Misplaced Trust: Vendor Fraud

IIA/ACFE Conference
Patrick Mitchell, Managing Director
Sharon Delgado, Senior Manager

April 17, 2015
Today’s Discussion Summary

Vendor fraud is a form of occupational fraud where the fraudster manipulates the company’s accounts payable and payments systems for illegal personal gain. Vendor fraud generally falls into three categories:
• Billing schemes
• Check tampering or
• Bribery and extortion.

This presentation is intended to provide specific techniques that will improve your ability to identify and investigate vendor fraud, as well as provide you with insight into building preventive controls through a vendor risk management program.

Topics covered will include:
• Identifying Vendor Fraud
• Developing an Investigative Plan
• Enhancing Your Vendor Risk Management Program
Identifying Vendor Fraud
Definitions of Common Vendor Fraud Schemes

• Billing Schemes
  ─ Shell company
  ─ Non-accomplice vendor schemes

• Check Tampering Schemes
  ─ Forgery
  ─ Altering payee information
  ─ Issuing inappropriate manual checks

• Bribery or Extortion Schemes
Identifying Vendor Fraud

- Review Vendor Master files
- Look for unknown company names
- Perform periodic background checks
- Look for trends or patterns with approved vendor invoices
- Compare mailing addresses against employee database
- Investigate vendors with PO Boxes for addresses
- Verify tax ID and business phone number
- Confirm ownership through state, business registration databases
- Look for potential employee or Board Member conflicts
- Perform periodic independent review of vendor set-up process
- Establish segregation of duties between receipt of goods and payment of invoices
Background Investigation Resources

Tools to assist with investigating vendor fraud can include:

- Lexis-Nexis
- Secretary of State Records
- Local/Federal Criminal and Civil Filings
- Media and Internet Sources
Does your organization have a dedicated fraud investigation department or is it incorporated within another initiative, such as Internal Audit?
Developing an Investigative Plan
Developing an Investigative Plan

<table>
<thead>
<tr>
<th>Define the Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chain of Command</td>
</tr>
<tr>
<td>Who Needs to Know?</td>
</tr>
<tr>
<td>Protocols for Communication of Progress</td>
</tr>
<tr>
<td>Timeline for Completion and Status Updates</td>
</tr>
<tr>
<td>Preservation of Evidence</td>
</tr>
<tr>
<td>Who Will Collect Evidence/Chain of Custody</td>
</tr>
<tr>
<td>Prepare an Interview List</td>
</tr>
<tr>
<td>Who Will Conduct the Interviews?</td>
</tr>
<tr>
<td>Anticipated Methods of Data Collection</td>
</tr>
<tr>
<td>Attorney Client Privilege</td>
</tr>
<tr>
<td>Documentation/Deliverables</td>
</tr>
</tbody>
</table>
Establishing Investigative Protocols

- Review concern or complaint
- Understand your whistleblower policy (i.e., anonymity and confidentiality)
- Establish communication protocols
- Conduct informational discussions
- Secure data in whatever form; this may include changing locks
- Preserve originals (i.e., do not staple, hole punch, write-on, mark or alter in any way)
- Review books and records, including information that may be maintained off-site in archives

- Review office contents of relevant individuals
- Confirm balances with customers/vendors
- Perform background checks
- Review the work previously performed by Internal Audit, including any system or internal control narratives
- Review Board of Director and/or Audit Committee minutes
- Perform “undeletes” and review hard-drive contents
- Recover and review e-mail
- Interview relevant individuals
Investigations – Sources of Data

- Email and file servers
- Desktops, laptops, peripherals and electronic devices
- Structured data: Identifiable data that is organized in a structure
  - Databases
  - Logs
  - Records
  - Transactions
- Unstructured data: Information that either does not have a pre-defined data model and/or does not fit well into relational tables
  - Often text-heavy information
  - Documents
  - Email
  - Voicemail
- User-created or system-generated data
Internal Investigations – The Written Report

- Allegation and Background
- Methodology Utilized
- Observations and Discussion of Evidence
- Recommendations
- Ownership of Corrective Action Items
Enhancing Your Vendor Risk Management Program
Audience Question

Who within your organization is primarily responsible for vendor management?

• Dedicated Vendor Management Department
• Procurement
• Decentralized/Managed by Individual Business Units
• Other?
Protiviti’s Vendor Risk Management Survey

2014 Vendor Risk Management Survey

• Nearly 450 respondents across multiple industries provided data.
• Rated components of their programs on the Capability Maturity Model (CMM)
• Overall topics covered:
  — Program Governance
  — Policies, Standards & Procedures
  — Contracts
  — Vendor Risk Identification and Analysis
  — Skills and Expertise
  — Communication and Information Sharing
  — Tools, Measurement and Analysis
  — Monitoring and Review
• More information at www.protiviti.com/vendor-risk
Vendor Risk Management Survey - Results

**Summary**

- Financial services tend to have relatively mature vendor risk management programs when compared to other companies.
- Insurance organizations are at a lower overall maturity level when compared to financial services.
- Overall maturity in key areas varied between 2.3 (Repeatable) and 3.0 (Defined).

<table>
<thead>
<tr>
<th>Vendor Risk Management – Overall Maturity by Area</th>
<th>Maturity Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program Governance</td>
<td>2.9</td>
</tr>
<tr>
<td>Policies, Standards, Procedures</td>
<td>2.9</td>
</tr>
<tr>
<td>Contracts</td>
<td>3.0</td>
</tr>
<tr>
<td>Vendor Risk Identification and Analysis</td>
<td>2.7</td>
</tr>
<tr>
<td>Skills and Expertise</td>
<td>2.3</td>
</tr>
<tr>
<td>Communication and Information Sharing</td>
<td>2.6</td>
</tr>
<tr>
<td>Tools, Measurement and Analysis</td>
<td>2.4</td>
</tr>
<tr>
<td>Monitoring and Review</td>
<td>2.9</td>
</tr>
</tbody>
</table>

Respondents were asked to rate its maturity level as it applies to their organization, according to the following scale: 1) Initial visioning, 2) Repeatable, 3) Fully defined and established, 4) Fully implemented and managed, 5) Continuous improvement – optimizing.
Enhancing Vendor Risk Management Program Maturity

Two key areas (Program Governance, and Policies, Standards & Procedures) were rated 2.9 on the scale.

These areas serve as the cornerstones of a strong vendor risk management program. Higher maturity levels for them would be expected but are not evident in the survey results.
Program Management

**Termination**
Institutions should ensure they can **terminate relationships when required** due to a variety of reasons, and as such have appropriate plans in place to transition activity if needed based on the products and/or services being provided.

**Planning**
An established process that outlines the **strategic requirements** for an individual process and the associated requirements for a new (current) third party relationship.

**Due Diligence and Selection**
Institutions should conduct **risk based due diligence** on all potential third parties before selecting and entering into contracts or relationships.

**Contract Negotiation**
Established processes should be defined to ensure that **new contracts capture the risks** appropriately, appropriate reviews and approvals are completed, and **periodic assessments of current contracts** are completed against recent standards.

**Ongoing Monitoring**
Enterprise wide processes that ensure **adaptive oversight** activities based on key risk factors for each vendor.

**Effective Third Party Management**

**Oversight and Accountability**
**Documentation and Reporting**
**Independent Reviews**
Best Practices

- **Professional Qualifications**
  - Check if a vendor has specific licenses, bonds and experience relevant for the services.

- **Outsourcing Risk Management Program & Customer Service**
  - Establish a comprehensive outsourcing risk management program to address outsourced activities and relationships with service providers.

- **Flexibility of the Contract**
  - Establish a written procedure for the contract review, including expectations for analysis, notation, and escalation of key contractual issues.
  - Contracts that have severe penalties for seemingly small incidents should be avoided. If the vendor asks for an extremely long term contract, ask for a shorter term with a renewal option.

- **List & Rate Each Vendor**
  - List anyone you’re doing business with – anyone you outsource to in some function and rate each vendor on criticality and confidentiality.

- **Rate Each Vendor on Confidentiality**
  - Identify what customer information each vendor has access to – account numbers, names, addresses, account info. As with criticality, rank this access high, medium or low.
  - Find out how payroll data is given to the provider each pay period. Ensure that it is secure.
## Best Practices (Contd.)

| **Due Diligence** | • Collect evidence of control and risk mitigation processes in place by vendor. Verify the vendor’s plan of action with the organization's plan for consistency.  
• Analyze their disaster recovery plan and liability policy.  
• Check references and be sure other clients report satisfaction. |
| **Monitor Performance** | • Monitor the vendor's performance constantly. This should include the requirements that are most critical to the business. For example: shipping times, quality of service performed, order completion, call answer time, etc. |
| **Request improvements or switch vendors** | • If the vendor doesn’t have adequate controls in place, an organization needs to have a dialogue and convince the vendor to meet the standards. In the event the vendor does not meet the requirements, the organization should change the vendor. |
| **Reevaluate** | • Annually, evaluate the risk ratings of the vendors. In addition, reevaluate high risk vendors to make sure their controls are appropriate for the current risk environment. Has the relationship changed in the last year? Have security threats evolved? Are their certifications up-to-date and contracts current? |
| **Communicate Constantly** | • A well established and well maintained line of communication will avoid misunderstandings and proactively address issues before they become problems. |
Vendor Management Internal Audits

- Scope Considerations (applicable for both prospective and current vendors)
  - Background information on vendor
  - Documentation and licenses on file
  - Risk rating process
  - Evaluation of internal, ongoing vendor monitoring
  - Access Controls
  - Network Level Security
  - Change Control
  - Reporting & Visibility

- Frequency
  - Classification of vendors by criticality
Contact Information

Patrick Mitchell  
Managing Director

Director: (954) 712-3109  
Mobile: (954) 531-2662  
patrick.mitchell@protiviti.com

Sharon Delgado  
Senior Manager

Director: (954) 712-3126  
Mobile: (305) 321-3656  
sharon.delgado@protiviti.com
Confidentiality Statement and Restriction for Use

This document contains confidential material proprietary to Protiviti Inc. ("Protiviti"), a wholly-owned subsidiary of Robert Half ("RHI"). RHI is a publicly-traded company and as such, the materials, information, ideas, and concepts contained herein are non-public, should be used solely and exclusively to evaluate the capabilities of Protiviti to provide assistance to your Company, and should not be used in any inappropriate manner or in violation of applicable securities laws. The contents are intended for the use of your Company and may not be distributed to third parties.