



### **Fraud: Is It Getting Easier to Hide?**

Computers have done great things for business efficiency. Unfortunately, they've also done great things for criminal efficiency. The Association of Fraud Examiners estimates that the average loss associated with computer-related fraud is \$1.9 million, and that number continues to increase every year.

As CPAs and business valuation experts, we want to help our clients protect their assets and preserve the value of their companies. Obviously, every dollar lost to fraud impacts the value of a business. Robbing a bank nets only as much as the thief's arms can carry. Manipulating computer records, deleting transactions and falsifying electronic signatures offers much more lucrative results.

Most fraud schemes run an average of 18 months, and the initial detection typically comes from a tip from an employee, customer, vendor or anonymous source. So the most effective measure to prevent fraud is strong internal controls — written, enforced policies and procedures; random reviews; changes of procedures; external evaluations and verification. But even with these safeguards in place, fraud still occurs.

## Use Computers to Uncover Computer Fraud

Most CPAs and valuation experts are not computer experts, but there are certainly ways to ferret out fraud using digital evidence. While every transaction can't be analyzed individually, data mining software and sample transactional analysis can quickly uncover patterns that indicate fraud.

Using software to discover fraud offers substantial advantages over manually analyzing records. Software can analyze an unlimited amount of data, and can efficiently compare data from disparate sources.

Plus, electronic sampling can occur frequently, which means that patterns are discovered more quickly — maybe before too much damage is done.

The biggest issue often is where to start. As with any question of fraud, the focus of the investigation should be on the weak points in the company's internal controls. Where are overrides common? Are "miscellaneous" codes or categories overused? Are amounts just below certain control thresholds showing up with frequency?

## What To Do If Fraud Is Discovered

If you suspect fraud, you should take several steps quickly. First, notify your insurance company and legal counsel. In some cases, failure to notify the insurance company can void the policy. At the same time, protect all digital evidence.

## Popular Scams

- **Check Fraud**
  - Kiting
  - Raising
  - Forgery
  - Altered Payee
  - Pay and Return
- **Accounts Payable**
  - Fictitious Payee
  - Bid Rigging
  - Kickbacks
- **Accounts Receivable**
  - Lapping
- **Expense Accounts**
  - Travel & Entertainment
  - Supplies
  - Seminars
- **Inventory**
  - Overstatement
  - Quality Substitution
  - False Weights & Measurements
  - Short Shipments
- **Payroll**
  - Ghost Employees

Your company's information technology department should have a policy in place regarding protection of evidence and steps to take when a request is made. (If it doesn't, now's a good time to create this policy!)

At some point early on, you must decide how to deal with the perpetrator. While it is imperative to move quickly to stop any damage, often the "correct" timing and course of action regarding the alleged perpetrator are unclear. Companies frequently keep the suspected employee on during the investigation stage. Legal advice regarding the rights and responsibilities of both the employee and the employer is especially important in cases of suspected fraud.

Unless there's a trained fraud team in-house, your company should not investigate its own suspected fraud. Without the benefit of specific fraud expertise, it is easy to make mistakes that can open the door to legal problems later on.

*We want to help you preserve the value of your company. Please contact our office if you are concerned about computer-based fraud.*