICR data. RCCs may go over a check clearing network or be processed as Automated Clearing House (ACH) debits and follow appropriate rules.
- See FFIEC IT Handbook: http://ithandbook.ffiec.gov/it-booklets/retail-payment-systems/payment-instruments,-clearing,-and-settlement/check-based-payments/remote-deposit-capture.aspx

Office of the Comptroller of the Currency (OCC) Bulletin 2008-12

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, *Cybersecurity Assessment Tool (CAT)* (June 2015): The CAT is a support tool issued by the FFIEC to assist financial organizations with managing cyber-risk. CAT is strongly encouraged by some US states, but in general it is based on existing guidance and thus does not constitute new regulation.

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)

For ACH transactions, see applicable regulations in the ACH Payment Lifecycle and Security Profile. See 12 CFR § 1005.3(c)(1) (under Regulation E, the term "electronic fund transfer" does not include "a/any transfer of funds originated by check, draft, or similar paper instrument").

Office of Foreign Assets Control (OFAC)/Sanction Screening

OTHER REFERENCES

ANSI ASC X9 Technical Report (TR) 8 – Check Security Guidelines

- Provides information for people involved in paper check or electronic check processing to become more familiar with industry practices and processes that identify and deter fraudulent use of paper checks, check images and electronically transmitted check data.
- Discusses tools that detect and prevent fraud, covering topics from high-tech software to low-tech physical control of the source documents.

ANSI X9.100 Series Check Image Exchange Basics (Formerly Check 21)

- X9.100-181 TIFF Image Format for Image Exchange
- X9.100-187 Electronic Exchange of Check and Image Data

NIST Cybersecurity Framework (CSF)

Electronic Clearing House Organization (ECCHO) rules

CHALLENGES AND IMPROVEMENT OPPORTUNITIES

Unclear if regulatory framework with FFIEC is sufficient to address RCC and RDC.

New security standards are needed to address potential increase in check fraud from fraudsters opening checking accounts to perpetuate overall ID fraud and develop ways to create counterfeit checks; or fraud associated with mobile RDC.

Customer's full routing transit and account numbers plus their personal information (name, address, and often a phone number and/or driver's license number) is all printed on each check.

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