How to Protect Against Fraud in an Evolving Payments Environment

Sarah Schaus
AVP/Assistant Treasurer
Allianz

Timothy Dwyer
AVP/Assistant Treasurer
Nationwide

Ravin Yadav
Vice President
J.P. Morgan
Are Fraudsters Keeping You Awake at Night?
Your Panelists

Sarah Schaus
AVP/Assistant Treasurer
Allianz

- Responsible for cash management, cash operations, Accounts Payable, unclaimed property, banking relationships, suspense and cash reconciliations

Timothy Dwyer
AVP/Assistant Treasurer
Nationwide

- In charge of Credit and Bank relationships
- Certified Treasury Professional

Ravin Yadav
Vice President
J.P. Morgan

- Responsible for developing comprehensive payables solutions for corporate clients
- Frequent speaker on payment trends, innovations, and fraud protection
Presentation Summary

- Discuss latest statistics and trends in payments fraud as highlighted in the 2013 AFP fraud survey.

- Various payment types and fraud protection techniques will be examined ranging from traditional (check), electronic (ACH/card), to emerging (mobile/email).

- Panel will describe real world implications of these trends and experiences in combating them.
### AFP Fraud Survey: Who’s at Risk? What’s at Stake?

#### 2013 AFP Payments Fraud and Control Survey

#### Percentage of Organizations Reporting

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>61%</td>
<td>Experienced attempted or actual payments fraud in 2012</td>
</tr>
<tr>
<td></td>
<td>Median loss $20,300</td>
</tr>
<tr>
<td>67%</td>
<td>Revenues over $1 billion</td>
</tr>
<tr>
<td>50%</td>
<td>Revenues under $1 billion</td>
</tr>
<tr>
<td>27%</td>
<td>Incidents of fraud have increased</td>
</tr>
</tbody>
</table>

Source: 2013 AFP Payments Fraud and Control Survey
AFP Fraud Survey: Who’s at Risk? What’s at Stake?

Percent of Organizations Subject to Attempted or Actual Payments Fraud

Fraud attacks – or notice of fraud attacks – are decreasing…

…yet successful fraud attacks have resulted in greater loss amounts

Median loss: $17,100 → $18,400 → $19,200 → $20,300

Source: 2013 AFP Payments Fraud and Control Survey
Shift to Electronic Payments Creates Opportunities to Reduce Fraud Risk…

Optimizing payables could offer substantial benefits including freeing capital, reducing processing costs, and mitigating operational risk.

Corporate mandates and inefficiencies in the payables process…

<table>
<thead>
<tr>
<th>Issue</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reduce overall payment costs</td>
<td>69%</td>
</tr>
<tr>
<td>Stakeholder demand for improved operational efficiency</td>
<td>64%</td>
</tr>
<tr>
<td>High invoice payment error rate</td>
<td>18%</td>
</tr>
<tr>
<td>Lack of predictability of cash flows</td>
<td>13%</td>
</tr>
<tr>
<td>Growing risk of payment fraud</td>
<td>13%</td>
</tr>
</tbody>
</table>

Source – Aberdeen May 2010 Payment Survey
Shift to Electronic Payments Creates Opportunities to Reduce Fraud Risk….

Optimizing payables could offer substantial benefits including freeing capital, reducing processing costs, and mitigating operational risk.

…are driving the adoption of electronic disbursement methods

Payment volume shifts in the past 12 months

<table>
<thead>
<tr>
<th></th>
<th>Increased</th>
<th>Decreased</th>
<th>Stayed same</th>
</tr>
</thead>
<tbody>
<tr>
<td>Checks</td>
<td>11%</td>
<td>57%</td>
<td>32%</td>
</tr>
<tr>
<td>Wire</td>
<td>43%</td>
<td>11%</td>
<td>46%</td>
</tr>
<tr>
<td>Cards</td>
<td>45%</td>
<td>9%</td>
<td>46%</td>
</tr>
<tr>
<td>ACH</td>
<td>59%</td>
<td>5%</td>
<td>36%</td>
</tr>
</tbody>
</table>

Source – Aberdeen May 2010 Payment Survey

AFP® Annual Conference
However, Fraudsters are Increasingly Targeting Electronic Payments

Of the 61% of organizations that reported fraud...

Prevalence of Fraud by Payment Type (% of Respondents)

Source: 2013 AFP Payments Fraud and Control Survey
However, Fraudsters are Increasingly Targeting Electronic Payments

Of the 61% of organizations that reported fraud...

Prevalence of Fraud by Payment Type (% of Respondents)

- Fraud by check was reported most often – 87%
- Corporate card has overtaken ACH debits as the second most-targeted payment type

<table>
<thead>
<tr>
<th>Payment Type</th>
<th>% of Respondents</th>
<th>Financial Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHECK</td>
<td>16%</td>
<td>26%</td>
</tr>
<tr>
<td>Card</td>
<td>26%</td>
<td>12%</td>
</tr>
<tr>
<td>ACH</td>
<td>12%</td>
<td></td>
</tr>
</tbody>
</table>

Source: 2013 AFP Payments Fraud and Control Survey
Taking the Fight to Fraud
### Mitigating the Risk of Payments Fraud

**Fight fraud with a comprehensive approach**

The right plan includes effective controls within your operations and a strong partnership with your bank.

<table>
<thead>
<tr>
<th>Your Operations</th>
<th>Your Bank</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check fraud</td>
<td>Check printing and mailing services</td>
</tr>
<tr>
<td>Check stock quality and security</td>
<td>Secure online banking systems</td>
</tr>
<tr>
<td>Document storage and destruction process</td>
<td>Fraud protection services / transaction monitoring / pattern detection</td>
</tr>
<tr>
<td>Transition to electronic documents and processes</td>
<td></td>
</tr>
</tbody>
</table>
Mitigating the Risk of Payments Fraud

Fight fraud with a comprehensive approach

The right plan includes effective controls within your operations and a strong partnership with your bank

Your Operations

- Segregation of duties / dual approval
- Separate accounts for different activities
- Daily account reconciliation and monitoring
- HR policies around employee on-boarding and departures

Your Bank

Internal controls

AFP® Annual Conference
Mitigating the Risk of Payments Fraud

Fight fraud with a comprehensive approach

The right plan includes effective controls within your operations and a strong partnership with your bank

- Know your customers and vendors
- Protect sensitive information
- Awareness and vigilance around social engineering threats
- Incident response and research processes

Your Operations

Your Bank

- Data encryption
- Dual control options
- Multi-factor authentication – soft or hard tokens
- Customer education programs

Corporate security

AFP® Annual Conference
Nationwide Central Fraud Committee Transforms Response to Fraud Events and Prevention

• The Fraud Committee was chaired by Treasury and included representation from Claims, Internal security, Legal and Controllership

• The goal of the committee is to identify and reduce fraud

• The committee decided on a phase approached
  – Phase 1 Consolidate instances of Fraud under a centralized location
  – Phase 2 Develop reporting and metrics on fraud
  – Phase 3 Manage to reduce instances of fraud
Pillars of Allianz Fraud Protection Structure

Key Components

- Ethical Culture
  - Establish appropriate tone from the top
  - Implement policies, procedures, handbooks
  - Establish reporting mechanisms

- Training & Communication
  - Establish training programs tailored to key audiences
  - Maintain awareness
  - Measure effectiveness

- Risk Assessments
  - Maintain ongoing risk assessment process
  - Report on findings
  - Remediate gaps
  - Maintain an inventory of anti-fraud controls

- Fraud Deterrence & Detection
  - Establish preventative & detective controls
  - Drive enhancements to control environment
  - Develop and utilize an effective data mining strategy
Pillars of Allianz Fraud Protection Structure

Key Components

Response & Investigations
- Uphold and enact response plans and policies
- Maintain an internal Special Investigation Unit (SIU)
- Leverage external investigations support

Oversight, Monitoring & Testing
- Have an effective oversight model
- Enhance systematic oversight
- Implement control and risk scenario testing
Check Fraud: #1

- Despite decline in U.S. check payments, check fraud results in the greatest financial fraud losses

<table>
<thead>
<tr>
<th>Payment Trends</th>
<th>2006</th>
<th>2009</th>
</tr>
</thead>
<tbody>
<tr>
<td>Checks paid volume</td>
<td>30.5 billion</td>
<td>24.5 billion</td>
</tr>
<tr>
<td>Avg $ per check</td>
<td>$1,366</td>
<td>$1,292</td>
</tr>
</tbody>
</table>

-7.1% CAGR*

* Compound Annual Growth Rate
Source: 2013 AFP Payments Fraud and Control Survey
Check Fraud: #1

- Despite decline in U.S. check payments, check fraud results in the greatest financial fraud losses

### Payment Method Responsible for the Greatest $ Loss

- Checks: 69%
- ACH debits: 9%
- Wire transfers: 5%
- ACH credits: 7%
- Corporate/commercial cards: 10%

Source: 2013 AFP Payments Fraud and Control Survey
Check Fraud: #1

- Despite decline in U.S. check payments, check fraud results in the greatest financial fraud losses

Why Checks?

- Attraction of paper-based crimes
- Better quality and availability of technology

- Easier to commit than electronic fraud methods
- Increase in organized, professional fraud ring activity
- Access to scanners, printers, desktop publishing software, and other tools used to print and alter checks
- Weaknesses in the modern image exchange environment

Source: 2013 AFP Payments Fraud and Control Survey
Check Fraud: #1

- **Despite decline in U.S. check payments, check fraud results in the greatest financial fraud losses**

### Most Widely Used (Reported) Check Fraud Techniques

<table>
<thead>
<tr>
<th>Method</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-payroll counterfeit checks with your MICR</td>
<td>63%</td>
</tr>
<tr>
<td>Payee name alteration on checks issued</td>
<td>49%</td>
</tr>
<tr>
<td>Dollar amount alteration on checks issued</td>
<td>28%</td>
</tr>
<tr>
<td>Counterfeit check with your name but fake account info</td>
<td>29%</td>
</tr>
<tr>
<td>Loss / theft / counterfeit of payroll checks</td>
<td>14%</td>
</tr>
</tbody>
</table>

Source: 2013 AFP Payments Fraud and Control Survey
The Risk of Checks

How Checks Can be Used Against You

- Your account information becomes public and can be used fraudulently
- Physical theft of check stock
- Copies, forgeries, and alterations of checks
  - Counterfeit checks using your valid MICR line data
  - Payee name and/or dollar amount alteration on checks issued
  - Counterfeit checks with your name using fake account information
The Risk of Checks

Reconsider Your Paper-based Operations

- Payees can report checks as “lost”, then attempt to negotiate both the original and the reissued item
- Negotiating the same item via multiple methods (paper and images)

- Avoid checks…
  - Transition to electronic transactions
  - Outsource check printing or take extra precautions
  - Keep your check stock physically secure
  - Manage your document destruction process
  - Use check stock security features
Effective Use of Fraud Prevention Tools Reduces Risk

**Basic Fraud Prevention**

<table>
<thead>
<tr>
<th>Positive Pay</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enables payors to authorize certain items to be paid from their accounts as a way of monitoring and controlling check debits</td>
</tr>
<tr>
<td>Bank uncovers any payments that do not match this pre-authorized list and flag them as exceptions</td>
</tr>
<tr>
<td>Exceptions are available to view each morning via ACCESS</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACH Debit Block</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allows payors to specify which companies are authorized to post ACH debits from certain accounts, blocking all others</td>
</tr>
<tr>
<td>Payor can also set dollar limits on ACH debits</td>
</tr>
<tr>
<td>Client has the option to block all ACH debits from posting to an account</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Post No Checks Block</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fully blocks checks from a deposit account or from an account used for electronic debits only</td>
</tr>
</tbody>
</table>
Effective Use of Fraud Prevention Tools Reduces Risk

Value-Add Fraud Prevention

Automated Issue File Transmittal
- Payor receives automated acknowledgement of account reconciliation and positive pay issue input files via a secure web page or via fax
- Ensures transmissions are received by the bank and are accurately recorded

Stale-Dating
- Allows the payor to define the number of days after the issue date that a check may be honored
- Checks that come in after this date can either be automatically returned or referred to the client for a pay or return decision
- Only available with Full Reconciliation
Effective Use of Fraud Prevention Tools Reduces Risk

Value-Add Fraud Prevention

**Reverse Positive Pay**

- Allows for the client to self-identify any potential check frauds
- Bank sends the client a file with presented checks for the client to determine any discrepancies
- Images of checks are available online for investigation
- The client sends any return items back to Bank

**Payee Verification**

- Enhances Positive Pay by matching payee names on issued checks with those provided by the client in their check issue file
- Bank reports any exceptions as part of the positive pay review and the client decides whether to pay or return the items
Effective Use of Fraud Prevention Tools
Reduces Risk

Value-Add Fraud Prevention

**ACH Transaction Review**
- Allows client to review and confirm ACH debit and credit transactions online (through Payables Web Service) and return unauthorized transactions
- Available on a case-by-case basis

**Maximum Dollar Limit**
- Client is notified when checks exceed a pre-set maximum dollar limit
- Checks that exceed this limit can either automatically be returned unpaid or can be referred to the client to decide whether to pay or return
Electronic Fraud and Social Engineering

Social Engineering Identity Fraud

- Phishing – attempting to acquire sensitive information, typically via email, phony websites, and malware

- Posing as a known individual (or individual with a “trusted” affiliation)
  - A “technical support associate” calls a high risk online banking user to offer unsolicited assistance on “technical problems” – hoping the target will reveal private account information
  - A “vendor” provides a corporate client with instructions to change expected ACH or wire payments to a different account controlled by the fraudster

- Creating or using a false identity, then maneuvering their way into obtaining access to payment systems
Electronic Fraud and Social Engineering

Unauthorized Access to Payment Systems

- Launching attacks against corporate networks
- Using compromised credentials to access payment systems or email accounts to submit instructions in the legitimate account holder’s name
Importance of Periodic Review of all Payables Processes

Allianz Check Print Example

- Put out an RFP this year for check stock, key objectives
  - Consolidate providers
  - Lower Cost

- Result of RFP process was a successfully consolidation to one provider (from 3) and 40% lower costs
Importance of Periodic Review of all Payables Processes

Allianz Used the RFP Opportunity to Make Related Value-added Improvements

- Utilized the check testing process to also simplify signers by using a non-individual name as the signer

- Selected check stock with added fraud protection features such as:
  - Security watermark
  - Micro printing
  - Invisible florescent fibers
  - Thermo-chromic ink

- Lesson learned – without examining check print processes Allianz would not be aware of existing check stock security deficiencies
Increased Usage Results in Increased Corporate and Commercial Card Fraud

Payment Method Responsible for the Greatest Loss:
- Checks: 69%
- Corporate/commercial cards: 10%
- ACH debits: 9%
- ACH credits: 7%
- Wire transfers: 5%
Increased Usage Results in Increased Corporate and Commercial Card Fraud

Card Types Experiencing Fraud

- Purchasing Cards: 84%
- T&E Cards: 58%
- Virtual Cards: 48%
- Fleet Cards: 30%
- "One Card": 21%
- Travel Cards: 5%
- Other: 1%
Increased Usage Results in Increased Corporate and Commercial Card Fraud

<table>
<thead>
<tr>
<th>Fraud vs. Misuse</th>
</tr>
</thead>
<tbody>
<tr>
<td>Card Fraud</td>
</tr>
<tr>
<td>Unauthorized transaction(s) made with a lost, stolen, or counterfeit card or number - 74%</td>
</tr>
<tr>
<td>Card Misuse</td>
</tr>
<tr>
<td>Unauthorized activity by an employee (not following internal procedures) -26%</td>
</tr>
</tbody>
</table>

Types of Breaches – External Factors

- Counterfeit card made with stolen stripe data
- Merchant compromise – hacking or physical theft
- Skimming (data capture) devices placed on card readers
Increased Usage Results in Increased Corporate and Commercial Card Fraud

Organizations Suffering the Loss

- Card Issuing Bank: 49%
- The Organization: 26%
- Merchant: 23%
- Card Processor: 11%
- No Organization Suffered Loss: 11%
Corporate/Commercial Cards

- 87% of organizations reported using corporate or commercial cards for B2B payments

**Card Fraud**

- Unauthorized transaction(s) made with a lost, stolen, or counterfeit card or number

**Card Misuse**

- Unauthorized activity by an employee (not following internal procedures)

---

**Defenses Against Fraud & Misuse**

- Card issuer’s fraud detection and spending analysis tools
- Card controls offered by the card issuer – restrictions on merchant category codes and spending limits
- Manager and employee training

---

Source: 2013 AFP Payments Fraud and Control Survey
Corporate/Commercial Cards

- Reports of employee incidents have decreased from 38% of organizations in 2011 to 26% in 2012

<table>
<thead>
<tr>
<th>Primary Party Responsible</th>
<th>Central Party Responsible</th>
</tr>
</thead>
<tbody>
<tr>
<td>External</td>
<td>Internal</td>
</tr>
<tr>
<td>Unknown external party</td>
<td>Employee</td>
</tr>
<tr>
<td>Third party or outsource</td>
<td></td>
</tr>
<tr>
<td>(e.g. vendor, professional services provider, business trading partner)</td>
<td>26%</td>
</tr>
</tbody>
</table>

- Unknown external party 74%
- Third party or outsource 6%

Types of Breaches – External Factors

- Counterfeit card made with stolen magnetic stripe data
- Merchant compromise – hacking, data or physical theft
- Skimming (data capture) devices placed on card readers

Source: 2013 AFP Payments Fraud and Control Survey
## Mitigating Card Misuse by Clearly Outlining Policies

**Allianz T&E example:**

<table>
<thead>
<tr>
<th>Overview</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Allianz comprehensively updated its internal travel and expense policies this year</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Key features</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Mandatory training class</td>
<td></td>
</tr>
<tr>
<td>Clarified acceptable and unacceptable spend at a more granular level</td>
<td></td>
</tr>
<tr>
<td>Requiring corporate credit card for anyone who spends more than $500 annually regardless of whether they travel</td>
<td></td>
</tr>
<tr>
<td>Accounts Payable runs reports of out of pocket spend, and out of policy charges and escalated weekly to senior leadership for review and action</td>
<td></td>
</tr>
<tr>
<td>Human Resources sends daily list of termed employees so corporate credit cards can be cancelled immediately.</td>
<td></td>
</tr>
<tr>
<td>Use MCC codes to manage expense types</td>
<td></td>
</tr>
</tbody>
</table>
Mitigating Card Misuse by Clearly Outlining Policies

<table>
<thead>
<tr>
<th>Key Benefits of revised policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increased employee awareness of rules</td>
</tr>
<tr>
<td>Better control and easier monitoring of card usage</td>
</tr>
<tr>
<td>Timely cancellation of cards</td>
</tr>
<tr>
<td>Streamlined reporting</td>
</tr>
</tbody>
</table>
Combating ACH Fraud

Types of ACH Fraud Breaches

- Trusted business associates or vendors use ACH debit/credit agreements for unauthorized purposes
- Insiders at a merchant or bank manipulate an ACH origination file to skim funds from a company
- ACH kiting – an ACH debit is originated from one account and drawn on another account; the available balance is taken out before settlement

ACH Payment Trends

<table>
<thead>
<tr>
<th></th>
<th>2006</th>
<th>2009</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACH volume</td>
<td>14.6 billion</td>
<td>19.1 billion</td>
</tr>
<tr>
<td>Average $ per ACH</td>
<td>$2,123</td>
<td>$1,948</td>
</tr>
</tbody>
</table>

*Compound Annual Growth Rate
Combating ACH Fraud

**Best practices to protect against ACH fraud**

- Segregate accounts by usage and choose appropriate fraud protection service
  - **Accounts not making payments**
    - Block all debits
  - **Accounts making some payments**
    - Set up “authorized” list and dollar limits through your bank
    - Review transactions with ACH Positive Pay / ACH Transaction Review

- **All accounts**
  - Know your customers and vendors
  - Protect sensitive information
    - Mask and encrypt electronic communications and data transfers
    - Use Universal Payment Identification Code (UPIC) for ACH credits
  - Monitor internal access to payment systems – ensure tokens are collected and credentials changed after employees leave
Payables Innovations: Using Data Analysis to improve protection

Innovative technology based analytics tools, provide companies with:

- Comprehensive examination of existing usage of accounts and services.
- Systematic identification of areas that can be targeted for improvement due to fraud gaps and/or reliance on paper intensive services.
- Highlights of actions that can be taken immediately to convert to electronic options.
- Quantification of benefits

Go Green Analysis Summary

58 accounts were analyzed for Go Green opportunities. Please contact us to discuss our recommended implementation plan.

- Already green
  - 20 accounts

- Turn off paper
  - 16 accounts
  - $2,580 savings

- Add electronic solution and turn off paper
  - 22 accounts
  - $16,504 savings

Total Annual Bank Fee Savings*

$19,184

*Bank fee savings are calculated using a three month trailing average. Savings relate to paper-based products and do not include additional fees related to adding electronic services.
Case Study: Needs Assessment

- Hypothetical Property & Casualty Insurance Provider
  - Large check volume of claims payments
  - All transactions performed through a single operating account
  - 12 fraud attempts in the last 30 days

<table>
<thead>
<tr>
<th>Account</th>
<th>Account Type</th>
<th>Monthly Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>XXXXXXX7412</td>
<td>• Check – client claims, misc payables</td>
<td>• 87,263 checks</td>
</tr>
<tr>
<td></td>
<td>• ACH – payroll through ADP, vendor payments, refunds</td>
<td>• 69 ACH debits</td>
</tr>
<tr>
<td></td>
<td>• Deposit – client receipts</td>
<td>• 7 ACH credits</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 370,440 deposits</td>
</tr>
</tbody>
</table>
Case Study: Recommendations

1. Close compromised account
2. Segregate activity into multiple accounts – by purpose, payment type, volume, amount
3. Apply fraud protection solutions
4. Establish processes and procedures to minimize possibility of recurrence

<table>
<thead>
<tr>
<th>Account</th>
<th>Account Type</th>
<th>Monthly Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>XXXXXXXX3451</td>
<td>Check – client claims</td>
<td>87,526 checks</td>
</tr>
<tr>
<td>XXXXXXXX3452</td>
<td>ACH – A/P, payroll through ADP</td>
<td>4 ACH debits</td>
</tr>
<tr>
<td>XXXXXXXX3453</td>
<td>Deposit – A/R, client receipts</td>
<td>370,440 deposits</td>
</tr>
<tr>
<td>XXXXXXXX3454</td>
<td>ACH – vendor payments, refunds</td>
<td>65 ACH debits</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7 ACH credits</td>
</tr>
<tr>
<td>XXXXXXXX3455</td>
<td>Check – misc payables</td>
<td>263 checks</td>
</tr>
</tbody>
</table>
Case Study: Fraud Protection Solutions

Which solutions match these payment behaviors?

<table>
<thead>
<tr>
<th>Account</th>
<th>Account Type</th>
<th>Fraud Protection Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>XXXXXX3451</td>
<td>Check – client claims</td>
<td></td>
</tr>
<tr>
<td>XXXXXX3452</td>
<td>ACH – A/P, payroll</td>
<td>through ADP</td>
</tr>
<tr>
<td>XXXXXX3453</td>
<td>Deposit – A/R, client</td>
<td>receipts</td>
</tr>
<tr>
<td>XXXXXX3454</td>
<td>ACH – vendor payments</td>
<td>refunds</td>
</tr>
<tr>
<td>XXXXXX3455</td>
<td>Check – misc payables</td>
<td></td>
</tr>
</tbody>
</table>
### Case Study: Fraud Protection Solutions

- Which solutions match these payment behaviors?

<table>
<thead>
<tr>
<th>Account</th>
<th>Account Type</th>
<th>Fraud Protection Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>XXXXXXX3451</td>
<td>Check – client claims</td>
<td>• Positive Pay &amp; Payee Name Positive Pay</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Block all ACH debits</td>
</tr>
<tr>
<td>XXXXXXX3452</td>
<td>ACH – A/P, payroll through ADP</td>
<td>• Block all ACH debits except ADP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Post No Check</td>
</tr>
<tr>
<td>XXXXXXX3453</td>
<td>Deposit – A/R, client receipts</td>
<td>• Block all ACH debits</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Post No Check</td>
</tr>
<tr>
<td>XXXXXXX3454</td>
<td>ACH – vendor payments, refunds</td>
<td>• ACH Positive Pay</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Post No Check</td>
</tr>
<tr>
<td>XXXXXXX3455</td>
<td>Check – misc payables</td>
<td>• Positive Pay &amp; Payee Name Positive Pay</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• No Check Cashing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Block all ACH debits</td>
</tr>
</tbody>
</table>
Key Take-Aways

- The protection of your accounts and financial information is a top priority

- The right plan includes effective controls within your operations and a strong partnership with your bank

Stay Informed on fraudster practices and crime innovations

Adapt & Implement internal controls and external security services
Your Thoughts?

Q & A

AFP® Annual Conference
Contact Information:

Sarah Schaus
Allianz
763.765.2809
sarah.schaus@allianzlife.com

Timothy Dwyer
Nationwide
614-249-7725
DwyerT@nationwide.com

Ravin Yadav
J.P. Morgan
212-552-3027
ravin.k.yadav@jpmchase.com