

Recognizing the Red Flags of Fraud

by Donna Davis, Director, ES Ethics

According to the U.S. Chamber of Commerce, fraud costs American corporations more than \$40 billion a year. Although we believe it can't happen at our company, any lapse in procedures may create opportunity for fraud to occur.

What Is Fraud?

Fraud involves deliberate deception or misrepresentation for personal gain. Fraud can be difficult to detect because it often involves small amounts of money or goods, stolen or misappropriated occasionally over a long time period. The person committing fraud will, of course, take steps to avoid being caught, and may stop at the first sign of suspicion, making the deception even harder to spot.

The most blatant type of fraud involves the actual physical theft of cash, checks, inventory or other property. Obviously, areas such as finance and accounting are most vulnerable to fraud, since there is more access to assets. However, these areas are subject to strict controls. Therefore, other areas of the company where rules are less stringent may be more vulnerable to fraud. Remember also that cash does not always imply access to a "cash register"—cash may be available through receivables, overpaid payables, conversion of other assets and even inflated amounts on expense reports.

How Does it Happen?

Most employees are honest people who would never consider stealing. It's hard for most of us to even imagine how to "pull off" a fraudulent scheme, or how to spot one in the making. The more we understand the type of fraud schemes that have worked in the past, the more able we are to prevent them in the future. Some of the most common fraudulent activities reported within industry include:

- Making sales or purchases at unauthorized rates (in return for gifts, gratuities or kickbacks), or dealing with "bogus" customers or suppliers. This can't happen when we use authorized price lists and credit approval procedures. New customers, vendors or suppliers should always be given special scrutiny.
- Improper access to computers, to acquire information, passwords or account data that is then sold or otherwise misused. Sensitive data is password protected. You are responsible for changing your password regularly. Remember to never share or post a password.
- Shipping products or services without billing. Another twist on this is purchasing items for the company but having them shipped elsewhere, or writing off company property and taking it for personal use. Prevention measures include proper handling of documents, including reconciliation to incoming or outgoing goods, and checking materials as they are shipped or received. This is also why it's necessary to separate functions such as billing and shipping, or purchasing and receiving.

- Falsifying expenses or petty cash disbursements. Proper review of check or cash requests, with accompanying receipts as required, is the best prevention.

Warning Signs of Fraud

Most businesses today, including ours, have safeguards and procedures in place that make it difficult to commit fraud: authorization requirements for credit or sales, cross-checking of transactions and controlled access to assets such as goods or cash. But reported cases of fraud share some similar characteristics that help us understand how they occurred:

- Procedures were not scrutinized and followed;
- Supervision or cross-checks were lax;
- Too much approval authority was given to a single function or individual; and
- Open communication, enabling inquiries and reports of suspected fraud, was not encouraged by the organization.



What You Can Do

Simply put, no individual should be able to improperly appropriate assets or record a transaction without being discovered. All employees can play a part in preventing fraud:

1. Be sure you fully understand and observe procedures and controls for authorizing transactions.
2. If you are assigned to approve a transaction, be sure to thoroughly review it. Don't automatically "rubber stamp" it no matter who sent it through.
3. Provide a truthful and accurate record of all transactions. Be sure all authorized transactions record the correct amount, date and assigned account. Of course, you should also be certain that all recorded transactions are within scope of the statement of work, have actually occurred and are recorded truthfully.
4. Safeguard access to assets. This includes both physical access (controlling storage and security), as well as access to information.

5. Cooperate with efforts that ensure accountability, such as regular audits and cross-checks of records and documentation. These checks help ensure that fraud, if committed, is quickly detected and corrected.
6. If you notice a procedure that opens the opportunity for fraud, or if you suspect fraudulent behavior, report it immediately to management or the ethics OpenLine (1-800-247-4952). Northrop Grumman ensures no reprisal for good faith calls, and calls may also be made anonymously.

Prevention of fraud is up to everyone. Be diligent about following the procedures put in place to prevent fraud, and report any areas where you note potential problems. These actions will help us see the "red flags" of fraud before extensive damage or costs are incurred.

I've made contact with a new distributor who can get our company a great deal on parts needed for manufacturing—if we move fast. I know my supervisor will insist on putting the distributor through a bunch of paperwork and security checks that will take too long to complete. I don't want the company to lose the deal, so I'd like to push the purchase through with approval, and just explain it later.

The approval process for working with distributors and suppliers is designed to protect the company, and you, from improper or fraudulent activities. The procedures ensure that the distributor is legitimate, that the price paid for goods is fair and that our relationship is based on good business practices. Talk to your supervisor to see if there is a way to expedite the proper approvals, but don't just plan to skip them altogether. If you do, you're putting yourself and the company at risk.

Our timesheet process is a big waste of time. We have to record our hours by project and get a signature on everything. Why can't the company just trust us?

The company trusts you to report your time honestly, but there is still good reason to follow a strict process. Payroll and taxes are critical in our financial reporting, so it's important that they be accurate. Tracking time by project ensures that our customers are properly billed. Getting a sign-off is a standard procedure to make sure that everyone is fairly paid for hours worked.

A co-worker of mine refuses to take time off. He's a hard worker, and he says he'd rather have the vacation pay than the vacation. Our boss says he has to take vacation or risk disciplinary action. What sense does this make?

A lot! Although it may seem that someone who never takes time off is extremely loyal, it's also possible that their reluctance to be absent is part of a plan to cover up fraudulent activities. Most banks and financial institutions require certain personnel to take vacation because fraud can often be detected simply by having someone else take over a person's duties for a few days. Chances are good that your co-worker is sincere and has nothing to hide, and in that case, he can enjoy some time off.