



Managing Fraud Risk in Your Business

By Jim Vogt
Manager of Vectra Bank's Treasury Management Department

With the economy in the doldrums, and technology growing ever smarter, businesses are at risk for fraud from internal or external sources. Companies should consider turning to their banker to help plug security holes where dollars might be smuggled out of a business.

All businesses have exposure to fraud risk. According to the Association for Finance Professionals, in 2007, 71 percent of businesses were victims of actual or attempted payments fraud. What does this mean in real numbers? A study by the Association of Certified Fraud Examiners (ACFE) estimated that U.S. organizations lose 7 percent of their annual revenues to fraud. Applied to the projected 2008 United States Gross Domestic Product, that figure translates to approximately \$994 billion in fraud losses.

The question is, when will it happen to you? And will you be ready to stanch the flow of fraudulent dollars from your business?

Banks, and specifically Treasury Management departments, frequently have programs in place to help protect businesses from payments fraud:

- **Positive pay** - Check fraud comprised 94 percent of the fraud attempts mentioned above. Positive pay tracks the payees and amounts of issued checks. As checks clear, the bank reports any discrepancies to the business. Positive pay protects companies from losses from fraudulent checks. It also provides early warning of a possible problem with altered, stolen or counterfeit checks.
- **Avoiding ACH fraud** - A positive pay-like filter can help businesses avoid fraudulent or unauthorized electronic debits against their accounts.
- **Online account management** - Online treasury management tools can be designed specifically to assist businesses with internal controls, such as setting authorizations for certain transactions. For

example, attempts at fraudulent wire transfers by phone or fax are common. Experienced bankers help customers establish controls and approvals to order online wire transfers. This policy can eliminate some exposure to bogus wire transfers.

- **Lockbox services** - The service isn't new, but its relevance in fraud prevention is growing. A lockbox allows businesses to accept payments directly via a bank "lockbox" at the post office rather than by mail at their business location. Payments that don't come in to a business are never available for internal theft. Today, more businesses use a lockbox as an audit control and fraud prevention mechanism.
- **Account reconciliation services** - Simply reconciling account activity promptly can limit fraud risk. Most banks can provide reports that assist in the account reconciliation process. The more diligently a business performs these reconciliations and reports any exceptions to its bank, the more easily it can limit problems.

In contrast to external fraud, which may be somewhat random, internal or occupational fraud occurs when the "fraud triangle" of three components is present. The individual who commits fraud must perceive some sort of pressure; have an opportunity (such as access to accounts); and rationalize the fraud -- for instance, intending to borrow and then repay money to pay a big medical bill. In economically difficult times, the pressure component builds, and often we see an uptick in fraud. People who are faced with more difficult situations do things they normally wouldn't.

Occupational fraud schemes tend to be extremely costly, with a median loss in the ACFE study above of \$175,000. More than one-quarter of the frauds involved losses of at least \$1 million. And occupational fraud can continue for years before it is detected. The typical fraud in the ACFE study lasted two years from the time it began until the time it was caught by the victim organization.

A banker who has specific fraud prevention expertise can counsel a business to reduce risk of internal fraud by taking these steps:

- **Separate duties** - Dividing responsibilities closes loopholes to fraud. The employee responsible for accounts payable should not be responsible for reconciling accounts; the worker handling deposits should not manage disbursements.

- **Internal controls** - Appropriate checks and balances ensure finances are well managed. Many businesses, particularly small businesses, give a trusted employee too much control.
- **Know your employees** - Internal fraud is almost always executed by a first-time offender. A longtime employee might face extensive medical bills or be under other pressures that drive them to consider crime.

A business without appropriate controls in place presents an opportunity for an employee to commit fraud. Fraud harms a business's bottom line and its reputation, and it disrupts internal operations. Ask your bank business partner for help in taking the offensive to protect your business against this dangerous deception.

###

Jim Vogt is Treasury Management & Merchant Services Manager for Vectra Bank Colorado. He received a Master of Science degree in Economic Crime Management and is a Certified Fraud Examiner. With assets of \$2.78 billion, Vectra Bank Colorado is a proactive, customer-focused organization dedicated to real relationship banking. Part of the Zions Bancorporation family of banks, Vectra serves Colorado's small, middle-market and corporate business clients with 42 locations throughout Colorado, and one in Farmington, N.M.