

Six Excuses Organizations Use to Ignore Fraud Risk and Anti-Fraud Measures

By Marc Courey, Director of Litigation Support, Fraud and Forensic Services

December 2009

Fraud happens. It happens to organizations of all sizes and across every industry. It happens even to the best of organizations. And in almost every instance, organizations hit by occupational fraud say they never dreamed it would happen to them.

Thanks to research and reporting, we understand much about how fraud is committed and how it can be prevented and identified. Despite this, many organizations fail to implement proven anti-fraud measures like hotlines for the simple reason that they don't feel it's necessary.

Do any of these justifications against implementing a hotline or some other anti-fraud effort sound familiar?

"We trust our employees."

"Our employees have been with us a long time and would never do that; they're like family."

"We don't need a hotline; we have an open-door policy."

"Our nonprofit's mission in the community protects us from being targeted for fraud."

Professionals who work in the field of fraud deterrence and detection hear examples of this rationale far too often. Although the explanations sound great on the surface and typically come from well-meaning organizations, sadly, the "logic" is seriously flawed and ineffective at managing risk or preventing fraud.

Here are six frequently used justifications for not recognizing fraud risks and implementing sound risk management practices, and explanations as to why they represent misguided thinking.

"We're a small organization; we know all our employees." Small businesses are especially vulnerable to occupational fraud, according to the Association of Certified Fraud Examiners.¹ In its 2008 Report to the Nation, it stated the median loss suffered by organizations with fewer than 100 employees was \$200,000. This was higher than the median loss in any other category, including the largest organizations.

"We have an open-door policy; if employees suspect wrongdoing, they know they can talk directly to us." Trouble is, they won't and they don't. Confidentiality, more than any other factor, is the most vital aspect of a successful reporting program. Employees must be confident that their anonymity will be protected in order to report **suspected** ethical lapses or wrongdoing without fear of reprisal. This is demonstrated in that nearly half of all hotline calls happen outside normal business hours², long after the "open doors" are closed and locked.

"Our employees have been with us a long time; they would never do anything like that!" You may think you know your long-time employees based on their work history; however, you should know that the great majority of employees who commit fraud are generally first-time offenders. Only 7% of fraud perpetrators in the 2008 ACFE report had prior convictions. Over half of the fraudsters had been with their organization more than five years, and more than half of these had over 10 years of service with their organization.

Research also reveals that longer-term employees commit frauds resulting in much larger losses. These trusted employees have learned where the control weaknesses are and how to exploit them. In addition, fraud schemes frequently continue for years before they are ever detected. The median length of time a fraud went undetected was 24 months!³ Do you really know what your long-time employees are capable of and the potential risk?

"We mostly have a young work force, with employees who are eager to succeed; they wouldn't risk their careers with unethical behaviors." Brace yourself—a 2008 survey of nearly 30,000 teens across the country revealed entrenched habits of dishonesty, with stealing, lying, and cheating rates climbing to alarming rates.⁴ According to the survey's sponsor, "there's a hole in our moral ozone."

Despite the high levels of dishonesty, these same kids have high self-images when it comes to ethics. Almost 60 percent agreed that "successful people do what they have to do to win, even if others consider it cheating." A whopping 93 percent said they were satisfied with their personal ethics and character at the same time that 23 percent reported stealing from parents or relatives and 19 percent reported stealing from friends, all within the past year. Such news doesn't bode well for organizations as this generation moves into the work force.

"We trust our employees, especially our managers and those professionals we're grooming to be our next leaders." Trust is not a control. Sadly, most occupational frauds are committed by those in management positions. Moreover, the losses caused by fraud are directly related to the positions held by perpetrators—the higher the position, the greater the loss.⁵

And if you think filling your leadership pipeline with degreed professionals will shore up the integrity factor, be aware—recent studies have shown that cheating among graduate students is not only prevalent, it's also acceptable as peer behavior.⁶ In a survey of 54 colleges and universities in the U.S. and Canada, including 32

³ Ibid.

⁴ Josephson Institute's 2008 Report Card on the Ethics of American Youth.

⁵ 2008 Report to the Nation on Occupational Fraud & Abuse, Association of Certified Fraud Examiners, www.acfe.com.

⁶ McCabe, Donald L., Butterfield, Kenneth D., Teviño, Linda Klebe, "Academic Dishonesty in Graduate Business Programs: Prevalence, Causes, and Proposed Action," *Academy of Management Learning & Education*, 2006, Vol.5, No.3, 294-305

¹ 2008 Report to the Nation on Occupational Fraud & Abuse, Association of Certified Fraud Examiners, www.acfe.com.

² Ibid.

graduate business programs, 47 percent of all graduate students self-reported cheating or other questionable behavior within the past year, while 56 percent of the graduate business students admitted to engaging in cheating or other questionable behavior within the past year.⁷

“We don’t need a hotline; we already have controls in place to detect fraud.” Occupational frauds are more likely to be detected by tips than through any other means, including audits or other specific control procedures. In fact, 46 percent of fraud cases in the 2008 report were detected by tips from employees, customers, vendors, and other sources.⁸

No Excuses

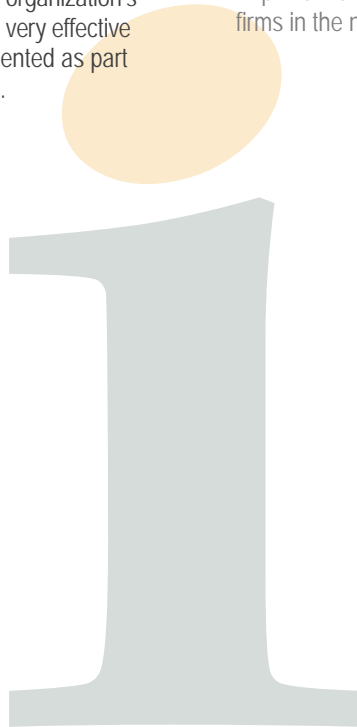
There’s really no good excuse for not implementing an anonymous hotline. Keep in mind, a hotline isn’t a definitive prevention program in and of itself, and it’s not as simple as setting up a phone number in the personnel department. It’s just one component of the organization’s commitment to ethical conduct, but it’s one which can be very effective and cost-efficient and that absolutely should be implemented as part of any successful enterprise risk management program.

About the Author

Marc Courey, CPA, JD, LLM, CFE, CICA, CFF, CCEP, is director of litigation support with Wipfli’s Fraud and Forensic Services group. He has conducted financial forensic investigations and fraud risk assessments, assisted public companies with Sarbanes-Oxley compliance requirements, and conducted regulatory compliance engagements and internal investigations disclosing fraud and resulting in regulatory enforcement action and referral for criminal prosecution. He also has significant experience with organizational formation and governance, including risk management, business ethics, and employment practices. Contact Marc at 952.548.3439, or e-mail him at mcourey@wipfli.com.

About Wipfli LLP

With more than 800 associates and 15 offices across the Midwest, Wipfli ranks among the largest accounting and business consulting firms in the nation. For more information, visit www.wipfli.com.



⁷ Ibid.

⁸ 2008 Report to the Nation on Occupational Fraud & Abuse, Association of Certified Fraud Examiners, www.acfe.com.