



## THE DIVERSITY OF FRAUD

Recent news stories highlight the challenges of fraud deterrence facing organizations today; companies are constantly besieged by both high-tech and low-tech challenges, each with their own potential pitfalls. Organizations need to be diligent to these threats to ensure their risk is mitigated; a strategy of continuous monitoring, education, and improvement in fraud deterrence activities is the best course of action.

On the high-tech front, two doctors must pay more than \$500,000 to Medicaid and private insurers after billing for free vaccines. The culprit, according to the doctors, was outdated software on a computer system used to perform billing for patient services. The computer glitch meant the practice had fraudulently billed for vaccines provided under a Connecticut program that paid for the vaccine. According to the doctors the archaic billing system was set up in 1994, three years before the over-billing started and before they owned the practice. Still, the excuse of a computer glitch was not sufficient to avoid the double-damage penalty imposed by Medicaid for submitting false claims. Apparently the practice had not performed an analysis of their billing system including identification of standard processing procedures for some time.

An example of a simple, low-tech scam was recently revealed at Wal-Mart. The perpetrators, two Tennessee couples, scanned and duplicated bar codes from low price items, and surreptitiously placed them over the correct bar codes in the store. The cashier, unaware of the switch, scanned the lower price. An accomplice then would return the items to the store and receive store gift cards, which were then resold at a discounted rate. The thieves nabbed \$1.5 million over 19 states. Analysts noted that this scam was partially enabled by a key Wal-Mart objective: to keep the line moving. The cashiers were, for the most part, following their instructions.

Both of these examples highlight the need to educate all members of an organization about the importance of solid business processes and appropriate internal controls, procedures defined to reduce the risk of processing errors, including errors caused by fraud. Also, organizations should be aware of objectives or instructions given to employees that might additionally create fraud risk for the organization.

Given the diversity of threats, organizations cannot attempt to react to every identified error and correct the problem once incurred. Organizations should view process improvement and fraud deterrence as a continuous journey, involving all individuals and business processes. Such an approach should be integrated with their other organizational improvement initiatives, and executed as a consistent approach.

Below are a few suggestions to get you thinking about a culture of fraud deterrence in your organization:

- Examine your organizational objectives and ensure that processes are aligned with those objectives
- Develop methods to proactively evaluate internal control structures and identify potential improvements
- Be aware of ad-hoc changes or "workarounds" to any standard processing procedures that could introduce risk into the process
- Continuously reiterate to all employees the need to be aware of potential fraudulent activities