SECURE PAYMENTS TASK FORCE

PAYMENT LIFECYCLE AND SECURITY PROFILE: Automated Clearing House (ACH)

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 ACH Lifecycle and Security Profile maps out the lifecycle of an ACH 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).

AUTOMATED CLEARING HOUSE (ACH)

Definition: An ACH payment (credit or debit) may include direct deposit payroll, Social Security payments, tax refunds, person-to-person (P2P) payments and the direct payment of business-to-business and consumer bills. Within the ACH system, the originator is the entity that originates transactions, and the receiver is the entity that receives the credit or debit payment (i.e. the payment is credited to or debited from their transaction account). The transactions pass through sending and receiving financial institutions that are authorized to use the ACH system.

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	Originating depository financial institution (ODFI) onboards originator utilizing Know Your Customer (KYC), underwriting, and assigning exposure limits. Originator required to execute origination agreement with the ODFI.	RDFI onboards receiver (payer) utilizing Know Your Customer (KYC), credit underwriting, and assigning exposure limits.
			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	Receiving depository financial institution (RDFI) validates receiver's identity as part of onboarding the receiver's account.	ODFI validates originator (payee) identity as part of onboarding the originator's account.
TRANSACTION	Payer Authentication	PAYMENTS/TRANSFERS FLOW IN BOTH DIRECTIONS	**Payer Authentication** Verification of payer when originating payments	ODFI authenticates customer (originator) utilizing a variety of methods within regulatory guidelines.	RDFI authenticates customer (receiver) utilizing a variety of methods within regulatory guidelines.
	Initiation		**Access Mode / Network** Environment in which the payment origination is requested	Originator provides instructions through various means to the ODFI. ODFI may utilize ACH operator or transmit directly to the RDFI.	Originator provides instructions through various means to the ODFI. ODFI may utilize ACH operator or transmit directly to the RDFI.
			Device/Method Used to Initiate Payment Type of interaction or device used to enter payment account information	Originator provides instructions through various means to the ODFI. ODFI utilizes communications methods as agreed upon with ACH operator or RDFI.	Originator provides instructions through various means to the ODFI. ODFI utilizes communication methods as agreed upon with ACH operator or RDFI.
			Funding Account for Payment Entry and/or identification of the funding account (with format checks)	Verification of account information can occur between ODFI and RDFI prior to initiation (e.g. traditional ACH where a pre-note is sent prior to the actual transaction) based on underwriting and established exposure limits. (See Payee ID/Enrollment)	Verification of account information can occur between ODFI and RDFI prior to initiation (e.g. traditional ACH where a pre-note is sent prior to the actual transaction) based on underwriting and established exposure limits.
			Payment Initiation Mechanism Payment network, system and/or third-party accessed	ACH network via ACH operators (Federal Reserve or Electronic Payments Network (EPN))	ACH network via ACH operators (Federal Reserve or Electronic Payments Network (EPN))
	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	Originator must obtain authorization per NACHA operating rules. Verification of receiver's account information can occur between ODFI and RDFI prior to initiation. RDFI can return for a variety of reasons to include account closed or other operational reasons as outlined in the NACHA rules.	Originator must obtain authorization per NACHA operating rules (i.e. in writing and signed or similarly authenticated). Authorization occurs between the originator and receiver prior to initiation. RDFI can return for a variety of reasons to include account closed or other operational reasons as outlined in the NACHA rules.
	Format Exchange		**Format Exchange** Payment instructions, rules, and formatting	NACHA rules and formats apply	NACHA rules and formats apply
	Receipt		**Acknowledgement/ Guarantee** Notification and confirmation of payment completion including terms for use		
	Payee Authentication		**Payee Authentication** Mode of access to funds (or accounts)	See Enrollment	See Enrollment
	Clearing and Settlement		**Settlement / Exchange of Funds** Actual movement of funds to settle funding arrangements and applicable fees	ACH clearing effects interbank settlement on Federal Reserve accounts or directly between financial institutions in accordance with established agreements.	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	RDFI may return ACH entry for a variety of reasons including account closed, account frozen, or invalid account.	RDFI may return ACH entry for a variety of reasons including account closed, account frozen, or invalid account. Additionally, for consumer payments, the RDFI has an extended right of return for unauthorized payments.
			User Protection / Recourse Applicable rules, regulations, and legal means of recourse	UCC 4A applies to corporate credit transfers. Regulation E consumer protections apply to consumer credit.	Regulation E consumer protections apply to consumer debit.

OVERVIEW OF SECURITY METHODS AND ASSOCIATED RISKS

		SECURITY METHODS	RISKS
ENROLLMENT	PAYER ID / ENROLLMENT	ODFI 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'. ODFI employee training Comply with the requirements of regulator(s) in developing a risk based compliance program.	Financial institution legacy accounts may lack Know Your Knowledge (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	Per the National ACH Association (NACHA) Operating Rules, establish commercially reasonable methods of authentication to verify the receiver.	Fraudulent use of account. 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		ODFI authenticating the originator – Federal Financial Institutions Examination Council (FFIEC) Guidance "Authentication in an Internet Banking Environment" applies. Authentication techniques include: shared secrets, tokens, Smart Card, password-generating tokens, biometrics out-of-band authentication, and one-time passwords. Section 1.6 Security Requirements applies; for internet-initiated debits (WEB), Subsection 2.5.17.4 applies. Additional ODFI Warranties for Debit WEB Entries, including use of fraudulent transaction detection system and commercially reasonable methods to authenticate the identity of the receiver Section 1.7 Secure Transmission of ACH Information via Unsecured Electronic Network applies 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 Device log-on (if used) Encryption Debit Block and ACH Positive Pay for Corporate Customers ODFIs have Know Your Customer (KYC) responsibilities for third-party payments they originate. 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, which could include business email compromise, masquerading fraud, imposter fraud, etc. Machine takeover (payee, financial institutions, network/operator, payer) Destination account compromise (e.g. payment redirect due to third-party compromise) Billers typically work through their financial institutions for origination; independent origination is suspect in account takeover era. Unauthorized authentication; no end-to-end encryption to protect the access keys in all the pieces of the ACH network. Third-party sender risks when the ODFI does not have a direct business relationship with clients of a third-party sender. The speed of payment processing and reconcilement may impact the ability to identify fraud in time to recover funds. Inadequately-controlled enrollment often poses additional risk at the time of transaction.
RECONCILIATION	RECONCILIATION / EXCEPTION HANDLING		Auto-debits, where billers control financial institution account access, present additional data to be protected (at rest and in transit).
	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	<u>Sensitive Data used to enroll or open an account:</u> Name | Date of Birth | Address | Social Security Number | Demand Deposit Account Number (DDA) | Savings Account Number (SAV) | Loan Account 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		<u>Account Holder Data (must be protected wherever it is processed, stored or transmitted):</u> Company ID (often times a Tax ID originator) Company Name (originator) Beneficiary Account Number Beneficiary RFI ABA Beneficiary Name <u>Specific to ACH File:</u> XML Extended Data Initiator Total Dollar Amount ***Consider anything that could be used to pass an authentication method*** <u>Sensitive Addenda Data (must be stored):</u> *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 Government tax information	Compromised ACH data can be used by a criminal to create a fraudulent credit/debit ACH file. This requires a customer to be onboarded as an ACH origination customer. Criminals can print fraudulent or counterfeit checks using the ABA and account number obtained through compromised ACH data. Additional compromised data, including Health Insurance Portability and Accountability Act (HIPAA), account, invoice and address data could be used for fraudulent account setup and account takeover.
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
Regulation E: Electronic Fund Transfer Act (EFTA) (Consumer ACH), 15 U.S.C. § 1693 *et seq.* / Reg E: 12 CFR § 1005.2 *et seq.*
Uniform Commercial Code Article 4A: Funds Transfers (as adopted by the states) (Non-Consumer ACH)
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 C.F.R. § 248.201 (SEC)
Office of the Comptroller of the Currency (OCC), 2006-39 and 2008-12
OCC, Third-Party Relationships, OCC Bulletin 2013-29 (Oct. 30, 2013): Risk management guidance directed at outsourcing and third-party relationship management, a key focus of the guidance is on requirements to adopt processes to manage third-parties in manner commensurate with risks over the full lifecycle of those relationships.
OCC, Supplemental Examination Procedures for Risk Management of Third-Party Relationships, OCC Bulletin 2017-7 (Jan. 24, 2017)
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)

Federal Reserve Operating Circular 4 – Automated Clearing House Items

Federal Reserve Operating Circular 5 – Electronic Access

Office of Foreign Assets Control (OFAC)/Sanction Screening

OTHER REFERENCES

ANSI X9.119-2 Tokenization (NACHA Payment Alliance is analyzing tokenization for ACH payments – OF and RAFI options, complex)

ANSI X9.122 Secure Consumer Authentication for Internet Debit Transactions (draft currently out for comment):

- The internet provides a ubiquitous, but insecure, channel that is susceptible to eavesdropping, phishing, man-in-the-middle, counterfeit websites and system intrusions including malware, spyware, screen scraping, key stroke loggers, mouse monitors, and man-in-the-browser attacks. Consequently, secure authentication methods for internet payment transactions are p varamount. This standard addresses common and discrete requirements for over-the-internet authentication methods which remain compatible with traditional payment authentication techniques.

ISO 12812/X US version (mobile financial services)

Online initiation for generic browser-based authentication (in progress)

ACH transactions can also be initiated from a mobile phone, so standards for mobile payments may apply.

NIST Cybersecurity Framework (CSF)

NIST Special Publication 800-53

National ACH Association (NACHA) Operating Rules/Guidelines govern ACH standards

- ODFIs and RDFIs cannot use ACH Network without being members and following rules for formats, information passed, authentication, etc. governed by NACHA. There are only two ACH Operators in the United States, the Federal Reserve and the Electronic Payments Network (EPN), through which all transactions flow.
- NACHA operating rules require users to register/authenticate by providing username, password, financial institution details (e.g. checking account number), routing transit number (RTN). Validation of financial institution RTN number is also required.
- TEL and WEB (Internet via PC or mobile device) transactions (i.e. similar to CAP): Originator must use commercially reasonable methods to verify identity of customer before processing T/C. These could include collecting/verifying driver's license or social security number, using third-party ID services, asking customers to confirm test deposit amounts (See NACHA WEB Proof of Authorization Industry Practices). Originator must also use commercially reasonable methods to identify fraudulent transactions to prevent them from entering the ACH Network for processing.
- NACHA rules require ACH participants, including merchants, to protect financial/other sensitive ACH data.
- New rule 2017: OFIs must register/authenticate third-party originators and notify NACHA
- Section 1.2.4 (OR1) Risk Assessments
- Subsection 1.4.4 (OR3) Electronic Signatures
- Section 1.6 (OR 3) Security Requirements
- Section 1.7 (OR3) Secure Transmission of ACH Information via Unsecured Electronic Networks
- Section 2.2.1 ODFI Verification of Originator or Third-Party Sender Identity
- Section 2.2.3 ODFI Risk Management (requiring ODFI to perform due diligence sufficient to form a belief that the originator or TPS has capacity to perform its obligations under the NACHA Operating Rules; requires risk assessments; exposure limits to be set and monitored; returns to be monitored, etc.)
- Section 2.3 (OR6-OR9) Authorization and Notice of Entries
- Section 2.3.4 (OR9) Restrictions on Data Passing
- Section 2.4 General Warranties and Liabilities of ODFIs (warranties of authorization of account holder, timeliness, entry carries required information, etc.)
- Section 2.5 Provisions for Specific Types of Entries (provisions specific to each different SEC Code)
- Section 2.17.1 ODFI Reporting: Direct Access Registration
- Section 2.17.2 ODFI Reporting: ODFI Return Rate Reporting
- Section 2.17.3 ODFI Reporting: Third-Party Sender Registration (effective September 29, 2017)
- Section 4.1.4 (OR54) ACH Operator Must Conduct Risk Management OG22 – Risk Assessments
- OG22 – Electronic Signatures and Records
- OG24-26 – ACH Data Security Requirements
- OG26 – Commercially Reasonable Standard
- OG27 – ODFI ACH Data Security
- OG33 – Additional warranties for WEB
- OG35 – ODFI Data Security Requirements
- OG36 – Data Passing
- OG46 – ODFI Data Security
- OG63-64 – Originator Data Security

CHALLENGES AND IMPROVEMENT OPPORTUNITIES

ACH rules require transmission of customer financial institution information to be encrypted using "commercially reasonable" encryption technology if transmitting over an unsecured network.

Move to same-day settlement just beginning, with evaluation of impacts to follow (including risks).

If ACH moves to tokenization, an applicable protocol, specification or standard needs to be identified. There should be consideration given on the need to be interoperable with card-based tokens.

Is "commercially reasonable" well-defined? Is a real standard (e.g. with minimally acceptable security) needed instead?

ACH transactions can also be initiated from a mobile phone, so standards for mobile payments may apply.

Regulatory requirements and ACH compliance rules may be viewed as redundant by financial institutions.

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