# Stemming the flood of fraud

How to implement cost-effective anti-fraud tools **Interviewed by Kristen Hampshire**

Fraud floods the news these days, and any organization that lacks anti-fraud controls places itself at an increased risk of trying to plug leaks after the fact.

Many companies assume the greatest risks come from those outside the company, but oftentimes, fraud is committed by longtime employees who know how to work the system and disguise the financial leak, or by disgruntled workers who feel the company owes them something. Creating an anti-fraud policy is not enough; you also need to build an anti-fraud program and conduct regular assessments to truly mitigate the risk.

"The main type of fraud we are seeing today is asset misappropriation, which happens quite often," says Ron Steinkamp, principal, risk advisory services, Brown Smith Wallace LLC, St. Louis, Mo.

*Smart Business* spoke with Steinkamp about common fraud red flags and how businesses can effectively implement anti-fraud tools to mitigate risk.

**Ron Steinkamp**
Principal, risk advisory services
Brown Smith Wallace LLC

### How prevalent is fraud?

The Association of Certified Fraud Examiners (ACFE) 2010 Global Fraud Survey found that a typical organization loses 5 percent of annual revenue to fraud, with the average fraud occurring for 18 months before being detected. While any business is a potential target, the industries most commonly victimized are banking/financial, manufacturing, and government and public administration. Generally, there are three types of fraud: asset misappropriation, corruption and financial reporting. Asset misappropriation includes fraudulent disbursements, theft of cash receipts and other activities in which individuals steal or misuse resources. These frauds are the most frequent, with a median loss of $135,000, according to the ACFE.

With corruption — in which an employee uses influence in a business transaction to obtain personal benefit — there is a median loss of $250,000. The least frequent form of fraud is financial statement fraud, the intentional misstatement or omission of material information in an organization's financial report. However, its median loss exceeds $4 million.

### What are some common red flags for fraud?

Incentive, opportunity and rationalization are the three characteristics that form the fraud triangle and are the red flags of fraud. Typically, fraud occurs where there is incentive or need, such as personal debt, living beyond one's means or job frustration. Second, there is an opportunity, such as access to cash or inventory, weak internal controls, close relationships with suppliers or vendors or weak management. An individual may rationalize the fraud, feeling as if he or she is not being fairly compensated, or justify stealing money with the intention of paying it back. The fact is, this payback never happens.

### How can an organization prevent fraud in a cost-effective manner?

The key is to create an anti-fraud culture, which begins by setting the tone at the top. Leaders must set the example by behaving ethically and openly communicating expectations to employees. There must be a formalized code of conduct founded on integrity that is communicated to all employees, and all employees must be treated equally.

Many businesses establish anti-fraud policies but fail to follow through with the key step of educating employees. Fraud prevention begins during hiring, when companies should conduct thorough background checks on potential employees. Upon hiring, employees should be trained on company policies and procedures, including the anti-fraud code of conduct. To foster an ongoing ethical environment, refresher training should be conducted regularly. By creating an environment where fraud is not tolerated and attempts at fraud are promptly dealt with, a business sends the message to employees, vendors and clients that dishonest behavior will not be tolerated.

### What are the best ways to detect fraud?

The best way is to leverage your employees who are often the first to detect fraud. That's why it's very important to have an anonymous method of providing tips, such as a phone system or web-based tool. This should be available to customers and vendors, as well. Such a reporting system builds awareness of the anti-fraud culture and gives individuals a way to safely and effectively report suspicions. Other effective ways to detect fraud are by identifying fraud risks and by management's implementation and monitoring of appropriate internal controls. Periodic internal audits are also a strong detection method.

### What are some anti-fraud tools that can be used?

The foundation of an anti-fraud workplace is a formalized company code of conduct, which should include detailed guidance on permissible and prohibited behaviors and actions. The code should outline employees' responsibilities in the prevention and detection of fraud, and explain the process for communicating concerns about potential fraudulent activities. It's also important to have a clear, accurate picture of your fraud risks. Where are your weak spots? Are you unintentionally providing opportunities for fraud to occur?

A fraud prevention checkup will help frame the picture. This high-level assessment of an organization's fraud health focuses on fraud risk oversight, ownership and assessment. It includes reviewing fraud policy, controls and detection efforts. A more detailed fraud risk assessment includes identifying how fraud could occur within critical processes and who might be in a position to commit it. Fraud monitoring involves using data analytics to highlight red flags and potential errors, fraud, inefficient operations and targets.

A formal fraud review/investigation is best directed by a Certified Fraud Examiner (CFE), who can conduct a thorough, independent, objective review and provide solutions. Don't wait until you're under water to stem the tide. Proactive measures can prevent fraud and well designed detection programs can uncover existing abuses. <<

**RON STEINKAMP**, CPA, CIA, CFE, is principal, risk advisory services at Brown Smith Wallace, St. Louis, Mo. Reach him at (314) 983-1238 or rsteinkamp@bswllc.com.