Curtis C. Verschoor, CMA, CPA, Editor

Fraud Continues to Cause Significant Losses

Proactive prevention and detection methods are critical in minimizing the losses from fraud. A new report lists fraud detection techniques that your company should implement today.

One of the widely recognized benchmark studies of fraudulent activities in business is the biennial study of occupational fraud conducted by the Association of Certified Fraud Examiners (ACFE). Its *2014 Report to the Nations on Occupational Fraud and Abuse* is based on analysis of 1,483 survey responses by Certified Fraud Examiners (CFEs) in more than 100 countries. CFEs were asked to report their firsthand knowledge of the single largest incident of occupational fraud in their company within the last two years. The findings, similar to those in previous reports and quite consistent across borders, illustrate that fraud continues to be a significant problem for companies around the world. Some of the weaknesses identified in the report help highlight strategies that companies could incorporate into their fraud protection practices.

Cost of Fraud

The most significant finding in the 2014 report is that the typical organization has an average estimated loss of 5% of revenues from fraud each year. This is the same as in the 2012 report and amounts to nearly $3.7 trillion if applied to the Gross World Product (GWP). The median loss in 2014 was $145,000, slightly higher than in 2012. More than 20% of the cases involved losses of at least $1 million.

Small and large entities are of particular interest, as they reported the largest fraud amounts: "The median losses for small businesses [defined as those with fewer than 100 employees] and the largest entities (those with more than 10,000 employees) were the highest, at $154,000 and $160,000, respectively." In addition, smaller businesses face different kinds of fraud risks than their larger counterparts. One possible cause is the presence of fewer control measures. Employees tampered with disbursement checks in 22% of small business cases but only about 7% in large organizations. Also, cash larceny and payroll theft occurred twice as often in small businesses as in larger ones.

Collusion was also a factor, enabling the circumvention of independent checks and balances as well as the evasion of other fraud control measures. The median loss from the work of a single person amounted to $80,000. When more individuals were involved, the amount increased dramatically: The median loss from two perpetrators was $200,000. It was $355,000 when there were three people involved, and it was more than $500,000 with four or more perpetrators.

The level of responsibility in the organization highly correlated with the amount of fraud loss. While owners or executives were involved in only 19% of the cases in the report, they caused a median loss of $500,000. On the other hand, other employees committed 42% of the cases but only caused a median loss of $75,000. Managers were ranked in the middle, causing 36% of the cases and a median loss of $130,000. About 77% of all frauds were committed by individuals from one of seven departments: accounting, operations, sales, executive/upper management, customer service, purchasing, and finance.

As in previous surveys, asset misappropriation is the most common type of occupational fraud. It was reported in 85% of this year's cases. It's also the least costly, with a median loss of $130,000. Financial statement fraud represented

only 9% of the cases but caused the largest financial impact with a median loss of more than $1 million. Various corruption schemes were middle ground in terms of frequency (37% of cases) and median loss ($200,000).

Fraud Detection

Over the years, fraud perpetrators have consistently displayed six behavioral red flags that can signal someone is a likely candidate to commit fraud: living beyond their means, having financial difficulties, having an unusually close association with a vendor or customer, control issues or unwillingness to share duties, having a "wheeler-dealer" attitude involving shrewd or unscrupulous behavior, and divorce or family problems. In addition, behavioral red flags not directly associated with fraud were displayed in 38% of the cases. The top-cited behavior in that category was bullying or intimidation, followed by an excessive absence from work. Finally, out of 1,000 responses to the question, only 25% reported that the perpetrator exhibited a red flag behavior associated with a topic related to human resources before or during the fraud—most commonly, a poor performance evaluation.

The *2014 Report to the Nations* suggests that performing background checks before hiring a candidate may not be effective in preventing occupational fraud: "The largest group of fraud perpetrators (41%) had been employed by their targets between one and five years before committing their crimes." Only a small amount of fraud perpetrators (5%) had ever been convicted of their crimes prior to the crime reported in the study, and a majority of these perpetrators (82%) had never been reprimanded by an employer for their misconduct.

The most frequent and consistently common successful fraud detection method continues to be inside information or tips from whistleblowers, with nearly half coming from employees and 14% from anonymous parties—possibly employees fearing retribution. More than 40% of all reported fraud cases were detected by a tip—more than twice the rate from any other detection method, including internal or external auditing combined. Since many tips do come from individuals other than employees, companies need to cultivate information from others, usually by informing them of the anonymous hotline. Performing external audits is the least effective method of fraud detection and was successful in only 3% of the cases—more fraud was detected by accident (7%). And internal auditing caught only 14% of the fraudsters.

For guidance in applying the *IMA Statement of Ethical Professional Practice* to your ethical dilemma, contact the IMA Ethics Helpline at (800) 245-1383 in the U.S. or Canada. In other countries, dial the AT&T USA Direct Access Number from www.usa.att.com/traveler/index.jsp, then the above number.

A hotline or other confidential mechanism to report wrongdoing was present in only 54% of cases, and whistleblowers were rewarded in less than 11% of them. Organizations having these reporting controls in place were much more likely to get a whistleblower's tip that led to successful uncovering and settlement of a fraud case. Also, frauds discovered in these organizations were 41% less costly and were detected 50% more quickly than in organizations without them. Earlier detection cuts off the fraudulent activity before it results in greater losses. According to the report, "Many organizations have room for improvement in encouraging the tips that so effectively help uncover fraudulent conduct."

The presence of other fraud controls also results in lower costs and earlier discovery. Some controls should be attractive to smaller businesses because they can be implemented with relatively little cost while greatly enhancing "small business' ability to protect their resources from fraud." These include adopting a code of conduct, implementing an anti-fraud policy, providing anti-fraud training, and enhancing management review of transaction information, account data, and processes. Only 35% of the victim organizations used proactive data monitoring and analysis, but the presence of this control correlates with fraud losses that were 60% lower and 50% shorter in duration. One-third of survey respondents cited lack of controls to prevent fraud as the principal cause of the loss.

continued on page 85

Ethics

continued from page 12

Increasing Fraud Reporting

Occupational fraud continues to pervade businesses around the world. This year's report shows that trends in wrongdoing are quite consistent over time and across borders. Since greater losses occur when a fraud scheme is allowed to continue, proactive and effective prevention and detection methods are critical. These include confidential reporting mechanisms, management review procedures, ongoing monitoring, and internal audits, including surprise audits. Although external audits are widely used as a governance process, they shouldn't be relied on as an organization's primary anti-fraud mechanism. Consider becoming alert to behavioral traits that may be warning signs, training your team to detect the signs of fraud, conducting internal fraud assessments, and creating a dedicated fraud team.

An analysis of global hotline contacts showed final quarter 2013 increases in both the number of fraud-related calls as well as a record high Fraud Index Percentage of more than 25% of total contacts. On May 29, 2014, The Network, Inc. and BDO Consulting announced results of their latest analysis of fraud reporting activity from almost 15 million employees around the world. According to Luis Ramos, CEO of The Network, "Fraud continues to be a huge risk in the workplace, and while it is concerning to see fraud growing as a percentage of all compliance issues, it's reassuring that these incidents are being caught and reported." Ramos described how companies are implementing new programs in order to "create a 'speak-up' culture" where employees know how to properly report wrongdoing when they see it and actually do so. Companies without these options, especially small businesses, would do well to consider developing a program that encourages employees and others to speak up when they witness fraudulent activity. **SF**

Curtis C. Verschoor, CMA, CPA, is the Emeritus Ledger & Quill Research Professor, School of Accountancy and MIS, and an honorary Senior Wicklander Research Fellow in the Institute for Business and Professional Ethics, both at DePaul University, Chicago. He also is a Research Scholar in the Center for Business Ethics at Bentley University, Waltham, Mass., and Chair of IMA's Ethics Committee He was selected by Trust Across America-Trust Around the World as one of the Top Thought Leaders in Trustworthy Business—2014. His e-mail address is curtisverschoor@sbcglobal.net.