Risk and Performance Quarterly

Organizations Must Address Fraud Risk on a Continuous Basis

By Larry Baye, CMC, CISA and Mark Bednarz, CPA, CISA, CFE

Unfortunately, fraud is an all-to-common occurrence and no industry is immune. Intentional deception to realize unlawful gains are often perpetrated by an organization's own management or employees, with or without the assistance of outside parties. Personal enrichment, stressful situations (e.g., the pressure to repay gambling debts or support a drug habit), getting even with a manager (e.g., an employee is disgruntled because they were passed over for a raise or promotion) and covering up prior financial reporting errors are just some of the many motivating factors that drive this behavior.

Consequences of Fraud

When an organization falls victim to fraud, they typically experience one or more of the following:

- Disruption of normal day-to-day operations that also distracts management
- Loss of confidence and trust, which may spur valued employees to seek other positions and shareholders, donors and customers to question whether they want to be associated with an entity with a tarnished reputation
- Potential liability to those charged with governance at the executive and Board levels
- Unwelcomed scrutiny by governmental entities and the media
- Unplanned costs incurred in connection with the investigation and taking corrective action

Proactive Measures Management Should Take

There are some basic "blocking and tackling" measures that each organization should take to prevent fraud. The starting point is good governance. At a minimum, all organizations should have a code of conduct, conflict of interest disclosure rules, formal policies and procedures, easy-to-access whistleblower hotline, independent Board members, a culture predicated on trust and accountability, strong operational and fiscal controls as well as an effective way to report and respond to alleged incidents of fraud.

Further, every organization should conduct a **Fraud Risk Assessment** and keep it refreshed that helps:

- Identify how fraud could occur based on the organization's specific points of vulnerability (e.g., people, process, systems, culture, locations, asset security, segregation of duties, transaction approval, account reconciliation and analysis)
- Determine the ways in which controls could be circumvented, overridden and masked
- Assess the likelihood and impact of such an occurrence
- Evaluate what controls are in place to prevent or detect fraud and how to remediate the gaps

Real Cases

By example, we have described below a number of actual frauds and the measures we believe could have prevented or detected the activity, had they been in place at each organization:

Diversion of Funds: An Accounts Payables Supervisor at a social services agency disbursed funds to family members by setting them up as vendors, creating fictitious invoices and then processing payments. *Had the agency established proper segregation of duties, required invoice approval by both the individual who initiated the purchase and the individual's Manager, required independent evidence that the goods*

were received and compared the vendor's address to the residences of the employees, this fraud could have been prevented.

Misappropriating Assets: A salesperson working for a software company stole copies of the customer list and forwarded the program source code to a friend who was developing a comparable product for a new business. *Had the organization restricted access to the underlying program code to only their development team and used data loss tools to prevent saving or forwarding sensitive files, they would not have had to rely on a customer alerting them to a new product that appeared to offer similar features and look and feel as the software they were already using.*

Receiving Kickbacks from Suppliers: A hospital Facility Manager received kickbacks in the form of cash and vacations from an air conditioning contractor responsible for the replacement and maintenance of the standalone units. *Had management questioned why these new units frequently failed and why the repair or replacement was not covered by the product warranty, this scheme could have been stopped early on.*

Obtaining Reimbursement of Personal Expenses: An employee of a professional services firm submitted receipts for gifts, massages and other expenses that were of a personal – not business – nature and, on occasion, requested reimbursement for the same items by submitting the credit card statement in a subsequent period. *Having the employee's supervisor review the expense report to check the business purpose and establishing a policy of requiring original receipts would have stopped this practice.*

Manipulating Financial Results to Enhance Profits: To meet sales targets, an electronics distributor provided incentives for customers to buy more product at quarter-end and had side arrangements that allowed them to return extra items the following period for full credit. In addition, on occasion, the dates of certain shipments were adjusted so they could be reflected in the period that was short of sales. *Having stronger revenue recognition and sales policies and enforcing cutoffs would have made this fraud harder to perpetrate.*

Doing Business with Related Parties: The President of a life sciences company retained a marketing firm owned by his wife to help launch a new product, but failed to disclose the relationship to the Board. *Had other senior executives questioned why normal purchasing and bid procedures were bypassed and performed the necessary due diligence regarding the vendor's reputation and ownership, this relationship might have been detected before a contract was executed and payments to the vendor were made.*

Evaluate and Address

How well do you know your organization's vulnerability points and what steps are you taking to ensure you do not become the next victim of a fraud?

Contact Us

If you believe your organization would benefit by having a trusted and experienced advisor help establish pragmatic approaches to project management or have an independent party evaluate your project playbook, you can reach out to Larry Baye, Risk Advisory Principal (lbaye@pkfod.com) or Mark Bednarz, Risk Advisory Partner (mbednarz@pkfod.com) who will be pleased to discuss your organization's project.

About PKF O'Connor Davies

PKF O'Connor Davies, LLP is a full-service certified public accounting and advisory firm with a long history of serving clients both domestically and internationally. With roots tracing to 1891, twelve offices in New York, New Jersey, Connecticut, Maryland and Rhode Island, and more than 800 professionals, the Firm provides a complete range of accounting, auditing, tax and management advisory services. PKF O'Connor Davies is ranked 29th on *Accounting Today*'s 2019 "Top 100 Firms" list and is recognized as one of the "Top 10 Fastest-Growing Firms." PKF O'Connor Davies is also recognized as a "Leader in Audit and Accounting" and is ranked among the "Top Firms in the Mid-Atlantic," by *Accounting Today*. In 2020, PKF O'Connor Davies was named one of the 50 best accounting employers to work for in North America, by *Vault*.

PKF O'Connor Davies is the lead North American representative in PKF International, a global network of legally independent accounting and advisory firms located in over 400 locations, in 150 countries around the world.