Fraud Discussion

Lore de la Bastide, Vice President & General Auditor
Consolidated Edison Company of New York

Christine Neely, Vice President, Internal Audit Services
Public Service Enterprise Group

Martin Biegelman, Managing Director
Deloitte Financial Advisory Services LLP
Agenda

• Introduction
• Defining Fraud
• Cost of Fraud
• Drivers for Committing Fraud
• Survey Key Takeaways and Examples
• Leading Practices for Fraud Prevention and Detection
• Takeaways
• Q & A
Defining Fraud

“The knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment and a misrepresentation made recklessly without belief in its truth to induce another to act.”
– Black’s Law Dictionary

“Any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises.”
– Mail Fraud Statute

“The use of one’s occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization’s resources or assets.”
– Association of Certified Fraud Examiners

“The crime of using dishonest methods to take something of value from another person.”
– Merriam-Webster Dictionary
Cost of Fraud

89% Of frauds are caused by asset misappropriation with a median loss of $114,000

53% Of victim organizations have not recovered any of their losses due to fraud

Only 4% Of perpetrators had prior convictions

5% Of an organization’s annual revenue is typically lost to fraud

Common fraud schemes

3% register disbursements
10% payroll
14% skimming
9% financial statement
21% non-cash
30% corruption
15% cash on hand
8% larceny
15% check tampering
17% expense reimbursements
26% billing fraud

Drivers for Committing Fraud

- Living beyond one’s means
- Unusually close association w/ vendor
- Financial difficulties
- Lack of segregation of duties
- Recent divorce/family issues
- “Wheeler-dealer” attitude
- Defensiveness
- Addiction problems
- Excessive pressure
- Social isolation
- Refusal to take vacations
- Past employment problems
- Past legal problems
- Inadequate anti-fraud controls
- Poor tone at the top/mood in the middle

Polling Questions

1. Is fraud one of your top enterprise risks?

2. How many of you have a dedicated anti-fraud program?

3. Does your organization actively and continuously promote a speak-up culture to report concerns?
Survey Key Takeaways

How would you rate the overall maturity of your Fraud Prevention Program?

- Low: 8%
- 2: 12%
- 3: 36%
- 4: 44%

Note: 1 was 0%

EEI-AGA 2018 Chief Audit Executives Conference
Survey Key Takeaways

Do you plan to do something different with your Fraud Prevention Program in the next 6-12 months?

- Yes
- No

- Implement a formal fraud risk management program
- Refine fraud risk assessment information to focus on most significant risks
- Identify internal controls to mitigate fraud risk schemes
- Enhance anti-fraud capabilities in Internal Audit and strengthen collaboration with key stakeholders across organizations
- Launch fraud awareness campaign
- Increase training and emphasis on third-party cyber fraud
- Assess ways to prevent and monitor internal fraud risks
- Review/update policies (anti-fraud, anti-bribery, whistleblower, etc.)
- Implement a fraud monitoring tool to help identify high risk transactions, etc.

48%
52%

Yes
No
Fraud Risk Management Program Example

• Review our existing strategies
  – Investigate incident locally, take corrective action, and communicate broadly
  – Maintain employee reporting systems to facilitate fraud detection

• Understand why fraud is missed
  – Too much trust is placed in those you work with
  – Not having a questioning attitude
  – Feeling a need to be liked by others and avoid conflict
  – Not prepared for or experienced in dealing with fraud
  – Lack of understanding of controls
Fraud Risk Management Program Example

• Conducted workshops to raise fraud awareness and encourage alert and proactive employees

• Conducted a Fraud Risk Assessment (FRA) for key areas to identify and prioritize fraud risk schemes

• Included fraud specific audits into the audit plan, as well as ongoing program review audits

• Included fraud steps in each audit, which included developing a repository of fraud risk schemes, and strengthening our fraud capabilities

• Created a separate group in Internal Audit to build a sustainable program that focuses on fraud proactively and enterprise-wide

~ Financial Integrity Group
Fraud Risk Management Program Example

Everyone has a seat at the table
Survey Key Takeaways

Where we are falling behind or want to improve

- Enhance use of data analytics was the most frequently identified area for improvement
- Conduct periodic third party assessments of anti-fraud program effectiveness
- Use metrics or KPIs to track anti-fraud activities
- Utilize a QA approach to systematically evaluate and monitor fraud risk management program effectiveness
- Improve current detailed risk assessment to focus on more meaningful, common fraud scenarios and true risks
- Monitor disciplinary actions for consistency and trend analysis
Survey Key Takeaways

Examples of leading practices from the survey:

• Investigations and Audits:
  – Performed investigations-like audits with formal findings and recommendations
  – Choose auditors with an aptitude for conducting interviews to investigate
  – Corporate investigators provide input into planning for each audit
  – Periodic fraud risk assessments inform audits and high risk area reviews

• Training and Communication:
  – Developed training video using real employees to reinforce fraud prevention
  – Business integrity program activities/metrics are reported to the Board

• Organization:
  – Dedicated audit group to proactively prevent and detect fraud enterprise-wide
  – Multi-disciplinary anti-fraud committee meets quarterly to review trends and share information
Fraud Prevention Example – Phishing

Combined education, corrective measures and disciplinary actions to reduce the avoidable risk of a cyber breach from phishing email

Phishing Fundamentals training provided to employees followed by 6-10 phishing exercises annually

Failure 1 - Raise awareness
- User is provided with immediate education after failing a phishing exercise
- Reminder of available resources, and consequences for repeated failures

Failure 2 - Communicate to individual and supervisor of record
- User is provided with immediate education
- IT Information Security sends email to user and respective supervisor with awareness information, and reminder of consequences for repeated failures

Failure 3 - Escalate to EOG/Officer and require training
- User is provided with immediate education
- CIO notifies supervisor, EOG member and Vice President of the third consecutive failure
- Individual must complete Phishing Fundamentals training

Failure 4 - Suspend without pay and require training
- One month suspension without pay
- CIO notifies supervisor, EOG member and Vice President of the fourth consecutive failure
- Company network access removed for one month
- Individual must complete training
- Corrective action letter issued and impact to overall performance evaluation

Failure 5 – Discharge of employment
- Employee is discharged

*Failure is defined as taking the following actions in response to a phishing email exercise: clicking a link, opening an attachment, and/or providing sensitive information. Measured based on consecutive failures.
Polling Questions

1. How many of you require periodic job rotation?
2. How many of you require mandatory vacations?
3. Does your organization share sanitized versions of fraud investigation results with your employees?
4. Does your organization have a standalone anti-fraud policy?
Leading Practices for Fraud Prevention and Detection

- Code of conduct
- Strong tone at top
- Background checks
- Anti-fraud policy
- Dedicated anti-fraud program
- Hotline
- Fraud risk assessments
- Fraud training for employees
- Predictive data analytics capabilities
- Certified Fraud Examiner certification
- Segregation of duties
- Job rotations
- Mandatory vacations
- Effective internal audit
- Surprise audits
- Culture surveys
- Compliance & ethics newsletter
- Proactive data monitoring

Takeaways

How would you rate the overall maturity of your Fraud Prevention Program?

Do you plan to do something different with your Fraud Prevention Program in the next 6-12 Months?
Thank you!

Q & A