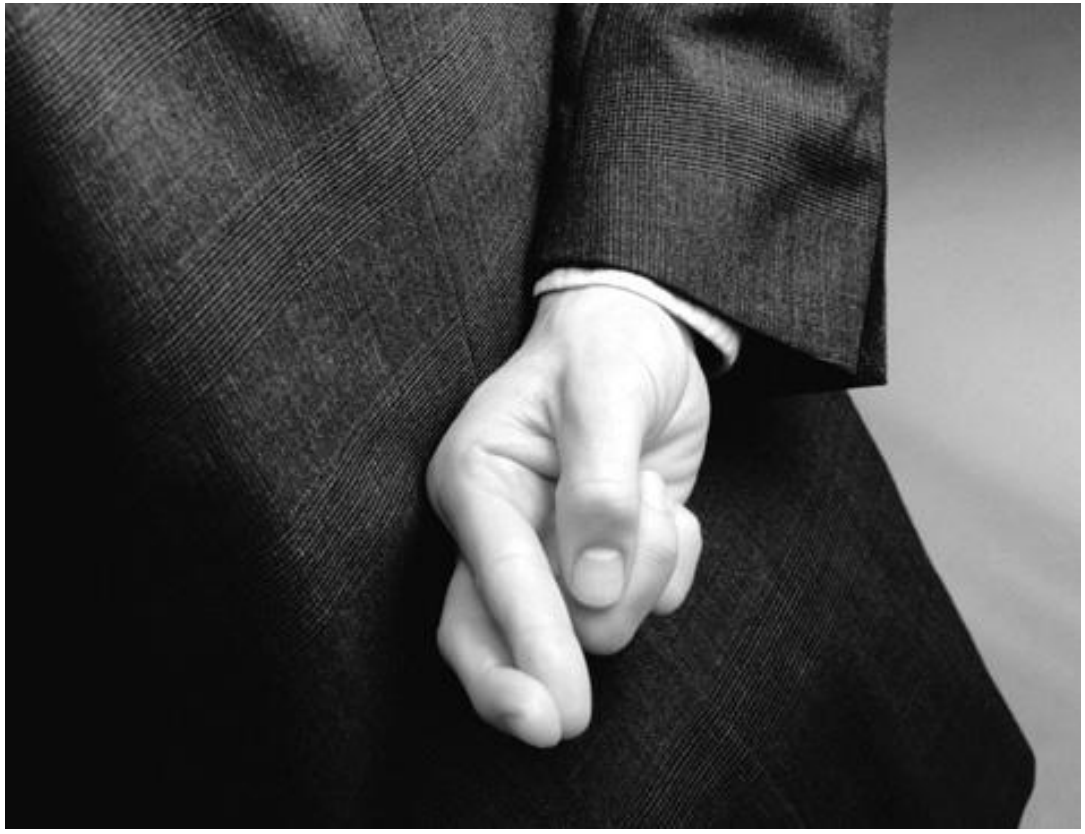
Fraud Prevention

Best Practices from a Provider and Bank Perspective



Presented by:

Kirt Slaugh

KeyBank National
Healthcare Payments
Sales Manager

October 14, 2013

KeyBank

KeyBank

Payments industry fraud: A few things to consider

According to the 2013 AFP Payments and Fraud Control Survey:

- 61% of organizations experienced attempted or actual payments fraud
- 27% reported an increase in the number of fraudulent incidents
- 16% reported a decrease
- 87% of affected organizations reported that checks were targeted
- 29% of those affected reported that corporate/commercial purchasing cards were targeted
- Average loss was $20,300
- 64% of respondents discussed fraud prevention/security with their bank at least once in 2012

Payments industry fraud: A closer look

(cont'd.)

Today's criminal:

- Oftentimes belongs to an organized group
- Stalks their victim and knows how to attack weak points
- Has access to very sophisticated physical and electronic tools

Fraud Origination	
Outside individual	80%
Organized crime ring	18%
Internal party	10%
Third-party or outsourcer	5%
Account takeover	5%
Other	5%
Lost or stolen laptop	1%
Compromised mobile device	<1%

Source of Payments Fraud in 2012, as reported in the 2013 AFP Payments Fraud and Control Survey. (Percent of Organizations Subject to Attempted or Actual Payments Fraud)

Fraud Risks to Healthcare Providers

Internal Risk / Employee Embezzlement

- Incoming Payment Risks
- Outgoing Payment Risks
- Illegitimate vendors

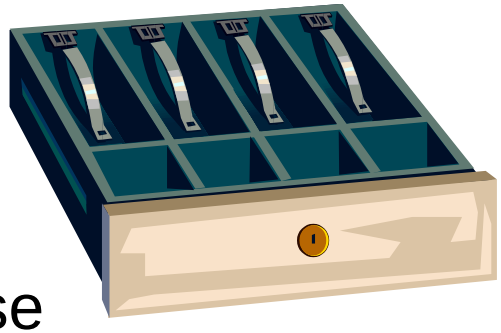
External Risk

- Organized Crime Rings
- Less sophisticated fraudsters
- Opportunists

Internal Risk – Fraud Triangle

Internal Risk – Incoming Payments

Dipping into the cash drawer



Rebate Programs

- Not typically a receivable set up for these
- Example – Commission Recapture
- Example – Securities Litigation Settlements
- Make sure you identify all rebate situations and have controls in place
- Be aware!

Internal Risk – Outgoing Payments

Lack of Sufficient Dual Controls

- Inadequate backups
- Sharing of passwords and improper access
- Use of “Super Users” who are outside of dual control process

Failure to Cross Train Employees

Lack of Sufficient or Updated Policy and Procedures or Lack of Training

Structuring Dual Controls in Treasury

Three Roles Identified at Intermountain

1. Payment and Template Initiation/Setup
   Treasury Operations

2. Review/Approval of outgoing payments
   Accounting

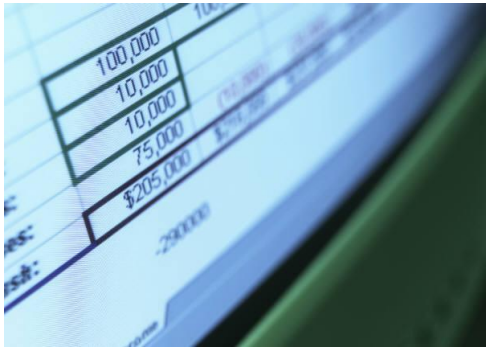
3. Security Administrator
   Senior Accounting and/or Treasury

Role of Treasury Operations

- Review all incoming requests for sufficient documentation
- Initiate and setup all new outgoing payments
- Setup or initiate modifications of new Fedwire or ACH templates
- Coordinate review process and signing of new account signature cards and banking contracts
- Manage process for opening new accounts
- Maintain documentation of wire and ACH templates

Role of Staff Accounting

- Approve all templated outgoing payments
- First approver on all non-repetitive wires and ACH
- Make entries to the general ledger to record outgoing payments
- Reconcile bank accounts to general ledger



Role of Security Administrators

- Final approver on non-repetitive wire or ACH transfers
- Assume self administration role in banking platforms
  - Set up and modify user access (Not a Super User)
  - Reset passwords
- Approve new ACH/Wire templates
- No ability to initiate wires or ACH payments
- Maintain Corporate Resolutions and Bank Signature Cards
- Role defined on the corporate resolution so that the bank was required to only accept signature cards from a security administrator
- Approves Bank Reconciliations
- Ensures Policy and Procedure are up-to-date

Logistical Challenges and Areas to Watch

- You need to have at least one and preferably two backups for each role in order to cover the cash desk when people are out

- Make every effort to cross train enough individuals so that you don't have to compromise dual controls.

- Don't automatically assume your bank's treasury platform automatically enforces dual controls, we had a situation at Intermountain where a bank's ACH module didn't enforce dual controls on template changes

External Fraud Risk

- Failure to utilize or fully utilize fraud prevention services provided by your bank
- Inadequate hardening of systems to protect payment card information
- Insufficient Policies and Procedures as it relates to:

Document Shredding/destruction

Unsecured data repositories (Physical or electronic)

External Risk - Things to Review with Your Bank

Should have **positive pay** or **payment protection** on all disbursement accounts

- No exceptions or hand check accounts
- Make sure that the default decision is set to “reject”
- Utilize payee name in the positive pay file if possible

For all accounts utilize ACH debit blocks or filters (EPA)

Make sure you also utilize check draft protection (controlled accounts) for all non-disbursement accounts

External Risk - Securing Your Payment Cards

- Fully understand the PCI DSS standards and ensure that you comply with both the letter and the spirit of the standards

- Before you spend enormous amounts of money to become compliant, look for ways to take large chunks of data out-of-scope.

-Consider a PCI Compliant Patient POS system for patient facing transactions

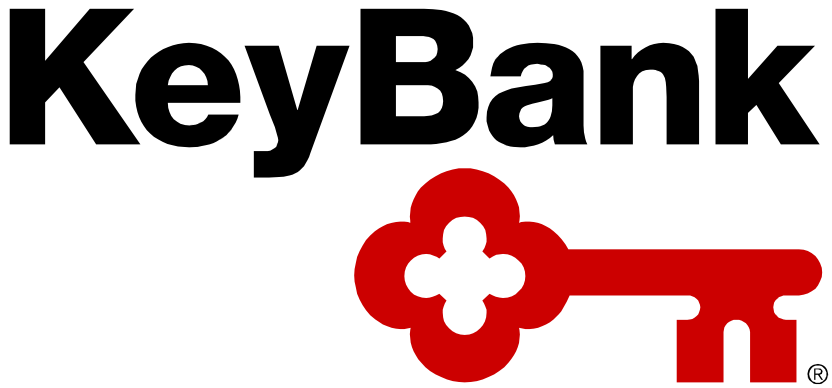
-Explore concepts such as “tokenization” to enhance security and decrease compliance expense and effort

External Risk - Keep your Policies and Procedures Updated

- Make revisiting processes and updating policies a scheduled part of your treasury and accounting team's job

- Have a systematic way to ensure new hires are properly trained on policy and procedure

- Make sure that you have buy-in from senior management on the importance of security and that this priority gets communicated down to Treasury, AP, IT and PAS areas of the organization.


KeyBank