ACH Fraud Prevention in the Electronic World

Presented by:
Debbie Smart, CTP, NCP
Senior Business Consultant
Q2

What We Will Cover

• Introductions and Overview
• ACH Volume Growth
• Types of ACH Risk
• Managing Credit Risk
• Managing Operational Risk
• Managing Fraud Risk
• Conclusion and Q & A

ACH Volumes by Payment Type

<table>
<thead>
<tr>
<th>Payment Type</th>
<th>2016</th>
<th>2017</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARC</td>
<td>1,464,566,198</td>
<td>1,458,263,179</td>
<td>-0.48%</td>
</tr>
<tr>
<td>BIC</td>
<td>62,073,172</td>
<td>59,477,692</td>
<td>-4.11%</td>
</tr>
<tr>
<td>CCD Debits</td>
<td>7,500,784,647</td>
<td>7,986,081,972</td>
<td>6.59%</td>
</tr>
<tr>
<td>CCD Credits</td>
<td>1,370,146,263</td>
<td>1,370,103,217</td>
<td>0.03%</td>
</tr>
<tr>
<td>DE</td>
<td>19,170,007</td>
<td>19,205,006</td>
<td>0.02%</td>
</tr>
<tr>
<td>CTX</td>
<td>111,841,164</td>
<td>106,780,168</td>
<td>-4.5%</td>
</tr>
<tr>
<td>WF</td>
<td>20,501,026</td>
<td>20,501,026</td>
<td>0.00%</td>
</tr>
<tr>
<td>POS</td>
<td>205,403,038</td>
<td>205,201,038</td>
<td>-0.10%</td>
</tr>
<tr>
<td>PPP Debits</td>
<td>3,004,049,994</td>
<td>2,994,492,991</td>
<td>-0.31%</td>
</tr>
<tr>
<td>PPP Credits</td>
<td>6,026,062,204</td>
<td>5,979,345,297</td>
<td>-0.73%</td>
</tr>
<tr>
<td>RIC</td>
<td>2,981,450</td>
<td>2,982,276</td>
<td>0.03%</td>
</tr>
<tr>
<td>TEL</td>
<td>583,954,520</td>
<td>583,456,520</td>
<td>-0.86%</td>
</tr>
<tr>
<td>360 Debits</td>
<td>6,693,070,143</td>
<td>6,694,581,036</td>
<td>0.20%</td>
</tr>
<tr>
<td>360 Credits</td>
<td>10,004,345</td>
<td>10,004,345</td>
<td>0.00%</td>
</tr>
<tr>
<td>Other</td>
<td>256,714,211</td>
<td>243,310,748</td>
<td>-5.23%</td>
</tr>
<tr>
<td>Total Volume</td>
<td>20,328,747,117</td>
<td>19,772,103,537</td>
<td>2.76%</td>
</tr>
</tbody>
</table>
ACH Risk Overview

- Five Types of ACH Risk:
  - Systemic: The risk that the inability of an ACH network participant to settle its commitments results in the ability of other participants to settle their obligations (the participating ACH has no capacity to settle obligations).
  - Operational: The risk of loss related to errors or omissions which may result in delayed, duplicated, or erroneous erroneous payments. Operational risk may result from human or equipment breakdown, software, communication failure.
  - Fraud: The risk due a payment transaction is initiated or allowed in an attempt to mislead or manipulate funds. Fraud risk includes the introduction of false transactions or the alteration of existing transactions.
  - Reputational: The risk that arises from adverse publicity related to a negative financial assault, resulting in a loss of business. Sources of reputational risk include word of mouth, media coverage and lease propagation.
  - Credit: The risk that one party to an ACH transaction will be unable to provide the necessary funds for payment settlement.
Credit Risk

• Risk that a party to a transaction cannot provide the necessary funds in order for settlement to take place

ACH Credit Origination – 2 day example

<table>
<thead>
<tr>
<th>Monday</th>
<th>Tuesday</th>
<th>Wednesday</th>
</tr>
</thead>
<tbody>
<tr>
<td>• ACH credit file sent from Company to Bank</td>
<td>• ACH credits are delivered to RDP’s by the ACH Processor</td>
<td>• Bank’s account is charged by the ACH Operator</td>
</tr>
<tr>
<td>• Entries are effective on Day 3 (Wednesday)</td>
<td></td>
<td>• Company declares bankruptcy</td>
</tr>
<tr>
<td>• Bank processes file and delivers transactions to ACH Processor</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

ACH Debit Origination

<table>
<thead>
<tr>
<th>Monday</th>
<th>Tuesday</th>
<th>Wednesday</th>
</tr>
</thead>
<tbody>
<tr>
<td>• ACH debit file sent from Company to Bank</td>
<td>• ACH debits are delivered to RDP’s by the ACH Processor</td>
<td>• RDP’s return debits</td>
</tr>
<tr>
<td>• Entries are effective on Day 2 (Tuesday)</td>
<td>• Bank credits Company for amount of debit file</td>
<td>• Company declares bankruptcy</td>
</tr>
<tr>
<td>• Bank processes file and delivers items to ACH Processor</td>
<td>• RDP’s reject debits for NSF</td>
<td></td>
</tr>
</tbody>
</table>
ACH Debit Origination

Thursday

- Bank receives debit return for NSF / Uncollected funds

Day 40

- Consumer payment unauthorized
- ACO / ROK stop payment, improper source doc, no notice given, inaccurate amount, source doc presented

Managing ACH Credit Risk

ODFI’s should:

- Know your customer!
- Treat all ACH origination customers as unsecured borrowers;
- As such, subject them to credit review and approval process;
- Establish acceptable credit limit;
- Monitor creditworthiness of customers on an on-going basis

Pre-funding as an Alternative

- Originate customer "pays in advance";
- When ACH files are submitted for processing, the customer’s account is debited prior to the transactions being released into the network;
- Eliminates need for the ACH credit review process;
- Consider for customers who are new to the bank or don’t pass credit standards for traditional origination services
Additional Sound Practices

• Set limits reflective of the customer’s credit limit
  • Receive alerts when limits are met/exceeded
  • Review and decision exception items

• Set limits reflective of the customer’s usual activity
  • Receive alerts when anomalies occur
  • Review and decision exception items

• Limit SEC codes to what the customer will be originating and/or is allowed to originate

ACH Operational Risk

• The risk of loss related to errors or omissions which may result in delayed, duplicated or otherwise erroneous payments.
• Operational risk may result from human or equipment (hardware, software, telecommunications) failure.
ACH Operational Risk

Examples of Operational Risk

- Slip of a finger on a keyboard
- Failure of a piece of hardware or software
- Communications protocol problems
- Narrow decision windows
- Inadequate information
- Being short-staffed
- Breaches in internal controls
  ..... to name a few

Managing Operational Risk

Sound Practices for Mitigating and Managing Operational Risk

- Quickly identify and act upon anomalies at the customer level.
  * Customer-level control enables OFIs to monitor a specific batch within an ACH file without delaying the processing of the rest of the file.
- Have an efficient notification system in the event of credit or debit cap breaches, or other issues that may impact the decision whether to release or reject an ACH batch.
- In the event of a hardware, software or power failure, maintain access to ACH activity. Services that use Web-based technology afford access to authorized/certified personnel from virtually any computer terminal with an Internet connection.

ACH Fraud Risk
ACH Fraud Risk

- The risk that a payment transaction is initiated or altered in an attempt to misdirect or misappropriate funds. Fraud risk includes the introduction of false transactions or the alteration of otherwise valid transactions.

Examples of Fraud Risk

- Account Takeover:
  - A type of identity theft in which a criminal steals a business's (or individual's) valid online banking credentials and then uses those credentials to initiate funds transfers out of the account.

- Business Email Compromise and Vendor Impersonation Fraud (phishing):
  - One method of gaining valid online banking credentials.

Phishing Examples

- Various phishing attempts depicted with images and text.
Phishing Examples

- Impersonating Vendors

Managing Fraud Risk

- Sound Business Practices for Financial Institutions
- Sound Business Practices for Companies
- Sound Business Practices for Third-Party Service Providers

Sound Business Practices for Financial Institutions

- Agreements & Minimum Security Procedures
- Dual Control for Payment File Initiation
- Out-of-Band Authentication and Alerts
- Enhancement of Account Security Offerings
- Exploration of Low-Tech Security Options
- Education
- Special Considerations for RDFIs
• Agreements & Minimum Security Procedures should include:
  • Advise implementation of multi-factor and multi-channel
    authentication for business accounts that are permitted to initiate
    funds transfers. Multi-factor authentication includes at least two of the
    following:
    • something the person knows (user ID, PIN, password)
    • something the person has (password-generating token, USB token)
    • something the person owns (biometric, e.g., fingerprint scan)

• Out-of-Band Authentication and Alerts
  • Use out-of-band alerts to warn an Originator of unusual activity.
    Triggers may include:
    • New payees: Recipients who have never received a transfer from
      the Originator before.
    • IP address authentication: A file is initiated from an IP address not
      previously associated with the Originator.
    • New credential requests: Someone at the financial institution
      should be evaluating requests for new Originator credentials before
      issuing and permitting use of the new credentials.
    • Abnormal patterns: time of day, day of week, unusual amounts and
      transaction counts.

• Enhancement of Account Security Offerings
  • Encourage Origirators to use value-added services like positive pay,
    debit blocks, and tokens to enhance Originator’s account security.

• Exploration of Low-Tech Security Options
  • Origination calendar: Consider using origination calendars that will
    alert a financial institution to files that are out of the normal behavior
    (e.g., different time of day or different amount than is typical) for the
    client.
  • Prenotification: Consider using prenotification for credit origination
    when an Originator makes changes to their origination file (e.g.,
    adding new Receivers or account number changes).
**Sound Business Practices for Financial Institutions**

- Special Considerations for RDFIs:
  - Educate front-line staff about money mules and what to do if one is suspected or identified.
  - Look for anomalies in deposits.
  - Develop procedures for what to do if a money mule is suspected or identified.

**Sound Business Practices for Companies**

- Computer Security:
  - Layered System Security
  - Online Banking Safety
  - Education
  - Websites
  - User Accounts
  - Staying Informed

- Account Security:
  - Dual Control
  - Reconciliation
  - Account Services
  - Reporting of Suspicious Activity
  - Credentials

**Sound Business Practices for Third-Party Service Providers**

- Third-Party Senders Performing Services on Behalf of an Originator:
  - Educate Originators
  - Dual Control for Payment Initiation
  - Agreements and Minimum Security Procedures
  - Exposure Limits
  - Enhancement of Account Security Offerings

- Third-Party Service Providers Performing Services on Behalf of an ODFI or an RDFI:
  - Follow Sound Practices for Financial Institutions
Summary

- ACH risk must be understood and monitored
- Many tools/sound practices help mitigate more than one type of risk
- Education – both employees and customers – is critical
- With the right tools in place, you can feel confident you are providing the right services to your customers and properly managing your exposure
- Remember – There is risk inherent in all aspects of banking – lending, merchant services, deposit accounts – understanding, managing and mitigating risk – it's what we do!
- Great resources for more information:
  * nacla.org
  * fcaservices.org

The End 😊

Questions??

Debbie Smart, CTP, NCP
Phone: 702-540-3061
Email: Debbie.smart@q2ebanking.com

www.q2ebanking.com