

Be committed to reducing your risk of theft by creating controls that might prevent it!

- ☑ ***Conduct background checks on prospective personnel.*** Many companies document internal controls with spreadsheets. This process isn't very secure and can quickly become cumbersome. Put the information underlying the documentation into a database instead to enhance consistency, security and search efficiency.
- ☑ ***Thoroughly check references and scrutinize all dates and time gaps in resumes.*** Have employees bonded if they have access to cash or work in financial functions.
- ☑ ***Send bank and credit card statements straight to the top.*** The company's owner, manager or a nonprofit audit committee member should be the first to review all bank account entries and canceled checks. Someone without authority to issue checks should reconcile bank statements and review them for forged or altered checks. Before paying credit card bills, support each charge with an original receipt.
- ☑ ***Review documentation for all check requests.*** Compare original vendor invoices, purchase orders and receiving reports for agreement on quantities, brands, product descriptions and services requested. All should be stamped "paid" and marked with the related check number.
- ☑ ***Monitor cash receipts and deposits independently of employees recording them.*** Have someone not involved in making deposits or recording accounts receivable open the mail, count money received and report totals to the owner-manager or other official who compares the reported amount to the amount deposited.
- ☑ ***Reconcile accounts receivable and accounts payable monthly.*** Have the owner, manager or nonprofit audit committee member review and clear all exceptions.
- ☑ ***Check out first-time vendors.*** Someone independent of buying and payment processing should review all entries for new suppliers. That person should call to verify the supplier's name, address and federal tax identification number.
- ☑ ***Restrict authorization and access to finances.*** Ensure that only appropriate employees can make transactions or have access to assets, documents and records. Password-protect computer files and set dollar limits on check authorization. Other safeguards include dual custody of cash receipts or cash on hand and ensuring cash and financial documents are secure.
- ☑ ***Make employees take vacations.*** Especially require personnel in accounting, human resources and cash-handling functions to take one to two weeks off each year, preferably at the end of an accounting cycle. Cross-train employees so that someone else can do their job—and double-check their work—during the vacation.
- ☑ ***Watch for red flags in employee behavior.*** They can include substance abuse, gambling, change in lifestyle, extramarital affairs, living beyond one's means, possessiveness of work, high personal debts, high medical bills, peer pressures or simply dissatisfaction with work.

Original Source: Leon A. LaRosa Jr., CPA, managing partner and chairman of litigation support services at Social Gerstein, LLC in Jenkintown, PA. He also is an adjunct professor and director of The Institute of Fraud and Forensic Accounting at La Salle University in Philadelphia.

This document is to be used for discussion purposes only and is not intended to be an authoritative source.