Mitigating the Risk of Payment Fraud

Stephen W. Markwell  
Disbursements Product Executive  
J.P. Morgan

Pamela R. Malmos  
Director, Treasury Operations  
ConAgra Foods, Inc.

Laura Howley, CTP  
Senior Manager, Global Treasury Operations  
The Boeing Company
Who’s at Risk and What’s at Stake?

In 2009:

- Almost three-quarters of organizations were victims of payments fraud
- 81% of organizations with annual revenues over $1 billion were victims of payments fraud
- 63% of organizations with annual revenues under $1 billion were victims of payments fraud
- 30% of organizations report that incidents of fraud increased
- The median loss of organizations that sustained any financial losses resulting from payments fraud was $17,100.

Source: 2010 AFP Payments Fraud and Control Survey
No Payment Type Is Immune

- Nine out of 10 organizations that experienced attempted or actual payments fraud in 2009 were victims of check fraud.

- Though electronic fraud is a tougher challenge for criminals, ACH Debit fraud ranks second as a target.

- Consumer credit/debit card fraud is up from 18% in 2008 to 20% in 2009; commercial card fraud is up from 14% to 17% in the same period.

### Prevalence of Payments Fraud in 2009
(Percentage of Respondents)

<table>
<thead>
<tr>
<th></th>
<th>All Respondents</th>
<th>Revenues &gt; $1 billion</th>
<th>Revenues &lt; $1 billion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Checks</td>
<td>90%</td>
<td>93%</td>
<td>89%</td>
</tr>
<tr>
<td>ACH debits</td>
<td>25</td>
<td>23</td>
<td>25</td>
</tr>
<tr>
<td>Consumer credit/debit cards</td>
<td>20</td>
<td>18</td>
<td>22</td>
</tr>
<tr>
<td>Corporate/commercial purchasing cards</td>
<td>17</td>
<td>18</td>
<td>13</td>
</tr>
<tr>
<td>ACH credits</td>
<td>7</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>Wire transfers</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>

Source: 2010 AFP Payments Fraud and Control Survey
Internal Best Practices

- Segregate Duties
  - Checks – Originate payment, Submit Issuance, Decision Exceptions
  - Wires - Creating, Approving, Releasing Wires
- Dual Approval
  - Require dual approval at critical checkpoints such as approving wires or approving Positive Pay exception decisions
- Segregate Accounts
  - Account Type: Deposits or Disbursements
  - Payment Method: Check, ACH, Wire
  - Payment Type: Payroll, Claims
  - Payment Amount/Volume: High or low
- Monitor and reconcile accounts daily
- Centralized Fraud Protection Governance
- HR Policy – Forced vacations and job rotations

Segregating accounts for different payment vehicles is a best practice highlighted by 90% of respondents.

Separation of accounts allows for timely and focused review of payment activity.

2010 AFP Payments Fraud and Control Survey, sponsored by J.P. Morgan

Source: 2010 AFP Payments Fraud and Control Survey
Check Fraud: #1 and Growing

- Follow the money
  - Checks as a percent of total payments is decreasing at a rate of approximately 7%
  - However, the value of checks is increasing

- A Growing Trend?
  - 64% of organizations suffering financial losses report that checks resulted in the greatest loss.
  - Fully 89% of the victims of check fraud attempts report that check fraud attacks have increased

- Why Checks?
  - Easy-to-commit, quick-hit crime
  - Requires no special skills
  - Technology-assisted crime (scanners, printers, desktop publishing software)
Check Fraud: Fraud Protection Solutions & Internal Best Practices

Use of Check Fraud Protection Solutions

<table>
<thead>
<tr>
<th>Services/Methods Used</th>
<th>All Respondents</th>
<th>Revenues &gt;$1 billion</th>
<th>Revenues &lt;$1 billion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Positive Pay &amp; Reverse Positive Pay</td>
<td>83%</td>
<td>85%</td>
<td>81%</td>
</tr>
<tr>
<td>Payee Name Positive Pay</td>
<td>52</td>
<td>60</td>
<td>45</td>
</tr>
<tr>
<td>Post No Checks</td>
<td>37</td>
<td>46</td>
<td>26</td>
</tr>
</tbody>
</table>

Use of best practices to mitigate check fraud (Right)

Other best practices include:
- Outsourcing check print
- Electronic forms of financial documents
- Document destruction process
- Manage check stock orders & storage
- Segregation of duties and dual approval

Source: 2010 AFP Payments Fraud and Control Survey
ACH Fraud: As Use Broadens, ACH Fraud Schemes Grow

Popular ACH Fraud Schemes

- **Account Hijacking** Fraudsters use compromised customer credentials to hijack the origination system and use it in the legitimate account holder’s name.

- **Identity Fraud** Criminals create false identities, social engineer their way into obtaining ACH origination capabilities and then initiate fraudulent debits.

- **ACH Kiting** A version of check kiting with a cyber twist, ACH kiting involves a pair of accounts used for fraudulent purposes where an ACH debit is originated from one account and drawn on the other; the available balance is taken out before settlement.

- **Reverse Phishing** Instead of e-mails attempting to fraudulently obtain corporate banking information, perpetrators send e-mails to corporates that provide fraudulent banking information, redirecting ACH payments to an account they control.

- **Insider Origination Fraud** Insiders at a merchant or bank manipulate an ACH origination file to skim funds from a company.

- **Counterfeiting** ACH debits generated through the electronic conversion of a counterfeit check.

![ACH Fraud Attempts & Losses Pie Chart]

- 70% Reported Attempts - No Loss
- 27% Reported Attempts - Loss
- 3% No Attempts

AFP® Annual Conference
ACH: Fraud Protection Products & Best Practices

Use of ACH Fraud Protection Products

<table>
<thead>
<tr>
<th>Services/Methods Used</th>
<th>All Respondents</th>
<th>Revenues &gt;$1 billion</th>
<th>Revenues &lt;$1 billion</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACH debit blocks</td>
<td>77%</td>
<td>83%</td>
<td>69%</td>
</tr>
<tr>
<td>ACH debit filters</td>
<td>58</td>
<td>66</td>
<td>49</td>
</tr>
<tr>
<td>ACH positive pay</td>
<td>21</td>
<td>18</td>
<td>20</td>
</tr>
<tr>
<td>UPIC for ACH credits</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
</tbody>
</table>

Internal Best Practices

- Know your customers and vendors
- Segregate Accounts and Duties
- Protect Sensitive Information: Mask and Encrypt
- Monitor and reconcile your accounts daily
- Ensure tokens are collected and credentials are changed after employees leave

Source: 2010 AFP Payments Fraud and Control Survey
Phishing Casts a Wider Net

- Phishing = email fraud that dupes targets into providing sensitive information or unknowingly downloading malicious software from a phony, look-alike web site

- More than three quarters (76 percent) of consumers said they were aware of “phishing,” double the 38 percent that responded similarly in 2007

- Instead of decreasing effectiveness, increased awareness has simply forced innovation — and increased effectiveness

Phishing: Attack Methods and Protection from your Bank

- Popular Phishing Schemes
  - “Vishing” - uses the telephone system to solicit sensitive information
  - “Smishing” - SMS (Short Message Service) phishing
  - “Spear Phishing” - targets employees or high-profile individuals within an organization

- Protection from your Bank
  - Encryption
  - Multi-Factor Authentication: Soft or Hard tokens
  - Dual authority or Step Up Authentication for Transactions
  - Comprehensive fraud monitoring and detection systems
  - Customer education programs

Commercial Cards: Coming of Age

- In 2009, more than three quarters (77 percent) of businesses used some sort of corporate or commercial cards
  - 72 %, purchasing cards
  - 45%, travel and entertainment cards
  - 27%, multiple-use cards
  - 23%, ghost or virtual cards
  - 23%, fleet cards
  - 7%, other types

Types of Cards Used in Making B2B Payments
(Percent of Organizations that Suffered B2B Card Fraud)

Source: 2010 AFP Payments Fraud and Control Survey
Corporate Card: Common Threats & Best Practices

Typically, B2B payments fraud involving such cards is committed by an outside party; however, employees were responsible for over a quarter of 2009 fraud cases (27 percent).

<table>
<thead>
<tr>
<th>Primary Party Responsible for Fraud from Making B2B Card Payments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown external party</td>
</tr>
<tr>
<td>External</td>
</tr>
<tr>
<td>Third-party or outsourcer (e.g., vendor, professional services provider, business trading partner)</td>
</tr>
<tr>
<td>Internal</td>
</tr>
<tr>
<td>Employee</td>
</tr>
</tbody>
</table>

A J.P. Morgan Treasury Services survey of purchasing card clients identified best practices in managing a solid, secure card program, responders shared these key internal measures as most important in detecting and preventing card fraud:

- Senior management sponsorship
- Segregate duties and accounts
- Promote consistency within Policies and Procedures
- Effectively train managers and employees
- Define controls upfront
- Conduct peer reviews to validate business rules
- Partner with issuer that provides web based payment tools with rich spend analysis

Source: J.P. Morgan Treasury Services. Auditing and Compliance Strategies for a Solid Purchasing Card Program
Case Study: Needs Assessment

Property & Casualty Insurance Provider – Midwest Division

- P&C provider with large check claim payment volume
- Performs all transactions through single operate account
- 12 Fraud Attempts in the last 30 days

<table>
<thead>
<tr>
<th>Account</th>
<th>Account Type</th>
<th>Monthly Activity</th>
<th>Recommended Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check:</td>
<td>--Claims Payments</td>
<td>87,263 Checks</td>
<td>Close Compromised Account</td>
</tr>
<tr>
<td></td>
<td>--Misc Payables</td>
<td>69 ACH Debits</td>
<td>Segregate activity into multiple accounts</td>
</tr>
<tr>
<td>ACH:</td>
<td>--Payroll through ADP</td>
<td></td>
<td>Apply Fraud Protection Solutions</td>
</tr>
<tr>
<td>XXXXXX7214</td>
<td>--Vendor Payments</td>
<td>7 ACH Credits</td>
<td></td>
</tr>
<tr>
<td></td>
<td>--Refunds</td>
<td>370,440 Deposits</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Deposit</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>--Client Receipts</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Case Study: Segregate Accounts

Segregate Accounts By:
- Purpose
- Payment Vehicle
- Volume
- Amount

<table>
<thead>
<tr>
<th>Account</th>
<th>Account Type</th>
<th>Monthly Activity</th>
<th>Recommended Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>XXXXXXX8765</td>
<td>Check: Client Claims</td>
<td>87,526 Checks</td>
<td></td>
</tr>
<tr>
<td>XXXXXXX8768</td>
<td>ACH: AP, Payroll through ADP</td>
<td>4 ACH Debits</td>
<td></td>
</tr>
<tr>
<td>XXXXXXX8770</td>
<td>Deposit: AR, Client Receipts</td>
<td>370,440 Deposits</td>
<td></td>
</tr>
<tr>
<td>XXXXXXX8772</td>
<td>ACH: Vendor Payments &amp; Refunds</td>
<td>65 ACH Debits 7 ACH Credits</td>
<td></td>
</tr>
<tr>
<td>XXXXXXX8774</td>
<td>Check: Misc Payables</td>
<td>263 Checks</td>
<td></td>
</tr>
</tbody>
</table>

*Fictitious client created for purposes of this case study
Case Study: Fraud Protection Solutions

- Protect accounts with Fraud Protection Solutions that match your payment behavior

<table>
<thead>
<tr>
<th>Account</th>
<th>Account Type</th>
<th>Monthly Activity</th>
<th>Recommended Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>XXXXXXX8765</td>
<td>Check: Client Claims</td>
<td>87,526 Checks</td>
<td>Positive Pay with Payee Name verification</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ACH Debit Block-All</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Post No Checks</td>
</tr>
<tr>
<td>XXXXXXX8768</td>
<td>ACH: AP, Payroll through ADP</td>
<td>4 ACH Debits</td>
<td>ACH Debit Block- Exclude all but ADP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Post No Checks</td>
</tr>
<tr>
<td>XXXXXXX8770</td>
<td>Deposit: AR, Client Receipts</td>
<td>370,440 Deposits</td>
<td>ACH Debit Block-All</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Post No Checks</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ACH Transaction Review</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Post No Checks</td>
</tr>
<tr>
<td>XXXXXXX8772</td>
<td>ACH: Vendor Payments &amp; Refunds</td>
<td>65 ACH Debits 7</td>
<td>ACH Transaction Review</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ACH Credits</td>
<td>Post No Checks</td>
</tr>
<tr>
<td>XXXXXXX8774</td>
<td>Check: Misc Payables</td>
<td>263 Checks</td>
<td>Positive Pay with Payee Name verification</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>No Check Cashing. ACH Debit Block-All</td>
</tr>
</tbody>
</table>

*Fictitious client created for purposes of this case study
Payments Fraud Panel Discussion

Today’s Panel will discuss their Payments Fraud Experience
  - Making payment fraud protection a priority
  - Institutionalizing fraud protection measures across businesses
  - Monitoring and mitigating the latest in fraud trends
  - Calibrating internal best practices
  - Leveraging appropriate fraud protection solutions

Stephen W. Markwell  
Disbursements Product Executive  
J.P. Morgan

Pamela R. Malmos  
Director, Treasury Operations  
ConAgra Foods, Inc.

Laura Howley, CTP  
Senior Manager, Global Treasury Operations  
The Boeing Company