



Essential Tools: The Fraud-Fighting Tools of Treasury Management

Mitigate the Opportunity for
Fraud to Affect Your Bottom Line

Arlen S. Lasinsky, CPA /CFE/CFF/CTP – Frost, Ruttenberg & Rothblatt, PC
Kristen L. Saranteas, CTP – Wintrust Commercial Banking

Copyright 2011 Frost, Ruttenberg & Rothblatt, P.C. and Wintrust Financial Corporation All Rights Reserved

Treasury Management Essentials
Sponsored by:

WINTRUST
COMMERCIAL BANKING

Agenda



- The Fraud Landscape
 - Real-life Examples
- Actions Taken/Lessons Learned
- Prevent the Fraud-Be Proactive
- Heads Up; A Fraud May Be Occurring
- Tag-You're a Victim; Now What?

The Fraud Landscape



- 2011 AFP Payments Fraud & Control Survey
 - 71% of all organizations experienced attempted or actual fraud in 2010
 - The larger the company, the more prevalence of fraud
 - 29% responded that fraud increased in 2010
 - 93% affected had checks compromised
 - 25% ACH debit
 - 23% Consumer credit/debit card
 - 15% Corporate/commercial card
 - 4% ACH credits
 - 4% Wire transfers

The Fraud Landscape...continued



- 2011 AFP Payments Fraud & Control Survey
 - 71% of organizations that were fraud victims experienced no financial loss
 - \$18,400 was typical financial loss
 - Fraud tools used at bank to prevent financial loss
 - 84% Positive Pay/Reverse Positive Pay
 - 76% ACH debit blocks
 - 61% ACH debit filters
 - 58% Payee Positive Pay
 - 36% of companies that do not use fraud-prevention services cite cost/benefit not justifying the use

Real-life Example...



- Large medical institution decides to use positive pay since they were having issues with fraudulent checks
 - Two checks issued to pay US vendors
 - Client received call from bank that the checks were attempting to be deposited in South America for \$675M and \$820M
 - Checks were returned with no loss to the client
 - Perpetrators found; fraud stopped

Action Taken/Lessons Learned



- Bank tools to use to mitigate financial loss
 - Positive pay / ACH debit blocks & filters
 - Post no debit accounts
- Internal controls
 - Employees:
 - Segregation of duties; hiring procedures; testing of processes; approval levels; fraud hotline
 - Accounting / Treasury Department:
 - Audit, Review or Compilation and Testing

The Fraud Landscape...continued



- 2011 AFP Payments Fraud & Control Survey
 - 88% of organizations have increased their use of electronic B-to-B payments
 - 86% have increased use of electronic payments to employees
 - 80% have increased use of B-to-C payments with fraud prevention in mind
 - 75% of organizations have separate account for collections and disbursement
 - 47% have separate bank account per payment type
 - 36% have separate accounts for receiving ACH debits
 - 14% of organizations were subject to a fraud attempt targeting user IDs and passwords

The Fraud Landscape...continued



According to the ACFE Report to the Nation:*

- Occupational frauds are much more likely to be detected by tip than by any other means.
- Small organizations are disproportionately victimized by occupational fraud.
 - Lacking in anti-fraud controls due to size
- Perpetrators display warning signs
 - Living beyond their means (43% of cases)
 - Experiencing financial difficulties (36% of cases)
- Fraud lasted a median of 18 months
 - Lack of controls and testing

*2010 Report to the Nation by the Association of Certified Fraud Examiners

Real-life Example...



- Manufacturer was victim of payroll check fraud sporadically
 - Instituted direct deposit for those employees that elected
 - Decided to institute payroll cards for those not using direct deposit
 - Elimination of check fraud completely
 - Electronic payroll can save a company with 100 employees \$19M p/year*

*NACHA Press Release , Herndon, VA, October 14, 2010

Actions Taken/Lessons Learned



- Account structure to assist in fraud prevention
- Movement from paper-based to electronic payments
- Prevalence of Information Reporting, with security features
 - Use Alert Technology

The Fraud Landscape...continued



- 2011 AFP Payments Fraud & Control Survey
 - Check Fraud remains the top method
 - 68% are counterfeit checks using the MICR line data
 - 56% alter payee names on checks issued
 - 35% alter dollar amount on checks issued
 - 14% of organizations that were victims of check fraud suffered a financial loss
 - ACH Fraud prevalent, to a lesser degree
 - 12% of organizations that were victims of ACH fraud suffered a financial loss
 - Losses resulted from not following best practices and/or neglecting to execute own business rules (ie. timely ACH returns, takeover of systems, not using ACH positive pay)

Actions Taken/Lessons Learned



- Tools
 - Focus on checks – AR & AP
 - ACH debit blocks & filters
 - Clock is ticking – review account daily
 - Secure data in the office, online
 - Utilize CD-Roms
 - Utilize system security

The Fraud Landscape...continued



- 2011 AFP Payments Fraud & Control Survey
 - Business-to-Business Card Fraud
 - 77% of organizations with fraud on their own cards report an unknown external party committed fraud
 - 10% of organizations with fraud on their own cards report a third-party (such as a vendor) committed fraud
 - 32% of organizations subject to fraud suffered a financial loss
 - 14% of organizations that accept commercial cards from partners suffered a financial loss
 - Average cost of maintaining PCI compliance is \$13,400 per year

Actions Taken/Lessons Learned



- Card control
 - Online review
 - Open/close cards & manage limits
 - Centralize use
 - Utilize SIC code & other controls
 - Separation of duties for reconciliation

Preventative Measures



- General
 - Engage outside professional to test internal controls
 - Accounting firm for audit, review or compilation
 - Insurance policies
 - Protection of hardware & software
 - Security of documents / checks
 - Back-up information & review procedures
 - Observe behavior
 - Pursue unusual behavior or transactions

Preventative Measures...continued



- **Cyber Security**
 - Business use only
 - Proper use & security of passwords
 - Scan regularly
 - Firewalls / Security programs
 - Check software settings
 - Separate user accounts
 - Write and regularly test business continuity plan
 - Procedures for review

Warning Signs



- People
 - Employee habits/lifestyle
- Data
 - Information not being shared
- Vendor(s)/Bank(s) call with service or payment inquiries
- Accounting
 - Variances in results vs. budget
 - Slower-than-normal collection of A/R
 - Slower-than-normal reconciliation
 - Co-mingling of funds among various entities
 - Reports not prepared timely

Steps to Take if Fraud Occurs



- Quickly: Engage forensic accountant; contact banker; and contact insurance company
- Call law enforcement after checking with legal counsel
- Do not have IT personnel attempt to find the problem
- Implement disaster recovery plan
- Implement new controls

Steps to Take if Fraud Occurs...continued



- Banking
 - Harmed accounts can be monitored
 - Use new controls through new accounts
 - Appropriate signers / controls
 - Blocks to transactions
 - Securely notify approved clients / vendors of new account
 - Cancel credit cards

Tips



- Fraud is a crime of opportunity
- Don't be complacent
- Be sure there are checks and balances
 - Perpetrators take path of least-resistance
- Be pro-active, not reactive, in your response to fraud

QUESTIONS?

Treasury Management Essentials sponsored by Wintrust Commercial Banking

