The Fraud Drain
How to Deter and Detect Internal and External Fraud

Executive Summary with Greg Miles, Regions Senior Vice President, Head of Treasury Management Products and Services

While larger organizations are the target of attempted fraud more often than smaller ones, no organization is immune.

According to a recent study by the Association for Financial Professionals, 61 percent of organizations experienced attempted or actual fraud in 2012. And while check fraud continues to be the dominant payment form targeted by fraudsters, cyber attacks are on the rise.

Greg Miles, senior vice president and manager of treasury management product development at Regions Financial Corp., says the typical loss from a fraud event is $20,300.

“Companies that view fraud protection and mitigation as a sideline function instead of as a primary business function are taking a huge risk,” he says. “A one-time fraud event involving something like a wire transfer can put a company out of business.”

Miles recently shared his ideas on how to deter, detect and mitigate both internal and external fraud risks.

What are the biggest areas of fraud?

Cyber fraud grabs headlines, but in reality, the most prevalent form of fraud is internal. The sources of internal fraud manifest themselves in forged checks, misapplied payments and embezzlement. Old-fashioned checks continue to be involved in 87 percent of reported fraud incidents, and bookkeeper fraud, in which a trusted employee perpetuates the fraud, accounts for as much as 85 percent of all fraud activity.

What are the warnings signs?

Internally, employees living beyond their means or those with obvious financial difficulties can be red flags. And if an employee has something less than an arm’s-length relationship with a vendor or a supplier, that could be an indicator.

Externally, the warning signs can be subtle, such as an increase in the amount of spam, excessive pop-ups, unusual links or slowness when trying to access the Internet. Additionally, if your customers who interact with your company electronically report

they had to log in twice, that second login request is a major red flag. Anything out of the ordinary with respect to accessing your website or interacting with you electronically can be a sign that malicious software is present.

How can companies reduce risk?

Look at controls and implement systems such as rotating duties, maintaining dual control, and conducting regular and surprise audits. In addition, regularly check bank account records, look at the amount and volume of checks being written, and move checks to electronic channels.

What steps should be taken when fraud is suspected?

Contact your bank immediately. The banker will recommend documenting everything related to what you believe has happened, reviewing account reconcilements, audit logs, bank records and transaction journals, and looking at computers and hard drives. If you're in a network environment, you can look at the network folders that could provide a record of what has taken place.

If the fraud is external, the physical computer that may have been infected with malicious software can be the source of significant amounts of forensic evidence. Your banker can facilitate having that examined.

If the fraud is traced to an employee, then that person's access to critical systems should be suspended until you sort things out.

How can leaders set the tone that fraud will not be tolerated?

Create a strong, controlled accountability structure with checks and balances and rotation of duties, and encourage team members to report suspected fraud. A tip line or anonymous email address can help facilitate their willingness to do so and can be one of the best ways to identify fraud.

How can technology help identify or prevent fraud?

Banks are offering products such as Positive Pay services and account reconciliation, and increasing controls around entitlements, in which dual control practices are encouraged.

To limit exposure to cyber fraud, companies should not overlook incorporating firewalls, virus protection, malware protection and anti-spam software. In addition, services can help reduce the impact of the distributed denial of service attacks that are becoming more prevalent.