Payments Fraud: Risks and Controls

*Keeping Fraudsters Away from Your Agency’s Money*

Presented By:
Azba Habib
Associate Counsel, Federal Reserve Bank of Atlanta
May 9, 2012
The views presented are those of the individual presenter and do not reflect the views of the Federal Reserve Bank of Atlanta, the Retail Payments Office, the Board of Governors, or any person or entity.

The content of this presentation is intended to serve as general information and not as legal counsel or as expert advice about IT. If the issues in this presentation interest you, you should consult your own legal counsel and/or IT professional.
Presentation Outline

1. Role of the Federal Reserve System in Payments
2. Understanding Payments Fraud
3. Types of Fraud
4. Check Fraud and Controls
5. Electronic Payments Fraud and Controls
6. Card Fraud and Controls
7. Response Plan
8. Conclusion
Role of Federal Reserve in Payments

- **Regulator**
  - Promulgate rules around payments (e.g., check collection, electronic fund transfers, wires)

- **Provider**
  - Provide payments services to financial institutions and the federal government

- **Consumer Protector**
  - Review bank compliance with consumer protection regulations; investigate complaints from the public; direct community affairs program

- **Thought Leader**
  - Convene agencies and industry participants; identify, discuss and propose solutions to risk issues; house the Retail Payments Risk Forum
Role of Federal Reserve in Payments

- **NOT** a law enforcement agency
- **DO NOT** provider services to end users such as state and local agencies, businesses and consumers
What is Payments Fraud?

• Form of fraud that occurs when:
  • someone gains financial or material advantage
  • by using a payment instrument (think card or check) or information from a payment instrument (think routing and account number)
  • to complete a transaction
  • that is not authorized by the legitimate account holder
What are the Types of Payments Fraud?

<table>
<thead>
<tr>
<th>Prevalence of Payments Fraud by Method</th>
<th>Percent of Organizations Subject to Attempted or Actual Payments Fraud in 2011</th>
</tr>
</thead>
<tbody>
<tr>
<td>Checks</td>
<td>85%</td>
</tr>
<tr>
<td>ACH Debits</td>
<td>23%</td>
</tr>
<tr>
<td>Corporate/ commercial purchasing cards</td>
<td>20%</td>
</tr>
<tr>
<td>Consumer/ small business credit or debit cards</td>
<td>12%</td>
</tr>
<tr>
<td>ACH Credits</td>
<td>5%</td>
</tr>
<tr>
<td>Wire Transfers</td>
<td>5%</td>
</tr>
<tr>
<td>Payroll &amp; Other Benefit Cards</td>
<td>5%</td>
</tr>
</tbody>
</table>

Source: 2012 AFP Payments Fraud and Control Survey
What is Check Fraud?

- Forgery, alteration, counterfeiting or knowing issuance of a check on an account that has been closed or has insufficient funds to cover the check amount.
Types of Check Fraud

1. **Insider fraud**
   - Fraudster issues checks drawn on employer without proper authorization

2. **Theft and alteration**
   - Fraudster steals and alters checks to reflect a different payee or amount

3. **Improper endorsement and conversion**
   - Fraudster endorses the check and presents it for payment using false identification

4. **Counterfeiting checks**
   - Fraudster fabricates the check using desktop publishing software and draws on a non-existent account or uses an agency’s MICR line data to draw against the agency’s account
Insider Check Fraud

- Fraud Scenario
  - Employee works in the accounts payable department of her employer
  - As an account manager, employee has the authority to issue checks drawn on her employer’s account
  - Employee opens a bank account in the name of one of her employer’s vendors and issues checks from her employer’s account into the fraudulent account she controls
  - Employee further falsifies invoices to conceal her embezzlement

- How can your agency prevent this scenario?
Theft and Alteration

- **Fraud Scenario**
  - Thieves intercept valid checks issued by your agency to a vendor
  - The face value of the check is left in tact, but the recipient information is altered
  - Thief deposits the check in an account under his name
  - Withdraws the funds and closes the account

- How can your agency prevent this scenario?
Improper Endorsement and Conversion

• Fraud Scenario
  • State government agency issues payroll check
  • Payment is intercepted and check is stolen by fraudster
  • Fraudster improperly endorses the check
  • Presents the check for payment with false ID
  • Withdraws the funds immediately

• How can your agency prevent this scenario?
Counterfeit Checks

- **Fraud Scenario**
  - You make publicly available the routing and account number for your receipt account (e.g., state income tax payments, fines, etc.)
  - Fraudster gets hold of that information and creates counterfeit checks using desktop publishing software with your agency’s MICR line data
  - Fraudster presents the check which purports to pay him or his accomplices and draws on your agencies account
  - Fraudster withdraws the funds immediately and your account is debited

- How can your agency prevent this scenario?
Ways to Mitigate Check Fraud Risk

• Implement strong internal controls and procedures around key treasury functions
  • Move off of paper
  • Move the money to disbursement account “just in time”
  • Separate accounts (depository, disbursement, funding, investment)
  • Use dual controls and separation of duties
  • Secure blank check stock
  • Reconcile bank accounts daily and report suspicious activity
  • Immediately notify the bank of any change to your A/P process and personnel
  • Institute payment procedures during employee vacations and turnover
  • Educate and train employees on fraud prevention
  • Limit receipt instruments
  • Conduct frequent audits to verify controls applied
Ways to Mitigate Check Fraud Risk (Cont’d)

• Engage your banks and leverage the tools and processes available
  • Positive pay, positive pay with payee verification, or reverse positive pay
  • Posting blocks on depository accounts
  • Require signature verification
Electronic Payments Fraud

N.Y. Firm Faces Bankruptcy from $164,000 E-Banking Loss

European Cyber-Gangs Target Small U.S. Firms, Group Says

e-Banking Bandits Stole $465,000 From Calif. Escrow Firm

La. firm sues [bank] after losing thousands in online bank fraud

Cyber attackers empty business accounts in minutes

Zeus hackers could steal corporate secrets too

TEXAS FIRM BLAMES BANK FOR $50,000 CYBER HEIST

Computer Crooks Steal $100,000 from Ill. Town

FBI Investigating Theft of $500,000 from NY School District

Zeus Botnet Thriving Despite Arrests in the US, UK

Electronic Payments Fraud

- Any unauthorized fund transfer that occurs in a bank account
  - Consumer accounts are covered by Regulation E which caps consumer loss, in most instances, to $50; agency accounts do not have the same protection
Who are the Targets?

- Cybercriminals often target employees (e.g., senior executives, accounting personnel and HR personnel)
- Particularly susceptible are small to medium sized organizations that usually bank with community banks and credit unions (e.g., court systems, school districts, municipalities, and other public institutions)
  - Small organizations have the capability to initiate fund transfers via online banking
  - Many small organizations do not practice dual control, do not utilize value-added banking services, and do not monitor and reconcile their accounts on a frequent or daily basis
Electronic Payment Fraud Types

1. Insider fraud
2. Unauthorized debits
3. Unauthorized credits
   • Account Takeover
   • Mimicking Legitimate Credits
Insider Fraud

• Fraud Scenario
  • Agency issues “super credentials” to Senior Technology Officer
  • The Technology Officer with the super credentials initiates large dollar wires to accounts controlled by him or his accomplices
  • Immediately moves the money offshore

• How can your agency prevent this scenario?
Unauthorized Debits

- **Unprotected Government Account (True Story)**
  - Federal agency published its RTN and account number in the RTN directory
  - Maintained a large portion of its funds in that account
  - Did not have debit blockers or monitor account activity daily
  - Fraudsters found their way to the account
  - Used the RTN and account number to buy all sorts of cars
  - Car dealers debited the account not knowing it was a government account

- **Lessons learned**
  - Protect your account - use debit blockers and/or filters for both receipt and disbursement accounts
  - Minimize funds in your transaction account
  - Disclose only receipt account information
  - Have your bank suppress your ACH account number for outbound ACH
  - Provide your bank a list of employees who can originate
Unauthorized Credits ("Account Takeover")

**Fraud Scenario**
- You are the treasurer at a local municipality
- You receive a phishing email from IRS saying “Notice of Underreported Income”
- You click on the link and malware is installed on your computer
- Next time you log on, Zuesbot hijacks your session
- You are redirected to a spoof site
- Meanwhile, fraudster uses your legitimate session to initiate unauthorized credits out of your agency’s account
- Transfers the funds to “money mules” who subsequently transfer the money overseas

**How can your agency prevent this scenario?**
Unauthorized Credits (“Mimic Legitimate Credits”)

• Reverse Phishing
  • Instead of using e-mails to obtain banking credentials, fraudsters provide fraudulent banking information so as to re-direct ACH payments to an account they control

• Fraud Scenario (credits that look like vendor payments)
  • A company received e-mails from two vendors asking for changes to bank and account numbers used to receive ACH payments for invoices
  • The company believed the requests to be legitimate, as the e-mails looked like those from the vendors
  • The company originates ACH credits to the new bank account numbers
  • The ACH credits go to newly opened accounts, and the funds were withdrawn
  • Eventually, the company receives phone calls from the vendors about failure to pay
  • The company investigates and discovers that the original e-mails supplying new payment instructions were fraudulent
Ways to Mitigate Electronic Payments Fraud

- **Strong Access Controls**
  - Layered security (e.g., firewalls, security suites, anti-malware programs, encryption of all communication channels)
  - Dedicated, single purpose computer for online banking and cash management
    - should not allow web browsing, email, social networking
    - should not be networked
  - Disallow online banking from unsecured channels (e.g., wifi hotspots)
  - Multi-factor authentication
  - Limit use of administrative credentials

- Assume access controls will be defeated
Ways to Mitigate Electronic Payments Fraud

- **Account Security Measures**
  - Origination limits
  - Dual controls for origination
    - (e.g., two independent approvals from two different channels)
  - Out of band notification and approval
    - (e.g., callbacks, texts, faxes)
- **Transaction Monitoring**
- **Debit Blockers**
- **Debit Filters**
- **Positive Pay**
### Losses from Failure to Mitigate

<table>
<thead>
<tr>
<th>Primary Reason the Organization Suffered Losses from ACH Fraud</th>
<th>(Percent of organizations that suffered a financial loss resulting from ACH fraud)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did not use ACH debit blocks or ACH debit filters</td>
<td>55%</td>
</tr>
<tr>
<td>ACH return not timely</td>
<td>36%</td>
</tr>
<tr>
<td>Did not use ACH positive pay</td>
<td>36%</td>
</tr>
<tr>
<td>Account reconciliation not timely</td>
<td>18%</td>
</tr>
<tr>
<td>Criminal takeover of my online system to initiate fraudulent transactions</td>
<td>18%</td>
</tr>
<tr>
<td>Internal fraud (e.g., employee responsible)</td>
<td>9%</td>
</tr>
<tr>
<td>Inaccurate key-entry error</td>
<td>9%</td>
</tr>
<tr>
<td>Gaps in online security controls</td>
<td>9%</td>
</tr>
<tr>
<td>Other</td>
<td>9%</td>
</tr>
</tbody>
</table>

Source: 2009 AFP Payments Fraud and Control Survey
“The chief executive was at a dinner party late last summer when he received an odd message. First Midwest Bank, where his company held a corporate account, had sent an alert to his cell phone describing multiple pending funds transfers that would have siphoned thousands of dollars from the company's account, none of which the executive had authorized. But, instead of getting ripped off, and rather than trying to mitigate the theft attempt by running to the office to investigate or make frantic phone calls to the bank, ruining an otherwise pleasant night, he simply pressed "9" and the pound sign on his cell to report the fraud, and continued his evening. The transfers never went through. And even if he were unable to access his phone, no funds would have moved. That's because he had enrolled his company in First Midwest's phone-based, out-of-band verification system, provided by PhoneFactor, which had launched a few weeks earlier and requires the executive authorize any of his company's wire or automated clearing house transfers.”

Source: American Banker, December 2011
 Procurement Card Fraud

- Common types of procurement card fraud
  - Theft
  - Misuse
  - Compromised accounts
  - Skimming
Card Fraud Scenarios

• **Skimming** (*True Story*)
  - Interagency conference of bank examiners and their lawyers in Chicago and all of their cards got skimmed at the restaurant.

• **Employee Misuse** (*True Story*)
  - A program coordinator at a large state university was issued a purchasing card (p-card) for use in the course of her duties. She used the card to make purchases of personal items and pay for personal expenses totaling $173,186.46 during a four year time period. The theft caused money to be drawn from several of the university’s foundation accounts.
Ways to Mitigate Procurement Card Fraud

- Segregation of responsibilities
- Transaction and monthly limits
- Block unauthorized vendors
- Regular audits
- Transaction monitoring
Rapid Response Plan

- Evaluate agency risk profile with respect to the different types of fraud and implement a security and rapid response plan appropriate for the business (e.g., you can respond quickly and your bank can respond to you quickly)
  - Contact data security/IT to determine when, where and how your account was compromised
  - Immediately notify your bank and have a contingency plan in place to recover compromised systems and funds
  - Reverse the transaction
  - Contact recipient bank to hold/grab funds
- Notify executive management
- Disable online access to affected accounts and change username/password
- Check for account profile changes (new payee, phone, address, pin, new checks)
- Maintain chronology of what happened
- Report to insurance company, FBI, local law enforcement (police report)
Where Does that Leave Us?

- Banks and customers are in this together (with the “bad guys”)
- Data security more expensive in dynamic defense environment
- Institute strong controls and frequently audit
- Leverage tools provided by your bank
- Engage your bank for “worst case scenario”
- Educate and train your employees
The End – Questions?