BNA, INC.

Prevention of Corporate Liability

CURRENT REPORT

 ISSN 1067-6104

FOCUS
Fraud Prevention

Simple Measures Help Smaller Firms Reduce Risk Efficiently

BY DAVID SUMNER
AND ANDREA FOX

Small and medium-sized businesses historically have been more vulnerable to asset misappropriation fraud than their larger counterparts. The economies of scale, as well as legislative requirements that include the Sarbanes-Oxley Act, enable these larger companies to implement sophisticated financial controls and dedicate internal personnel such as Internal Audit to periodically test the efficacy of these controls and to identify schemes proactively rather than reactively.

The Association for Certified Fraud Examiners' 2008 Report to the Nation on Occupational Fraud & Abuse finds that private companies were more often victims of fraud than public, government, and not-for-profit entities. Additionally, the median loss due to fraud for a private company was almost twice as much as a public company.

According to Anthony Vittone, vice president and general counsel of Swimways, a Virginia manufacturer of pool toys, ''Our business does not have the scale to implement many anti-fraud controls and procedures that are available to companies larger than us. We must rely on more basic procedures despite the fact that fraud can impact us much more than it would a larger company.''

Tips Often Uncover Fraud

Even though the small or medium-sized business often doesn't have the ability to have best-in-class anti-fraud controls, several procedures can be implemented that are cost-effective and proven to reduce the risk of fraud.

The ACFE report indicated that most frauds in its survey were unveiled upon the receipt of a tip. While many business owners prefer that employees bring their misgivings to someone in authority, in many instances these tips are received via a formal tip line.[1] These tip lines help to protect the tipster from repercussions regardless of whether their concern was a legitimate fraud or a misunderstanding of the facts.

While tip lines are effective in pointing the organization in the direction of potential fraudulent activity that has already occurred, they are not as effective at preventing fraud before it occurs.

Tip lines can be set up through third-party vendors and are usually structured based upon number of users. Pricing can be impacted by a myriad of factors, including the format of the tip line (i.e., web-based vs. live operators) and whether there are international employees.

While tip lines are effective in pointing the organization in the direction of potential fraudulent activity that has already occurred, they are not as effective at preventing fraud before it occurs. Large and small businesses alike can utilize tip lines, but the smaller business is at a distinct disadvantage due to its inability to institute preventative controls.

We have found that employees at smaller organizations are less likely to call an anonymous tip line as they feel their group is too small and, therefore, the source of their tip would be easily identifiable. If the perception of anonymity is reduced, that may negatively impact the effectiveness of the tip line. Several controls, targeting vulnerabilities specific to smaller companies, are relatively inexpensive to implement and can help reduce the risk of fraud.

These controls, several of which are outlined below, are focused in certain key areas (e.g., purchasing, cash management, expense cards) that are typically the most frequently used by fraudsters in companies of all sizes.

Vacations Can Fight Fraud

Mandatory vacation for all accounting personnel: The ability of perpetrators to cover their fraud scheme is usually dependant on their ability to control underlying documentation and not allow others to gain access to evidence of their wrongdoing from external parties such as banks. Ensuring that all personnel take vacation with a backup performing their functions not only makes it harder for the fraudster to maintain secrecy, but it also cross-trains other personnel so that legitimate absences will not affect your organization's operations.

It will require a small investment of up-front time to cross-train employees, but the benefits of having employees fill in seamlessly for others who are out of the office for any period of time should outweigh the costs of any inefficiency created during the training period. For example, your organization could develop a program requiring the rotation of roles for one week each quarter that may in turn also boost employee morale as they increase awareness of the

(continued on page 207)

[1] The 2009 PricewaterhouseCoopers Global Economic Crime Survey also indicates that informal and formal tips are the most common method of detecting fraud.

David Sumner is a director and Andrea Fox is a manager in the Forensic Services Advisory Practice at PricewaterhouseCoopers, Philadelphia. The views expressed are not necessarily those of PwC.

  BACM ISSN 1067-6104

(continued from page 208)

business operations and gain variety in their daily tasks. As an added benefit, employees may recognize efficiencies to be gained in their shared function by observing them in someone else's routine.

Secondary approvals for large dollar disbursements: We have seen this very basic control limit the size and scope of disbursement schemes in many instances. Even when perpetrators have found weaknesses in the system, limiting their ability to transfer larger dollar amounts can help to reduce the impact of the fraud. Once approval limits are set and the procedure has been implemented successfully, extra attention should be paid to transactions just under the threshold limit or when multiple transactions under the threshold are made to the same vendor in order to bypass approval. The small business owner should also periodically review disbursements. Not only would this review deter fraud, but a greater understanding of expenses can be gained.

Periodic review of the vendor list: Most basic accounting systems can provide a summary report of vendors with their annual or year-to-date spend. A simple review of this list can identify anomalies that are related to fraud. We have seen dishonest employees utilize methods such as changing one letter in a vendor's name or reversing two words in a vendor's name such that the same vendor is in the listing multiple times. With multiple vendor listings, the dishonest employee is able to spread expenses over both accounts, making it appear that the vendor has less expenditure than is actually the case. Alternatively, the dishonest employee could change the address on one of the vendor listings to his own post office box, allowing payments to occur to a seemingly legitimate vendor. Review of the vendor listing may also help to identify cost-saving opportunities.

Issue credit cards in the employee's name instead of company: We have investigated several expense fraud schemes where employees used their corporate credit card for personal gain. When the employee is required to request reimbursement because the corporate card is issued in his name, the employee is much less apt to inflate expense amounts or purchase items for personal use as the employee is required to document business purpose prior to reimbursement. This requirement also serves to reduce those expenses that are ''gray'' as employees are less willing to push the expense policy.

Maintain a lock box: Utilizing a lock box for customer deposits is an excellent way to ensure that all funds are deposited in your organization's bank accounts; however, the cost of using this service may not be an option for a small organization. At a minimum, the small business owner should ensure appropriate segregation of duties exist around cash receipts such that the accounts receivable clerk is separate from the employee who receives checks and deposits them in the company's bank accounts.

We have found that a poor tone at the top of the organization may lead to inappropriate actions by the staff.

Monitor access to bank accounts and investments: Periodically review which employees have access to the company's bank accounts and their signatory limits. By minimizing the number of employees with access and ensuring that terminated employees are removed promptly from the bank's listing of approved signatories, you reduce the risk of inappropriate access to your organization's funds.

Restrict access to check stock: Keeping check stock behind a locked door with limited accessibility or in a safe can help deter a dishonest employee from utilizing your company's checks for personal use.

Performing many of these functions overtly can also serve to deter fraud as employees know that the owners are watching. The reviews shouldn't be performed in a predictable fashion as this can be taken advantage of in the same manner as if there was no review at all.

In most of the frauds that we have investigated, regardless of the scheme, the perpetrators were trusted by the individuals from whom they were stealing. This trust enabled the fraudster to get away with inadequate documentation and explanations and/or provided an ability to override controls in place. Unfortunately, it usually takes an instance of fraud to shake the smaller business owner from this trusting relationship with his employees, who in many instances are related to the owner. A little bit of skepticism has minimal cost and can provide great rewards.

We have found that a poor tone at the top of the organization may lead to inappropriate actions by the staff. For example, with increasing pressure to meet budgeted numbers, an employee may look for a way to mask the company's financial shortcomings in order to avoid the wrath of his superior. Alternatively, an employee may feel uncomfortable questioning instructions given to him by a boss even when he knows they are inappropriate. Maintaining an environment where an employee is comfortable raising questions and does not live in fear of infuriating his supervisors or losing his job is critical to the success of an organization.

Do Detective Work

The small business owner also should consider having some detective controls in place, such as holding oversight meetings. On a periodic basis, a group of qualified individuals with the appropriate level of industry-specific expertise should meet to review your company's financial statements. We have found that a simple comparison of budget to actual numbers with consideration given to the current operations of the company can help identify any anomalies.

Additionally, financial statements should be compiled in-house and an independent third party should audit or review the statements. Once the audit/review is complete, the financial statements should be provided by the third party directly to the board of directors or other designated committee, such as an audit committee or alternatively to the owner of a small business. This avoids giving the dishonest employee an opportunity to make any changes to the statements.

While few smaller companies have the funding or the resources available to develop a sophisticated, best-in-class controls environment, we recommend consideration of the above suggestions as cost-effective and simple measures to help prevent and reduce the risk of fraud. Many of these suggestions require minimal effort and will help smaller companies begin the critical process of effective fraud prevention within the organization.