Segregate Accounts Receivable Duties to Prevent Employee-Fraud Losses

Fraud continues to be a major financial drain on U.S. companies, and employees are a major perpetrator, according to recent industry studies. But the good news is that banks offer treasury management services that can assist with employee-fraud prevention.

In KPMG’s Fraud Survey 2003, 75% of companies reported experiencing fraud in the past year, up 13% from its 1998 fraud survey. Both KPMG and the Association of Certified Fraud Examiners (ACFE) agree that the majority of business fraud is committed by employees. Some 60% of fraud in the KPMG study was employee fraud, while the figure was 64% in a 2004 ACFE study.

Protect your receivables

One form of fraud that companies sometimes overlook is receivables fraud. “Companies generally understand that they have payables risk,” says Shawn Christian, a St. Louis-based Treasury Management Sales Team Leader for U.S. Bank. “They understand the need to use Positive Pay and ACH blocks and filters to protect their payables. But sometimes they let their guard down when it comes to protecting receivables.”

A critical fraud-prevention strategy is segregation of duties. In receivables, that means not letting employees have access to both receivables payments and the accounts receivable (A/R) system. Unfortunately, Mr. Christian notes, due to economic circumstances many companies have reduced their A/R staffs to one or two individuals and no longer maintain segregation of duties. “This creates a tremendous opportunity for someone to misappropriate funds,” he says.

A typical example: A customer remits a $500 check to your office to pay down a $1,000 debt. An accounting clerk with access to the A/R system writes off the $500 as part of a negotiation with the customer and then deposits the check into his or her own personal account. The money is stolen but neither the company nor the customer has any reason to investigate.

Lockbox as a solution

A treasury manager can ensure segregation of duties—and help prevent such receivables fraud—by using a lockbox service. When customers remit to your lockbox, their checks go directly to the bank, which deposits them into your company’s account. Your employees never have access to the payments.

Your bank can also help you fight receivables fraud by providing an automatic download of your account reconciliation data. That way you or your internal auditor don’t have to rely on paper bank statements.
submitted by employees, which may be intercepted or forged.

**Additional mitigation measures**
There are many other measures that companies can take to combat employee fraud. Here's a list of suggested steps from consultant Claudia Volk (CJVolk Associates, Inc.), who spoke on this topic at the 2004 Association for Financial Professionals Conference in November:

- Strengthen internal controls
- Establish employee hotlines
- Conduct periodic compliance audits
- Designate compliance personnel
- Establish a code of conduct
- Conduct background checks for finance personnel (ask for annual financial statements)
- Institute fraud awareness training
- Tie ethics objectives to employee evaluations

The most cost-effective way to deal with employee fraud is to prevent it, the ACFE says. Its study revealed that the median recovery among victim organizations was only 20% of the original loss, and almost 40% of victims recovered nothing.

To learn more about preventing employee fraud, contact your U.S. Bank Treasury Management Sales Consultant or Relationship Manager.