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 Overview
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.
PAGES OF A DOCUMENT

**PAYMENT FLOW OVERVIEW AND PAYMENT TYPE OPERATION**

### GENERIC FUNCTIONAL STEP

<table>
<thead>
<tr>
<th>PAPER CHECK</th>
<th>CHECK 21 / ELECTRONIC</th>
<th>ELECTRONIC FUNDS TRANSFER (EFT) CONVERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note: there is potential movement between paper and Check 21/electronic check</td>
<td>Note: EFT transactions are addressed in the ACH Payment Lifecycle and Payment Type Operation associated as ACH Debit transactions.</td>
<td>Financial Institution onboards account holder utilizing KYC and underwriting</td>
</tr>
</tbody>
</table>

### PAYEE ID / Enrollment

Enrollment of a payee includes identity (ID) verification, proofing, management of user (enrollment, de-enrollment, and changes) and determination of authority based on role.

### PAYEE ID / Enrollment

Enrollment of a payee includes identity (ID) verification, proofing, management of user (enrollment, de-enrollment, and changes) and determination of authority based on role.

### PAYMENT AUTHENTICATION

- **Authentication**
  - Paper of check may choose to request personal identification information from the payer.
  - Paper of check may choose to request personal identification information from the payer.
  - Payer may choose to request personal identification information from the payer.
  - Vendor creates Automated Clearing House (ACH) transaction and transmits data to vendor's financial institution.
  - Point of Sale (POS) or mail check to vendor for back-office conversion to ACH.

### PAYMENT FLOW IN BOTH DIRECTIONS

**Initiation**

- **Payment Authorization**
  - Payer's financial institutions onboard account holder utilizing KYC and underwriting

**Transaction**

- **Payment Flow Network System and Third-Party Access**
  - The payment of a check may be initiated by delivering the item with the intention of giving the recipient the right to endorse the item.
  - The payee or the payee's financial services provider truncates the paper check and deposits the item into their bank account at the Bank of First Deposit.
  - The payee or the payee's financial services provider truncates the paper check and deposits the item into their bank account at the Bank of First Deposit.

**Authorization**

- **Transaction Authorization**
  - 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.

**Clearing and Settlement**

- **Interbank settlement for checks may be structured by clearing house rules, Federal Reserve Operating Circular.**
  - Interbank settlement for checks may be structured by clearing house rules, Federal Reserve Operating Circular.**
  - Interbank settlement for checks may be structured by clearing house rules, Federal Reserve Operating Circular.**
  - Interbank settlement for checks may be structured by clearing house rules, Federal Reserve Operating Circular.**

**Reconciliation**

- **Reconciliation and Exception Handling**
  - 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 settlement may be varied or expanded by clearing house rules or agreements.
  - 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 settlement may be varied or expanded by clearing house rules or agreements.

**User Protection / Security**

- **Checks are governed by the Uniform Commercial Code, various federal statutes (Electronic Funds Availability Act, CFP Act), and Regulation CC.**
  - Checks are governed by the Uniform Commercial Code, various federal statutes (Electronic Funds Availability Act, CFP Act), and Regulation CC.**
  - Checks are governed by the Uniform Commercial Code, various federal statutes (Electronic Funds Availability Act, CFP Act), and Regulation CC.**
  - Checks are governed by the Uniform Commercial Code, various federal statutes (Electronic Funds Availability Act, CFP Act), and Regulation CC.**
# OVERVIEW OF SECURITY METHODS AND ASSOCIATED RISKS

<table>
<thead>
<tr>
<th>SECURITY METHODS</th>
<th>RISKS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Issuer verifies the individual during enrollment before issuing an account.</strong></td>
<td>Financial institution legacy accounts may lack KYC.</td>
</tr>
<tr>
<td>KYC, Customer Identification Program (CIP) background checks, etc.; ID verification of a ‘carbon-based lifeform’</td>
<td>Social Engineering, which could include business email compromise, masquerading fraud, imposter fraud, etc.</td>
</tr>
<tr>
<td>Employee training</td>
<td>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.</td>
</tr>
<tr>
<td><strong>KYC and CIP</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Fraud mitigation services where Data From Enforcement (DFE) can verify the status of the payor’s Demand Deposit Account (DDA)</strong></td>
<td>Limited opportunity to authenticate the payor at payment initiation</td>
</tr>
<tr>
<td>Employee training</td>
<td>ABA routing gap</td>
</tr>
<tr>
<td>Consumer and corporate customer education</td>
<td>Remote Deposit Capture (RDC) / multiple deposit risk at financial institutions</td>
</tr>
<tr>
<td>Magnetic Ink Character Recognition (MICR), microprint and other document-related security checks to affirm the integrity of the check</td>
<td>Social Engineering, which could include business email compromise, masquerading fraud, imposter fraud, etc.</td>
</tr>
<tr>
<td>As payments and technology continue to change, risk-based authentication is a way to continually evaluate and apply optimal security methods.</td>
<td>Inadequately-controlled enrollment often poses additional risk at the time of transaction.</td>
</tr>
<tr>
<td><strong>The speed of payment processing and reconcilement may impact the ability to identify fraud in time to recover funds.</strong></td>
<td></td>
</tr>
</tbody>
</table>
## INVENTORY OF SENSITIVE PAYMENT DATA AND ASSOCIATED RISKS

<table>
<thead>
<tr>
<th>SENSITIVE PAYMENT DATA (DATA THAT NEEDS TO BE PROTECTED)</th>
<th>RISKS ASSOCIATED WITH THE SENSITIVE PAYMENT DATA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensitive Data used to enroll or open an account: Name</td>
<td>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.</td>
</tr>
<tr>
<td>Date of Birth</td>
<td></td>
</tr>
<tr>
<td>Address</td>
<td></td>
</tr>
<tr>
<td>Social Security Number</td>
<td></td>
</tr>
</tbody>
</table>

### ENROLLMENT

#### PAYER ID / ENROLLMENT

- Payee ID / Enrollment

#### PAYEE ID / ENROLLMENT

- Payee’s Signature from Endorsement
- Payee’s Account Number
- Payee’s Financial Institution ABA

### 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).

### RECONCILIATION

### USER PROTECTION / RECOURSE

Sensitive payment data must be protected wherever it is processed, stored or transmitted.
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 Code of Federal Regulation (CFR) § 229.1 et seq.


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


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


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)

Remote Deposit (RDC) and Mobile Remote Deposit Capture (MRDC)

• 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.

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 Magnetic Ink Character Recognition (MICR) data. RCCs may go over a check clearing network or be processed as ACH debits and follow appropriate rules.


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)
CHECK PAYMENT LIFECYCLE AND SECURITY PROFILE | UPDATED FEBRUARY 21, 2018

**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.


**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)


**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**

**Americain National Standards Institute (ANSI) Accredited Standards Committee (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

**National Institute of Standards and Technology (NIST) Cybersecurity Framework**

**Electronic Clearing House Organization (ECCHO) rules**

---

**CHALLENGES AND IMPROVEMENT OPPORTUNITIES**

Unclear if regulatory framework with FFIEC is sufficient to address RCC and Remote Deposit Capture (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.