


Audits and hotlines stack up as the best crime busters in a new ACFE study.

Small Business, Big Losses

BY JOSEPH T. WELLS

ccupational fraud has become—at least so far—the crime of the 21st century. It is a widespread phenomenon that affects practically every organization. The frauds in the *2004 Report to the Nation on Occupational Fraud and Abuse*, from the Association of Certified Fraud Examiners, caused over \$761 million in total losses, with a disproportionate percentage committed against small businesses—almost half of the frauds in the study took place in businesses with fewer than 100 employees. Not surprisingly such businesses are less likely to be audited or employ antifraud measures than the larger ones.

The *2004 Report to the Nation on Occupational Fraud and Abuse*, from the Association of Certified Fraud Examiners, can be downloaded at www.cfenet.com.

Several broad conclusions can be drawn from the 2004 report. First, though the losses have been stable over the years, the fact that in one year alone they are approaching \$660 billion is cause for concern. Dishonest executives and employees are plying essentially the same schemes with the same results. Second, although large financial statement frauds receive the most attention, they are relatively uncommon compared to asset misappropriations and corruption. Third, small businesses remain the most vulnerable to occupational fraud because of three factors: They are the least likely to have an audit, a hotline or adequate internal controls. Fourth, audits—both internal and external—although excellent prevention devices are not the most effective means of detecting frauds. Fifth, hotlines and other reporting mechanisms are a vital part of any organization's prevention efforts but should go beyond employees to vendors and

customers, too. Finally, occupational fraud cannot be eliminated but organizations that use both hotlines and auditors can greatly reduce these costly crimes.

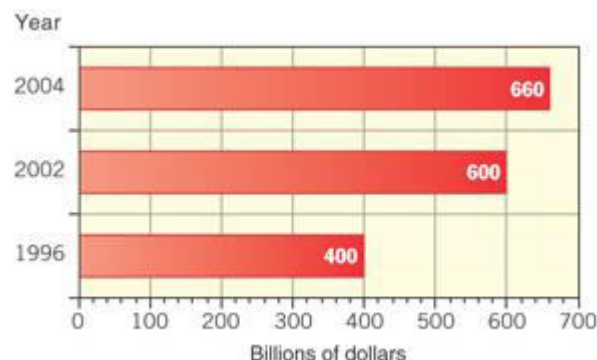
Occupational fraud schemes can be as simple as pilferage of company supplies or as complex as sophisticated financial statement frauds. This article summarizes some of the key findings of certified fraud examiners (CFEs) in cases they investigated. Internal and external auditors and CPAs advising small business clients will learn of the most effective antifraud measures.

MEASURING THE COST OF FRAUD

Determining the true cost of occupational fraud is an impossible task. Because fraud is a crime based on concealment, organizations often do not know when they are being victimized. Many frauds never are detected or are caught only after they have gone on for several years. Many of those are never reported or prosecuted. In fact, there is no agency or organization that is specifically charged with gathering comprehensive fraud-related information. All of these factors combine to make any estimate of the total cost of occupational fraud just that—an estimate.

The study asked CFEs to give their best estimate of the percentage of revenues a typical organization in the United States loses in a year as a result of occupational fraud. The median response was 6%, the same result obtained from previous studies. This is a staggering figure. If multiplied by the U.S. gross domestic product, which for 2004 will total over \$11 trillion, it would translate into \$660 billion in annual fraud losses (see [exhibit 1](#)).

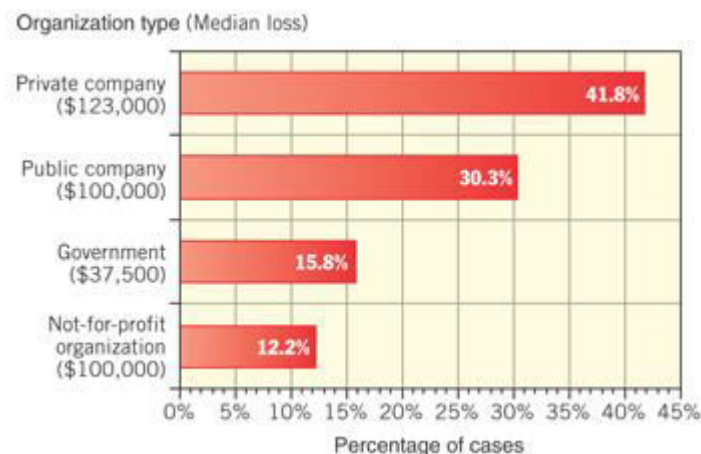
Exhibit 1: Total Occupational Fraud Losses



VICTIMIZED ORGANIZATIONS

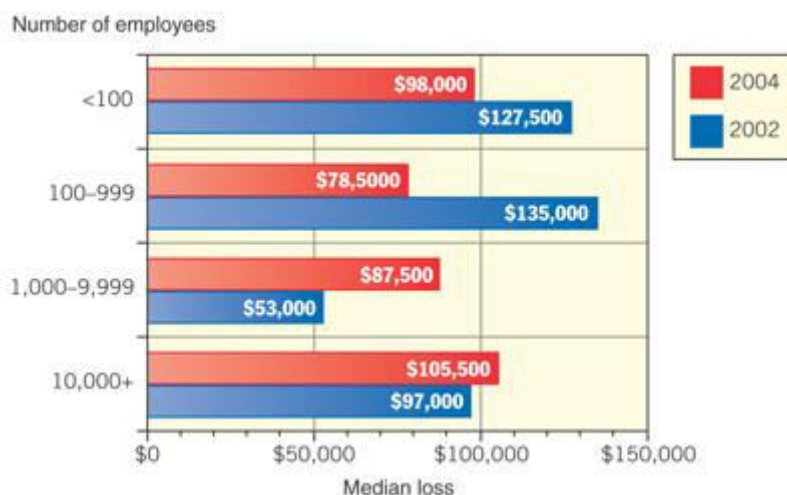
The victims of occupational fraud are the organizations that employ the fraud perpetrators and suffer losses as a result of these crimes. [Exhibit 2](#) shows the distribution of frauds in the ACFE survey, based on the type of organization that was victimized.

Exhibit 2: Type of Organization Victimized



Approximately 46% of the occupational frauds in our study were committed in small businesses (defined as organizations with fewer than 100 employees). The impact of occupational fraud on small businesses was much greater than on larger companies (see [exhibit 3](#)). Part of the reason for the larger losses is that small businesses are the least likely to be audited. As noted in the 2002 report, the audit appears to be a powerful deterrent to occupational fraud.

Exhibit 3: Median Loss Based on Size of Organization



HOW OCCUPATIONAL FRAUD IS COMMITTED

A major goal of the study was to gain a better understanding of how fraud is committed and the types of schemes that tend to produce the largest losses. We classified each fraud according to the methods used by the perpetrator. Breaking down occupational frauds into distinct categories also helps CPAs better understand the common characteristics, which in turn assists in the development of better antifraud tools.

There are three major categories of occupational fraud to consider:

Asset misappropriations. These schemes involve the theft or misuse of an organization's assets by such means as skimming revenues, stealing inventory or committing payroll fraud.

Corruption. Fraudsters wrongfully use their influence in business transactions to procure some benefit for themselves or another person. One of the most common is accepting kickbacks or engaging in conflicts of interest.

Fraudulent financial statements. These generally involve falsification of an organization's financial statements by overstating revenues or understating liabilities or expenses.

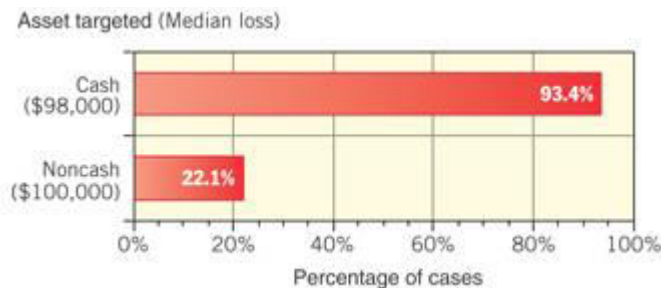
Exhibit 4: Methods of Fraud—All Occupational Frauds



Note: The percentages exceed 100% due to multiple schemes in more than one category.

While asset misappropriations were by far the most common of the three categories, occurring in over 90% of the cases, they also had the lowest median loss, at \$93,000. Conversely, fraudulent financial statements were the least common (7.9%) but had the highest median loss at \$1,000,000. (See [exhibit 4](#) and [exhibit 5](#).)

Exhibit 5: Breakdown of Asset Misappropriations



Note: The percentages exceed 100% due to multiple

schemes in more than one category.

CASH MISAPPROPRIATIONS

Of the cases in the study, 87% involved some form of cash misappropriation. Cash frauds fall into one of three categories:

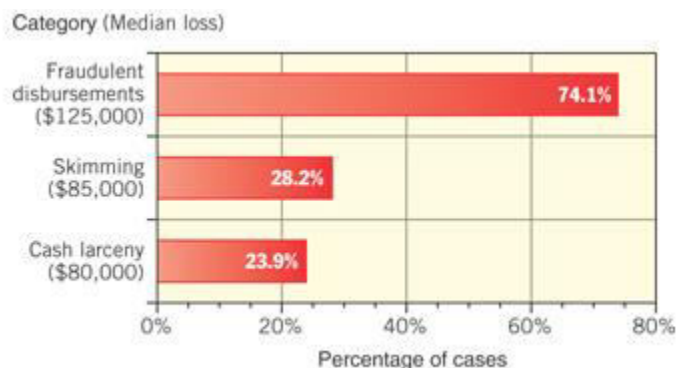
Fraudulent disbursements. A perpetrator causes his organization to disburse funds through some trick or device, such as submitting false invoices or forging company checks.

Skimming. Cash is stolen from an organization *before* it is recorded on the organization's books and records.

Cash larceny. Cash is stolen from an organization *after* it has been recorded on the organization's books and records.

Approximately three-fourths of the cash frauds in the study involved some form of fraudulent disbursement, making this the most common category by far. Schemes that involved a fraudulent disbursement also had the highest median loss, at \$125,000. (See [exhibit 6](#).)

Exhibit 6: Breakdown of Cash Misappropriations



Note: The percentages exceed 100% due to multiple schemes in more than one category.

FRAUDULENT DISBURSEMENTS

Just over half of the fraudulent disbursement cases in our study involved billing fraud, making this the most common type. Among these cases the highest median loss occurred in schemes involving check tampering. (See [exhibit 7](#).) The schemes included the following:

Exhibit 7: Breakdown of Fraudulent

Disbursements



Note: The percentages exceed 100% due to multiple schemes in more than one category.

Billing. A fraudster causes the victimized organization to issue a payment by submitting invoices for fictitious goods or services, inflated invoices, or invoices for personal purchases. Example: When a secretary for a public company interceded on behalf of an unpaid legitimate supplier and the accounts-payable department could not locate the original invoice, it nonetheless agreed to pay the vendor based on a fax copy. Seizing on this basic internal control deficiency, the secretary and two nonemployee accomplices set up three phony companies, submitting fax copies of doctored original invoices for “consulting fees.” The fraud was discovered when a manager questioned a huge variation in the budget—but not until four years and \$1.7 million later.

Payroll. An employee causes the victim organization to issue a payment by making false claims for compensation. Example: A controller for a small nonprofit organization, believing she should be earning twice her salary, added a “ghost” employee to the payroll. Since she managed both the bank accounts and the books—a serious internal control deficiency—that was easy enough to do. Every pay period, she wrote a paycheck to the nonexistent ghost, but thanks to the company’s direct payroll deposit policy, the money actually went straight to her bank account. The bank evidently never noticed the discrepancy. During a surprise audit of the payroll account, the controller mysteriously left town. It didn’t take the auditors long to figure out why when they matched the direct deposits and uncovered the scheme, which had cost the nonprofit \$208,000 over three years.

Expense reimbursements. An employee enters a claim for reimbursement of fictitious or inflated business expenses.

Check tampering. The perpetrator converts an organization’s funds by forging, altering

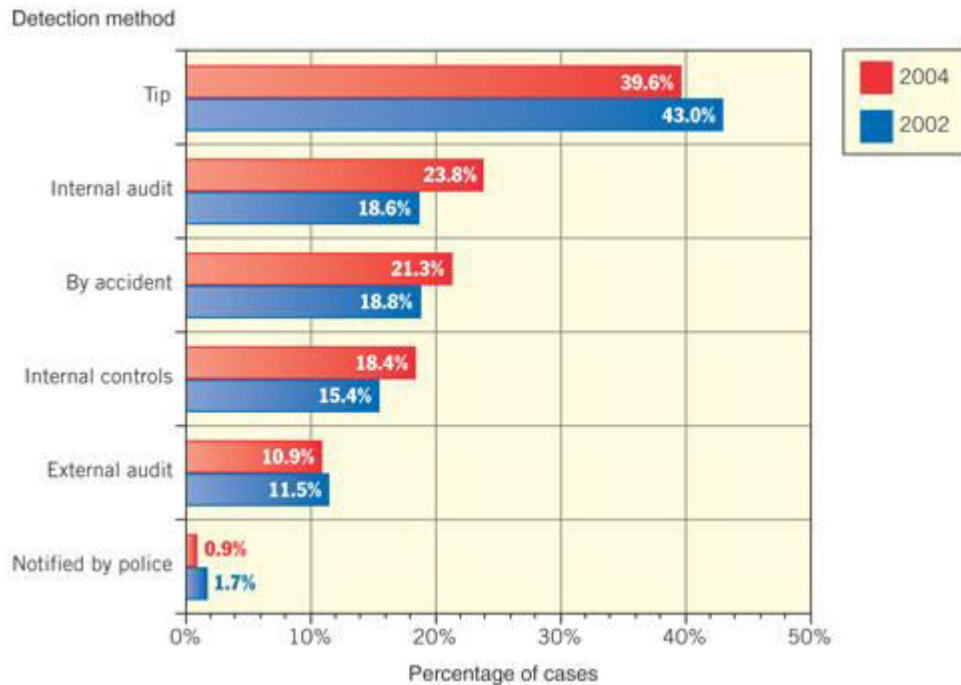
or stealing a check. Example: The administrative assistant to a CEO of a privately held company knew her boss's habits all too well. Each week, right before lunch, she presented him with a stack of checks, which he quickly signed. He didn't notice the checks were prepared in erasable ink. The administrative assistant—who also acted as the company's bookkeeper—would change the payee on the checks, deposit the funds to her own bank account and post the checks to various company expenses in order to conceal the fraud. When the checks were returned in the bank statement, the assistant would change the name back to the payee to whom the payment was originally directed. In her haste, however, she altered checks meant to pay the boss's personal expenses. In the end, the boss's appetite cost him a half-million dollars.

Register disbursements. An employee makes false entries on a cash register to conceal the fraudulent removal of currency. Example: A crafty service station attendant discovered a flaw in the cash register system; it could put a sale on hold until the transaction was completed. Simply depressing the “hold” button for a few extra seconds made the transaction disappear altogether. So when a customer bought gasoline, the clerk would erase the sale and pocket the proceeds. Company auditors finally noticed a large disparity when they compared fuel inventory to sales. After exhausting all other possibilities (including leaks in the fuel storage tanks), they installed surveillance cameras over the cash registers and caught the fraudster on tape. This simple scheme cost the company \$132,000.

DETECTING FRAUD

As in the 2002 study, the most common means of detection—by a wide margin—was through tips (see [exhibit 8](#)). Recognizing the value of encouraging tips, section 301 of the Sarbanes-Oxley Act requires audit committees of publicly traded companies to establish procedures for “the confidential, anonymous submission by employees of the issuer of concerns regarding questionable accounting or auditing matters.”

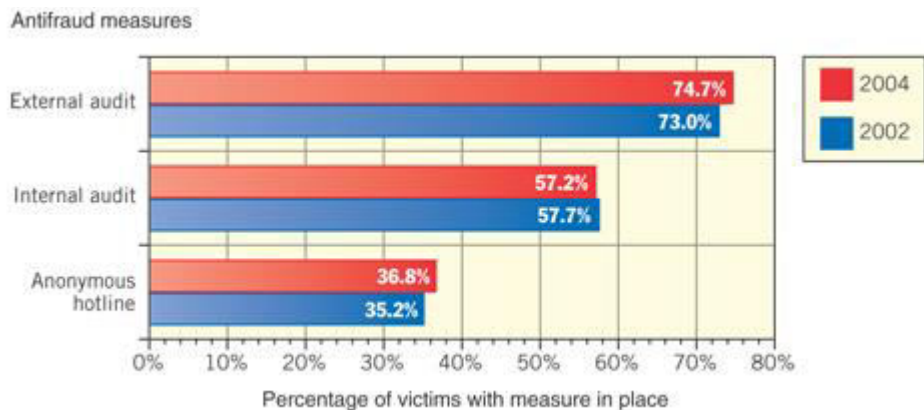
Exhibit 8: Initial Detection of Occupational Frauds



Note: The percentages exceed 100% because some respondents identified more than one method.

Respondents were asked what, if any, antifraud measures they had in place at the time the frauds occurred. They listed anonymous reporting mechanisms (typically hotlines), internal audit or fraud examination departments and external audits. [Exhibit 9](#) shows the percentage of victimized organizations that had implemented these mechanisms.

Exhibit 9: Frequency of Antifraud Measures



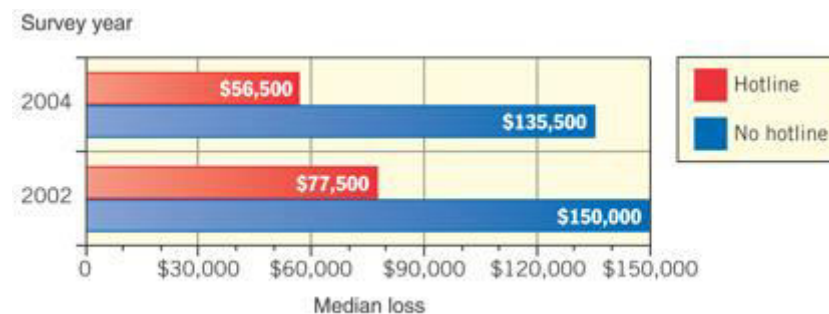
Note: Some respondents had more than one measure in place.

HOTLINES WORK

To test the effectiveness of each antifraud control, the study measured the median loss for organizations with controls against those without them. The figures showed that

anonymous reporting mechanisms had the greatest impact on reducing fraud losses. Organizations that did not have reporting mechanisms suffered median losses that were more than twice as high as organizations with them. (See [exhibit 10](#).) This was consistent with the findings of the 2002 report.

Exhibit 10: Median Loss Based on Whether Organization Had a Hotline



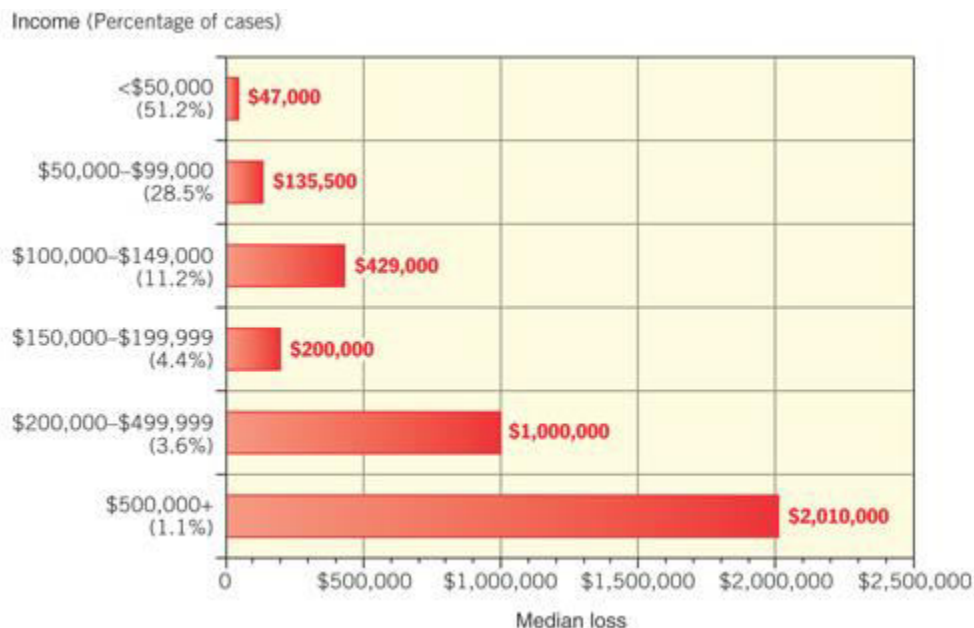
This result is also consistent with the data the ACFE gathered showing the most common way for frauds to be discovered is through tips. Obviously, hotlines and other reporting mechanisms are designed to facilitate tips on wrongdoing. The fact that tips were the most common means leading to detection—combined with the fact that organizations that had reporting mechanisms showed the greatest reduction in fraud losses—indicates this is an extremely valuable antifraud resource. The effectiveness of these reporting mechanisms is significantly higher when they are made available to customers, vendors and other third parties—not just employees. Organizations that rushed to implement employee hotlines to comply with Sarbanes-Oxley might profit from adding these valuable additional sources of information.

Curiously, anonymous reporting mechanisms were the least common antifraud measure of the three we tested for; only slightly more than one-third of victim organizations in our study had established anonymous reporting structures at the time they were victimized.

THE WAGES OF CRIME

Generally speaking, the position perpetrators held in an organization and their annual income tended to be the most significant factors in the size of losses in a fraud scheme. As the employees' level of authority rose, so did fraud losses. In just under 5% of the cases in the ACFE study, the perpetrator earned more than \$200,000 a year—but, in those cases, median losses exceeded \$1 million (see [exhibit 11](#)).

Exhibit 11: Median Loss Based on Perpetrator's Annual Income



OBSERVATIONS

In many respects, the ACFE's 2004 report supported its findings of 2002: Small businesses still were disproportionately affected by occupational frauds, asset misappropriations still accounted for approximately 90% of reported cases and the vast majority of perpetrators were still first-time offenders. As in 2002 occupational frauds still were much more likely to be detected by a tip than through an internal or external audit; and anonymous reporting mechanisms such as hotlines still exhibited the greatest impact on occupational fraud losses.

But the 2004 report also presents new information about occupational fraud that is especially critical in the post Sarbanes-Oxley world. For example, the ACFE found that over half of all frauds committed by owner/executives were detected through a tip, which was much higher than the rate for fraud in general. By comparison, only 6% of these cases were caught through internal controls. Obviously, this was because owners and executives often were able to override controls to commit fraud. Given the fact that schemes by owner/executives now must be disclosed to audit committees regardless of whether they are material, and that these schemes tend to be the most costly, the study offers strong support for Sarbanes-Oxley's requirement for the establishment of anonymous reporting mechanisms.