SECURE PAYMENTS TASK FORCE

PAYMENT LIFECYCLE AND SECURITY PROFILE: Wire

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 Wire Payment Lifecycle and Security Profile maps out the lifecycle of a wire payment to establish a common understanding of the payment journey and serve 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).

WIRE

Definition: A wire payment (or funds transfer as specified in UCC 4A) is the transfer of funds from the payer's account at one financial institution to the payee's account at another financial institution.

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

				WIRE Note: payment flow may be bidirectional to include reverse wire transactions
			GENERIC FUNCTIONAL STEP	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	The originator's financial institution validates the originator's identity at the time of onboarding an account.
			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	Originator provides the information identifying the beneficiary and the beneficiary's financial institution. The originator's financial institution is obligated to adhere to compliance requirements (e.g., AML/BSA) prior to the wire being released.
TRANSACTION	Payer Authentication	PAYMENTS/TRANSFERS FLOW IN BOTH DIRECTIONS[1]	**Payer Authentication** Verification of payer when originating payments	Determined by the originator's financial institution and may be in-person, phone, internet banking or email to confirm it's an authorized individual. Call-back procedure using phone number on record and/or authentication code may be used.
	Initiation		**Access Mode / Network** Environment in which the payment origination is requested	Financial institution may take a request in-person, over the phone, via internet banking, etc. May include recurring wire agreements.
			Device/Method Used to Initiate Payment Type of interaction or device used to enter payment account information	In-person, phone, fax, email or internet-accessible device (desktop, laptop, mobile)
			Funding Account for Payment Entry and/or identification of the funding account (with format checks)	Cash, debit to an account, or any other means acceptable by the participating financial institution.
			Payment Initiation Mechanism Payment network, system and/or third-party accessed	Connection to a proprietary network, SWIFT, correspondent bank, Fedwire Funds Service, CHIPS, or funds transfer processors.
	Payer Authorization		**Payment Network Traversed** "Rails" used to route authorization requests to the holder of the funding account	
			Transaction Authorization Determination of whether to approve or decline a transaction including authorization time-frame, obligations, and any recourse decisions	Every receiving financial institution in the wire payment flow is responsible for authenticating and authorizing its originator. Originator's financial institution verifies cash or balance is sufficient for transmission. Once transmitted, the originator's financial institution has little to no recourse and the beneficiary's financial institution may give immediate cash credit for funds received.
	Format Exchange		**Format Exchange** Payment instructions, rules, and formatting	Proprietary formats for wire are used but mapping mechanisms are well-established to help facilitate straight-through processing.
	Receipt		**Acknowledgement/ Guarantee** Notification and confirmation of payment completion including terms for use	Receiving financial institution does not necessarily provide acknowledgement of receipt to originating financial institution.
	Payee Authentication		**Payee Authentication** Mode of access to funds (or accounts)	Every receiving FI in the wire payment flow is responsible for authenticating and authorizing its originator. Beneficiary is verified by the beneficiary's financial institution, either through on-site verification or through an established account at the beneficiary's financial institution.
	Clearing and Settlement		**Settlement / Exchange of Funds** Actual movement of funds to settle funding arrangements and applicable fees	Each payment obligation that arises between financial institutions in the funds transfer chain settles according to the laws and funds transfer rules that govern the transfer. While settlement is generally final at the time it occurs, if the overall funds transfer is not completed, a financial institution that has settled a payment obligation is entitled to get its money back. Settlement occurs between the originator's financial institution and the beneficiary's financial institution in accordance with established agreements.
RECONCILIATION			**Reconciliation / Exception Handling** Process and responsibilities associated with reconciling and handling any exceptions or problems with a payment	A funds transfer is completed when the beneficiary's bank accepts. Acceptance by the beneficiary's bank cannot occur as a matter of law if no person has rights as a beneficiary (i.e., neither name nor account number identify a person entitled to payment). In such a case all prior payment obligations are excused and each party in the funds transfer is entitled to a refund of any amount paid. The beneficiary's bank may not know that the instructions refer to a nonexistent or unidentifiable beneficiary until after it has received the payment order. Similar outcome for a closed account.
			User Protection / Recourse Applicable rules, regulations, and legal means of recourse	UCC 4A contains rules that allocate loss for errors and fraud

[1] Generally wire payments flow in one direction.

OVERVIEW OF SECURITY METHODS AND ASSOCIATED RISKS

		SECURITY METHODS	RISKS
ENROLLMENT	PAYER ID / ENROLLMENT	Financial institution verifies the individual during enrollment before opening an account. Know Your Customer (KYC), Customer Identification Program (CIP) background checks, etc.; ID verification of a "carbon-based lifeform" Employee training	Inconsistent controls for user-identification vetting, monitoring and verification when initiating wire transfers. Lack of Know your Customer (KYC) identification programs for correspondent banks 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		UCC 4A Security Provisions Financial institution authentication of customer Authentication methods include: out-of-band, two-factor Participants in the payment transaction 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. Employee training Consumer and corporate customer education Payment initiation mechanism: mutual authentication between the originating financial institution and the receiving financial institution Established wire limits, (including additional security checks based on dollar amount) Dual approval of transactions Client training and education As payments and technology continue to change, risk-based authentication is a way to continually evaluate and apply optimal security methods.	Authentication method misuse and the assumption that proper enroll-ment and authentication methods are in place Account takeover Social Engineering which could include business email compromise, masquerading fraud, imposter fraud, etc. Machine Takeover (beneficiary, financial institutions, network/operator, originator) Email and fax may be used by FI customers to communicate with the FI. ABA routing gap Incorrect information or the lack of pre-processing Lack of verification for recurring wire agreements Lack of customer-to-customer acknowledgement (end-to-end) Inadequately-controlled enrollment often poses additional risk at the time of transaction.
RECONCILIATION	RECONCILIATION / EXCEPTION HANDLING	Participants in the payment transaction 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.	
	USER PROTECTION / RECOURSE		Finality of payment if fraud occurs

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 | Demand Deposit Account Number (DDA) | Login Credentials | Personal Identification Number (PIN) | Biometrics | Email Address	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): Originator Account Number Originator Financial Institution ABA Originator Name Originator Address Originator Phone Beneficiary Account Number Beneficiary Financial Institution ABA Beneficiary Name Beneficiary Address Beneficiary Phone Personal Identification Number (PIN) Login Credentials Biometrics Email Address Sensitive Addenda Data (must be stored): *Data that may accompany or describe a financial transaction that is not required to process the transaction (e.g., airline or train ticket numbers, hotel confirmations, invoice numbers, insurance policy numbers)* Account numbers Invoice numbers Address information Dollar amount Government tax information	Compromised wire data (ABA and account number) can be used by a criminal to create counterfeit checks, fraudulent ACH payments and wire payments. Additional compromised data could be used for fraudulent account set-up and account takeover (account, invoice and address data). Lack of access controls, data integrity checks, etc. can be problematic and could result in fraudulent wire activities.
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

Uniform Commercial Code Article 4A (UCC 4A): Funds Transfers (as adopted by the states)

Regulation J, Collection of Checks and Other Items by Federal Reserve Banks and Funds Transfers through Fedwire® 12 CFR § 210.25 *et seq.*

Financial Crimes Enforcement Network (FinCEN) BSA/AML compliance Bank Secrecy Act, 31 U.S.C. § 5311, *et. seq.;* 31 CFR § 1010.100, *et. seq.* (implementing regulations); 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, Wholesale Payment Systems (July 2004)
- 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)

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)

Office of Foreign Assets Control (OFAC)/Sanction Screening

OTHER REFERENCES

SWIFT/ISO 20022: Financial Services – Universal financial industry message scheme

- Interbank communications system that provides standardized method to share financial information between financial institutions globally.

SWIFT Customer Security Program (CSP)

ANSI X9.69-2012 Framework for Key Management Extensions

ANSI X9.73 Cryptographic Message Syntax – ANS.1 and XML

NIST Cybersecurity Framework (CSF)

NIST Special Publication 800-53

CHIPS Rules and Administrative Procedures

- International funds transfers, operated by The Clearing House

Source: https://www.theclearinghouse.org/-/media/files/payco%20files/chips%20rules%20and%20administrative%20procedures%202016.pdf?la=en, pp. 7-10

Federal Reserve Operating Circulars 5 – Electronic Access; and 6 – Funds Transfers Through the Fedwire® Funds Service

Fedwire® Application Interface Manual (FAIM)

Principles for Financial Market Infrastructures (PFMI)

CPMI-IOSCO guidance on cyber resilience for financial market infrastructures

CHALLENGES AND IMPROVEMENT OPPORTUNITIES

Enrollment: Need enrollment standards to identify/authenticate people authorized to initiate transfers.

Authorized access requires dynamic controls with expanded notifications. Terminals need to be protected from allowing unauthorized people from making transfers. Standards needed for token (hardware or software) authentication.

Management and exchange of encryption keys and having right keys to communicate.

Need to encrypt end-to-end, not just payment data, not just transmission. Breaches occur by getting at unencrypted data. Quantum computing could make breaking current/common encryption trivial, but new approaches (including non-key based) could resist quantum decryption.

Data integrity checks sometimes spot problem transactions, but need to gate permitted transaction completions.

Many wire transactions are transmitted over encrypted networks, but that doesn't mean the actual payment and associated data are themselves within the transaction are encrypted. No existing standards for data encryption.

Inconsistent/lack of controls over user ID vetting, monitoring, verification etc. for initiating wire transfers.

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