

Technology contributes to growth of fraud

By CHRISTOPHER A. GALLO

Technology is helping more crooks commit fraud more easily and with more success against the companies they work for, and also individuals.

Because of these technological advances, fraud may now be America's No. 1 crime, and is only becoming more prevalent. Fraud has quickly become "the" crime of the future.

Furthermore, with law enforcement authorities focusing more on violent crime, they are often not interested in prosecuting fraud unless the amount of money involved is very large.

A 2006 Association of Certified Fraud Examiners report on occupational fraud and abuse showed that eight in 10 small businesses were the victims of some form of employee theft, with the median loss for those companies totaling nearly \$200,000.

The technology of fraud that has sparked this crime wave consists of: the Internet, color copiers and scanners, credit card devices, ATMs and electronic payments. And these advances in fraud have led to such crimes as phony check scams, identity theft, "ghost" or fictitious employees and false insurance or medical claims.

Consider that in the past it typically took hours for a thief to reproduce a fake check. Today, with color scanners, a skilled thief can produce a bogus check in minutes that defies detection.

The 2006 ACFE report showed less than 8 percent of people who commit fraud were convicted. The truth is many companies are too embarrassed to report fraud, which limits the number of convictions.

The most common forms of fraud in business are manipulating checks, skimming revenue, especially inventory and cash, and paying invoices for fraudulent services. The most common type of fraud committed against individuals is identity theft.

Check and electronic payment fraud accounts for the greatest loss of money for businesses, which is understandable since there were more than 90 billion checks and

electronic payments processed by banks in 2006. In 2000, check fraud exceeded \$20 billion a year, and less than 2 percent of employees were caught and only a fraction of the stolen money was recovered.

The key to curbing fraud in business or personally is prevention. In the business landscape, trust has its limitations. Owners and managers need to tighten up their processes in place.

Ironically, red flags are often detectable, if management is alert and knows what to look for. Fraud usually occurs because of the lack of internal controls over:

- processing of vendor payments and receipts from customers;
- receiving, shipping and billing processes;
- poor security over inventory and tools; and
- lax inventory procedures.

When internal controls are lax, employees can be extremely creative in committing fraud for personal gain. Fraud can come in many forms — kickbacks, fake orders, vendor payments to post office boxes, purchasing excessive inventory to resell. It isn't just about stealing cash and checks.

Studies show that the typical profile of an employee who commits fraud is not what you might expect. Employee theft tends to be committed by longtime, trusted workers who have minimal supervision. It typically happens more than once and usually during business hours.

Individuals also need to be vigilant against fraud. The most prevalent now is identity theft. Through the Internet, scammers can uncover a great deal of information about people.

Perhaps the biggest danger comes from inadvertently handing out your Social Security number. Once a thief has access to that critical form of identity, he can open the door to other personal information, and provide access to credit cards and banking information.

Additionally, closely monitoring your back account or credit card statement can reveal inexplicable charges. Thieves are smart, and tend to charge small amounts to avoid detection. Remember that a \$10 charge fraudulently made to thousands of unaware individuals can add up to a large payday.

Reconcile your bank statements within 30 days — the legal limit to report fraud to a bank. The same thing for credit cards — don't forget to review your credit card statement each month for charges that you didn't make.

To avoid check fraud, avoid writing abbreviations on the "Pay To" line of a check. For instance, a check made out to the IRS can easily be manipulated to read MRS, then the thief adds a phony name and cashes the check.

In addition, both business owners and individuals should be careful with blank checks. Often, checks are easily accessible and kept in a desk drawer. Someone can steal a check from the bottom of the pile, making it difficult to detect until the cash is gone.

If you put a stop payment on a check, be aware that it is usually only in effect for 180 days. A thief could be aware of this and hold the check beyond the six-month period before cashing. For an additional fee, it's a good practice to put a 999-day stop payment; it's unlikely someone would hold onto a stolen check for almost three years.

Other scams that individuals should be wary of are:

- e-mails that say you've won an international sweepstakes, inherited a fortune, or that ask you to provide or confirm personal information;
- accepting a check for more than the amount due, then giving the difference back to the scammer;
- wiring money to people you don't know.

Employee theft and individual fraud schemes are soaring and technology is contributing to it. Business owners and individuals need to be aware of the threat. Fraud can be costly, ruining a business or draining an individual's bank account.

Christopher A. Gallo is a principal of Nishball, Carp, Niedermeier, Pacowta & Co with offices in Shelton and Waterbury. Gallo is director of the firm's Manufacturing Industry Services Group, and is a member and past president of the CPA Manufacturing Services Association. He also chairs the manufacturing committee of BKR International, a worldwide association of independent accounting, taxation and business advisers.