Automated Clearing House (ACH) Payment Use Case (DRAFT)

The ACH Payment Use Case maps out the lifecycle of a ACH Payment to establish a common understanding of the payment journey and serve as an educational reference guide to payment/security practitioners. Payment Use Case information includes 1) Payment Flow Overview 2) Payment Type Operation 3) Overview of Security Methods and Associated Risks 4) Inventory of Sensitive Data and Associated Risk 5) Overview of Standards

**ACH**

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 has authorized an originator to initiate a debit or credit entry to a transaction account. The transactions pass through sending and receiving banks that are authorized to use the ACH system.

### 1) Payment Flow Overview

<table>
<thead>
<tr>
<th>Enrollments</th>
<th>Payer Authentication</th>
<th>Access Mode / Network</th>
<th>Device Used to Initiate Payment</th>
<th>Funding Account for Payment</th>
<th>Payment Identification Mechanism</th>
<th>Payment Network Traversed</th>
<th>Transaction Authorization</th>
<th>Format Exchange</th>
<th>Receipt</th>
<th>Payer Authentication</th>
<th>Clearing and Settlement</th>
<th>Reconciliation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payer ID/ Enrollment</td>
<td>Payee ID/ Enrollment</td>
<td>Payee Authentication</td>
<td>Access Mode / Network</td>
<td>Device Used to Initiate Payment</td>
<td>Funding Network for Payment</td>
<td>Payment Identification Mechanism</td>
<td>Payment Network Traversed</td>
<td>Transaction Authorization</td>
<td>Format Exchange</td>
<td>Receipt</td>
<td>Payer Authentication</td>
<td>Clearing and Settlement</td>
</tr>
<tr>
<td>Definition</td>
<td>Description</td>
<td>ID proofing, management of users</td>
<td>(Enrollment, De-enrollment &amp; Changes)</td>
<td>and authority based on role</td>
<td>ID proofing and vetting of participant</td>
<td>(participant lifecycle)</td>
<td>Verification of payer when originating (or receiving) payments</td>
<td>The environment in which payment origination is requested</td>
<td>Type of interaction or device used to enter payment account information</td>
<td>Entry and/or identification of funding account (with format checks)</td>
<td>Network, system and/or 3rd party accessed</td>
<td>‘Rails’ used to route authorization requests to holder of funding account</td>
</tr>
</tbody>
</table>

### 2) Payment Type Operation

**Credit**

Originator validates Receivers identity and obtain assent to the transaction

Originating Depository Financial Institution (ODFI) authenticates customer utilizing a variety of methods within regulatory guidelines

Originating Depository Financial Institution (ODFI) utilizes proprietary transmission protocols to transmit entry to ACH operator

Originating Depository Financial Institution (ODFI) utilizes communications methods as agreed upon with ACH operator

Originating Depository Financial Institution (ODFI) utilizes good funds from the Originator (See Payee ID/Enrollment)

ACH Network via ACH Operators (Federal Reserve or Electronic Payments Network [EPNI])

National ACH Association (NACHA) rules and formats apply

**Debit**

Authorization occurs between the Originator and Receiver prior to initiation

‘IF’ can return for a variety of reasons to include account closed or payment not accepted after transaction has been received by Receiving Depository Financial Institution (RDFI)

N/A

See Enrollment

ACH Operators, effective interbank settlement on the Federal Reserve Accounts

Receiving Depository Financial Institution (RDFI) may return payment for a variety of reasons to include account closed, account frozen, or invalid account

UCC 4a applies to Corporate Credit Transfers

© 2017 Federal Reserve Banks. Materials are not to be used without consent.
The ACH Payment Use Case maps out the lifecycle of a ACH Payment to establish a common understanding of the payment journey and serve as an educational reference guide to payment/security practitioners.

Payment Use Case information includes:
1) Payment Flow Overview
2) Payment Type Operation
3) Overview of Security Methods and Associated Risks
4) Inventory of Sensitive Data and Associated Risk
5) Overview of Standards

© 2017 Federal Reserve Banks. Materials are not to be used without consent.

| Debit | Originator must obtain authorization in writing and signed or similarly authenticated. | Reg E applies to Consumer Debit and NACHA Rules apply to Corporate Debit | Originating Depository Financial Institution (ODFI) on boards | Originating Depository Financial Institution (ODFI) utilizes KyC, credit underwriting, and assigning exposure limits. | Originating Depository Financial Institution (ODFI) authenticates customer utilizing a variety of methods within regulatory guidelines | Originating Depository Financial Institution (ODFI) utilizes proprietary transmission protocols to transmit entry to ACH operator | Receiving Depository Financial Institution (RDFI) posts debit | ACH Network via ACH Operators (Federal Reserve or EPN) | N/A | Authorization occurs between the Originator and Receiver prior to initiation. A FI can return for a variety of reasons to include NSF, account closed or invalid account after transaction has been received by Receiving Depository Financial Institution (RDFI) | NACHA rules and formats apply | N/A | See Enrollment | ACH Operators effect interbank settlement on the Federal Reserve Accounts | Receiving Depository Financial Institution (RDFI) may return payment for a variety of reasons to include account closed, account frozen, or invalid account. Additionally for consumer payments the RDFI has an extended right of return for unauthorized payments | Reg E’s consumer protections apply to Consumer Debit and are affected via the NACHA operating rules |

### 3) Overview of Security Methods and Associated Risks

| Security Methods | ODFI to Originator | Know Your Customer ("KYC") and Customer Identification Program ("CIP") | ODFI Employee training | Comply with the requirements of regulator(s) in developing a risk based compliance program | Originator to Receiver | Per NACHA Operating Rules, establish commercially reasonable methods of authentication to verify the Receiver | Originating Depository Financial Institution (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, One-Time Passwords | Section 1.7 Secure Transmission of ACH Information via Unsecured Electronic Network applies | Anomaly and fraud detection | Employee training | Device long-on (if used) | Encryption |
The ACH Payment Use Case maps out the lifecycle of an ACH Payment to establish a common understanding of the payment journey and serve as an educational reference guide to payment/security practitioners. Payment Use Case information includes 1) Payment Flow Overview 2) Payment Type Operation 3) Overview of Security Methods and Associated Risks 4) Inventory of Sensitive Data and Associated Risk 5) Overview of Standards

### Risks
- ODFI to Originator
- ODFI responsible for Unauthorized Returns Limited
- Bad Actor List

### Fraudulent use of account
- Account Takeover
- Social engineering
- Machine Takeover (Payee, Financial Institutions, Network/Operator, Payer)
- Destination account compromise (e.g. payment redirect due to 3rd party compromise)
- Billers typically work through their banks for origination; independent origination is suspect in account takeover era
- ACH formats difficult to assimilate data for expedited enrollment, use, and information-sharing
- Unauthorized authentication; No end-to-end encryption to protect the access keys in all the pieces of the ACH system

### 4) Inventory of Sensitive Payment Data and Associated Risks

<table>
<thead>
<tr>
<th>Sensitive Payment Data (Data that need to be protected)</th>
<th>Sensitive Addenda Data (must be protected wherever it is processed, stored or transmitted)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account holder Data (must be protected whenever it is processed, stored or transmitted):</td>
<td><strong>Consider anything that could be used to pass an authentication method</strong> **</td>
</tr>
<tr>
<td>Company ID (Often times a Tax ID Originator)</td>
<td><strong>Consider anything that could be used to pass an authentication method</strong> **</td>
</tr>
<tr>
<td>Company Name (Originator)</td>
<td><strong>Consider anything that could be used to pass an authentication method</strong> **</td>
</tr>
<tr>
<td>Beneficiary Account Number</td>
<td><strong>Consider anything that could be used to pass an authentication method</strong> **</td>
</tr>
<tr>
<td>Beneficiary RFI ABA</td>
<td><strong>Consider anything that could be used to pass an authentication method</strong> **</td>
</tr>
<tr>
<td>Beneficiary Name</td>
<td><strong>Consider anything that could be used to pass an authentication method</strong> **</td>
</tr>
<tr>
<td>Specific to ACH File:</td>
<td><strong>Consider anything that could be used to pass an authentication method</strong> **</td>
</tr>
<tr>
<td>XML Extended Data</td>
<td><strong>Consider anything that could be used to pass an authentication method</strong> **</td>
</tr>
<tr>
<td>Initiator</td>
<td><strong>Consider anything that could be used to pass an authentication method</strong> **</td>
</tr>
<tr>
<td>Total Dollar Amount</td>
<td><strong>Consider anything that could be used to pass an authentication method</strong> **</td>
</tr>
<tr>
<td><strong>Sensitive Addenda Data (must be stored):</strong></td>
<td><strong>Consider anything that could be used to pass an authentication method</strong> **</td>
</tr>
<tr>
<td>Account numbers</td>
<td><strong>Consider anything that could be used to pass an authentication method</strong> **</td>
</tr>
<tr>
<td>Invoice Numbers</td>
<td><strong>Consider anything that could be used to pass an authentication method</strong> **</td>
</tr>
<tr>
<td>Address Information</td>
<td><strong>Consider anything that could be used to pass an authentication method</strong> **</td>
</tr>
<tr>
<td>Medical HIPAA Information</td>
<td><strong>Consider anything that could be used to pass an authentication method</strong> **</td>
</tr>
<tr>
<td>Government Tax Information</td>
<td><strong>Consider anything that could be used to pass an authentication method</strong> **</td>
</tr>
</tbody>
</table>

### Risks associated with the Sensitive Payment Data
- Compromised ACH Data can be used by a criminal to create a fake credit/debit ACH file, Print fraudulent / Counterfeit Checks (ABA and Account Number)
- Additional data compromised could be used for fraudulent account set-up and account takeover (HIPA Data, Account Data, Invoice Data, Address Data)

© 2017 Federal Reserve Banks. Materials are not to be used without consent.
### 5) Overview of Standards

<table>
<thead>
<tr>
<th>Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>X 119-2 Tokenization (NACHA Payment Alliance is analyzing tokenization for ACH payments — OF and RAFI options, complex)</td>
</tr>
<tr>
<td>X 122 Secure Consumer Authentication for Internet Debit Transactions (draft currently out for comment)</td>
</tr>
<tr>
<td>The Internet provides a ubiquitous but insecure channel that is susceptible to eavesdropping, phishing, man-in-the-middle, counterfeit web sites, 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 paramount. This standard addresses common and discrete requirements for over-the-Internet authentication methods which remain compatible with traditional payment authentication techniques.</td>
</tr>
<tr>
<td>ISO 12812/X US version (mobile financial services)</td>
</tr>
<tr>
<td>WK. online initiation for generic browser-based authentication (in progress)</td>
</tr>
<tr>
<td>ACH transactions can also be initiated from a mobile phone, so standards for mobile payments may apply</td>
</tr>
</tbody>
</table>

#### Other Potential Standards

- NIST Cybersecurity Framework
- NIST Special Publication 800-53

### Rules

- NACHA Operating Rules/Guidelines govern ACH standards
  - ODIs, OSIs, ROIs, and RIs 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 U.S. – Federal Reserve and EPN through which all transactions flow
  - NACHA rules require users to register/authenticate by providing username, password, bank details (e.g., checking account number), R/T number. Validation of bank R/T 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 SS#, using 3rd 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 ACH network for processing
  - NACHA rules require ACH participants, including merchants, to protect financial/other sensitive ACH data
  - New rule 2017: ODIs must register/authenticate 3rd party originators and notify NACHA
  - Section 1.2.4 (OR3) Risk Assessments
  - Section 1.6 (OR 3) Security Requirements
  - Section 1.7 (OR3) Secure Transmission of ACH Information via Unsecured Electronic Networks
  - Section 2.2.3 (OR6) ODPI Risk Management
  - Section 2.3.4 (OR9) Restrictions on Data Passing
  - Section 4.1.4 (OR54) ACH Operator Must Conduct Risk Management
  - Section 26 – ACH Data Security Requirements
  - OG27 – ODPI ACH Data Security
  - OG35 – ODPI Data Security Requirements
  - OG36 – Data Passing

### Regulations

- Regulation E: Electronic Funds Transfers
  - Financial Crimes Enforcement Network (FinCen) BSA/AML compliance
  - Customer Identification Program (CIP) 31 CFR
  - Non-Consumer ACH subject to Uniform Commercial Code Article 4A (UCC 4A): Funds Transfers
  - OCC CS Framework & Assessment tool
  - FRS 3rd Party Guidance (2013)
  - OFFICE – MFA, IT Handbook; 3rd Party Rules
  - Prudential regulators (e.g. OCC, FRS, FDIC, NCA) provide strong guidance that NACHA aligns with as appropriate

### Gaps/Issues

- ACH is not required to follow PCI-compliant standards, yet there are similarities with card payments
  - Move to same-day settlement (faster payments) just beginning, with evaluation of impacts to follow (including risks)
  - If the 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
  - ACH rules require transmission of customer bank information to be encrypted using 'commercially reasonable' encryption technology if transmitting over an unsecured network.
  - ACH is not subject to PCI/DSS encryption standards
  - 'Commercially reasonable' well-defined? Is it a standard (e.g., with minimally acceptable security) needed instead?
  - ACH process is a batch system, and shares many of the characteristics of wire transfer systems (e.g., endpoint security challenges)
  - ACH transactions can also be initiated from a mobile phone, so standards for mobile payments may apply
  - Regulatory overview and compliance requirements for ACH using FIs may be viewed as redundant