White Collar Crime

Where Has All the Money Gone?

By Michael A. Gips

"Without some dissimulation no business can be done at all," wrote the Earl of Chesterfield almost 250 years ago. The Earl is long forgotten, but his business philosophy flourishes among white collar criminals--although his modern disciples might quibble over the use of the word "some."

White collar crime in 1998 will take a toll that is impossible to tally, given that so much of it goes undetected or unreported. Experts agree, however, that the problem is growing. In 1974, the U.S. Chamber of Commerce estimated that white collar crime was at least a $40 billion problem. By 1996, the Association of Certified Fraud Examiners estimated that U.S. companies were losing more than $400 billion a year to occupational fraud and abuse--that is, internal fraud--alone. Criminals quickly find the "opportunities" in every business development, adapting each new technology to their nefarious needs.

To turn the tide on this army of amoral profiteers, law enforcement is mustering new resources and enlisting the help of private business forces. But no one expects an early victory.

Law enforcement officials, auditors, forensic accountants, consultants, security directors, and other white collar crime experts collectively paint a picture of white collar crime blooming in areas ranging from garden-variety occupational fraud to electronic transfer fraud, which are among the most common or rapidly growing types of white collar crime. Other hot topics in the field include financial institution fraud, healthcare fraud, Internet scams, telemarketing fraud, investment fraud, and warranty fraud.

Occupational fraud.
Occupational fraud refers generally to an employee's misuse of his or her occupation for self-benefit at the expense of the employer. Many experts see this arena, typically characterized by embezzlement, false statements, expense account fraud, and conflicts of interest, as the core of white collar crime.

One widely accepted indication of the size of the problem among U.S. businesses comes from a survey of 2,608 fraud examiners by the Association of Certified Fraud Examiners (ACFE). That 1996 *Report to the Nation on Occupational Fraud and Abuse* found that organizations lose about 6 percent of their revenues to fraud and abuse.

"Many of us were shocked [at the estimate]," says Joseph T. Wells, founder and chairman of the ACFE. "Most people thought it would be about 2 or 3 percent max."

Wells emphasizes that these numbers are just estimates and that there is no systematic way to measure occupational fraud. Still, Wells says, expert opinion holds that the problem is growing. "That is to say, we haven't seen the worst yet."

Experts with whom Wells has consulted specifically cite corruption schemes such as bribery--and especially conflicts of interest--as on the rise.

Another mainstay of occupational fraud is the kickback, which Wells says is still ubiquitous: "If you have a company of say $50 million or over in sales in the United States, I would say there is almost a dead-on likelihood that somewhere in the contracting process one of your employees is accepting kickbacks."

Perpetrators. The profile of who is committing these crimes may also be shifting. According to the ACFE's 1996 Report to the Nation, owners or equity executives accounted for only 12 percent of the problem. That's changing, says Stephen Alpert, national managing director of American Express Tax & Business Services, Litigation and Forensic Services. He asserts that fraud is increasingly committed by the most trusted people in the company--those at the highest levels.

The ACFE's Wells hasn't noticed such a trend. But no one disputes that it is the crimes committed by high-level executives that inflict the most damage. The ACFE report shows that the median loss inflicted by owners and executives is sixteen times greater than that caused by rank-and-file employees: $1 million versus $60,000.

Wells adds that it is often easiest for senior officers to perpetrate schemes, because they have the access to both the money and the books, which they can manipulate to keep the transactions hidden. They also have the most latitude to commit schemes that can be kept off the books and are, therefore, hard to trace. Moreover, he notes, it is often difficult for security directors to investigate charges against managers and officers who outrank them in the corporate hierarchy, because those high-level professionals can bring their influence to bear.

Nonprofits. Particularly hard-hit by employee abuse have been tax-exempt organizations, including foundations, universities, and not-for-profit hospitals, says Jack Taylor, managing director, KPMG Peat Marwick, Washington, D.C. These organizations are being victimized by their employees in every way from kickbacks to expense account abuse to employee sales of donated goods. In some cases such as sweetheart bidding arrangements, says Taylor, these organizations are being "victimized twice," once by the employee and once by the winner of a rigged bid, who will likely perform shoddy workmanship.

Taylor and Barrie Drum, a senior manager in the Baltimore office of KPMG Peat Marwick, note that the board members of these organizations are frequently unaware that white collar crime may threaten their tax-exempt status. The concerns are compounded, says Drum, because nonprofits often don't conduct background checks on prospective employees and don't prosecute criminals in their ranks for fear of

alienating contributors and getting stigmatized by the media. Moreover, according to Drum, many institutions lack good ethics policies and effective reporting systems.

Auditors and forensic accountants cite a few factors that are facilitating the growth of occupational fraud. First, many of the schemes are now conducted with the aid of a computer, where information can be more easily hidden, altered, or deleted.

Another factor involves the fallout from downsizing in the early nineties, some say. Many terminated workers who feel betrayed have exacted punishment on their employers by committing various types of fraud, says forensic accountant Howard Silverstone, a principal in the firm of Linquist Avey Macdonald Baskerville in Philadelphia. Silverstone notes that today more than ever, ex-employees are rationalizing their internal fraud. Other experts note that internal controls are weakened when personnel are laid off and one person has to handle several layers of a task with little or no oversight.

In addition, security and audit functions were the first to go when companies "reengineered" after downsizing, says American Express's Alpert. Now that companies in many industries are growing again, he says, the new jobs are going to workers in revenue-generating positions, not to security or audit specialists.

As a corollary, Alpert cites the effects of government downsizing and the growing sentiment to make government less intrusive in people's lives. The result, he suggests, is the shrinking power of federal watchdog agencies such as the Securities and Exchange Commission.

Financial institutions. The investigation of fraud involving financial institutions takes about 41 percent of the time and resources of the FBI's financial crime section, according to Charles Owens, chief of the Bureau's financial crime section.

The problem has been growing. According to Owens, at the end of 1991 the FBI was pursuing 7,613 financial institution fraud cases. By late 1997, that number exceeded 8,300.

Owens says that external frauds against banks, such as check frauds and mortgage loan frauds, are especially hot--now accounting for more than 60 percent of fraud affecting financial institutions. Driving these new external threats, he says, are organized bands of ethnic groups such as Vietnamese, Nigerians, Mexicans, and Russians. The FBI has tracked many fraudulent check schemes to the Los Angeles, San Francisco, and Sacramento areas--where most Vietnamese and Mexican groups operate--particularly Orange County, California, where Owens says the FBI's efforts are being focused.

Dana Brown, deputy special agent-in-charge, financial crimes division, U.S. Secret Service, recently testified before the Senate that most of the service's financial institution fraud investigations involve check fraud and access device fraud, many involving counterfeiting.

Mortgage loan fraud, Owens says, is also seeing "renewed interest." According to testimony by Owens

before the Senate, analysis of all financial institution fraud referrals received by the FBI in fiscal year 1996 revealed that 35 percent of the $3.3 billion in reported losses involved some type of loan fraud or false statement. In 1997 the Office of the Comptroller of the Currency revealed that credit risks arising from shaky loans were on the rise at almost 20 percent of 2,300 federally chartered banks, though risks were high at only 3 percent.

Electronic transfer fraud. Various experts predict that electronic transfer frauds--including those occurring via the Internet and with credit cards--will explode as society shifts away from paper and adopts new technology that most people don't understand. Companies are struggling to develop secure payment methods, such as the Secure Electronic Transaction (SET) system, designed to prevent theft of credit card numbers on the Internet.

Visa and MasterCard have been working with Microsoft, Sun Microsystems, and other companies on standards that would let merchants know they're dealing with legitimate cardholders and vice versa--while protecting the credit card numbers. Allan Trosclair, CPP, vice president of Visa USA Inc., says that the program is being pilot tested in the United States, United Kingdom, and parts of the Asian Pacific region. So far, no fraud has been detected by the system or reported by consumers in the pilot test, he says. A Visa director will discuss SET and the test findings at the National White Collar Crime Center's Economic Crime Summit in St. Louis this April (for information, 800/221-4424 x45).

Healthcare fraud.
As the baby boomers go, so does much of American society, and the prospect of 76 million Americans entering their golden years has many fraud experts concerned. According to the U.S. General Accounting Office (GAO), healthcare fraud was a $30 billion to $100 billion problem in 1995, and the stakes may be increasing.

The GAO estimates that healthcare fraud might account for as much as 10 percent of the healthcare dollar. The GAO has chronicled healthcare fraud, especially Medicare fraud, in a series of reports and published testimonies. (Many of these documents are on *Security Management Online*).

The GAO has also set up an Internet site, called FraudNET, through which the public can report fraud, mismanagement, and abuse by or against the federal government. The site has been receiving more and more reports of healthcare fraud.

Trudy Moreland, FraudNET's project manager, sees a "constant flow" of healthcare-related reports. FraudNET devotes an entire investigative team to that problem. Moreland adds that while many bursts of reporting of other types of fraud coincide with heavy media coverage of an issue, such as Internal Revenue Service abuses, reporting of healthcare issues "hasn't slowed up at all."

Christopher M. B. Disney, chairman of the ASIS Standing Committee on White Collar Crime, acknowledges the issue as a growing concern. With more people seeking medical services, he observes, healthcare practitioners will have a larger playing field on which to commit fraud.

"Virtually every aspect of the healthcare delivery system is prone to some sort of fraud," says the FBI's Owens. Common ruses include billing for services not rendered and misrepresenting services to obtain reimbursement. He notes that the FBI healthcare fraud caseload has mushroomed from 591 cases in 1992 to more than 2,400 in the third quarter of fiscal year 1997.

Certain parts of the country are particularly prone to healthcare fraud, he says. Two examples are Dade and Broward counties in southern Florida, which have heavy elderly populations. Ten percent of all Medicare expenses in the country occur in those counties, says Owens, which makes the problem there especially acute. In response, the FBI has set up three squads--more than in any other region of the country--in the Miami field office to fight the problem.

Internet fraud.
The Internet is the newest playground for creative scam artists. They bring to it many of their old tricks, enhanced with new technological twists. And while these frauds generally target individuals, the companies they work for are bearing more of the losses, explains Linquist Avey's Silverstone.

In one typical case, recalls Silverstone, a man stayed at his office after work hours to log onto the Internet for personal use. At one Web site featuring pornography, he downloaded software that, unbeknownst to him, disabled his speakers and modem, so that he would not hear his machine dialing out, then triggered his modem to dial a number in Moldova. He ended up racking up $8,000 worth of phone bills, which his company paid. (Silverstone says that whether companies are obliged to pay these charges is now a gray area in the law.)

To avoid this type of problem, Silverstone advises that companies have a well-disseminated, oft-reinforced policy confining Internet use to business purposes only. Industry is starting to respond to this problem by drafting and enforcing such Internet use policies for staff and by installing software that monitors employee Web use and blocks access to problematic sites. The National Computer Security Association, which recently formed a Secure Internet Filtering Technologies Consortium, counts about two dozen Internet filtering products on the market.

Internet fraud is wreaking havoc with the FBI's fraud caseload. According to Tom Harrington, a supervisory special agent responsible for an economic crimes squad in the Philadelphia office of the FBI, small cases that were once handled at the state and local level now require federal jurisdiction because they involve the Internet and therefore trigger interstate commerce laws. In these cases, such as when a man was swindled out of about $300 worth of baseball cards on the Internet, the FBI simply lacks the manpower to address the complaints.

Telemarketing fraud.
As with the Internet, telemarketing fraud often targets individuals, such as the elderly. But telemarketing fraud is also used to rip off businesses, especially small and medium-sized ones, says Harrington.

In a typical case, a telemarketer will call companies and offer to sell them maintenance supplies such as

light bulbs or cleaning solutions. The telemarketers will then arrange to pay a kickback to the purchasing manager if he or she buys the product, which is often grossly overpriced or of low quality.

Another twist on this scheme occurs when a telemarketer calls companies and then invoices them for products without having received approval for the purchase. Seeing a bill for small-ticket items, a busy accounts payable department will often issue a check. For example, the FBI is pursuing a case in which a man would send an invoice totaling $1,000 to companies for garbage bags that he had purchased for $12. The man allegedly billed the companies before they approved the order.

Investment fraud.
Ten years ago, penny stocks--highly speculative stocks selling for less than a dollar--were all the rage. Many of the stocks turned out to be shares of bogus companies. With the stock market at record highs, law enforcement officials say that penny stocks are on the rise again--and while many are legitimate, fraud is again a problem, this time with organized crime getting into the act to manipulate prices and cash out, leaving small investors holding the bag. For example, last November the United States Attorney in Manhattan indicted members of two New York organized crime families on charges that they swindled investors out of millions of dollars.

Experts in New York's security regulations offices estimate that investment fraud cost Americans $6 billion in 1996. They also note that complaints about stock market fraud were up 25 percent through mid-1997. The *New York Times* also recently reported that at the U.S. Attorney's office in Manhattan the number of indictments issued against people accused of organizing small stock scams has almost doubled in the last year.

The ACFE's Wells points out that fraud on the market might be far more rampant than anyone imagines. "Usually those frauds are not uncovered until bad economic times, like the S&L crisis in the late eighties."

Warranty fraud.
This ploy, often practiced by electronics dealers, involves fraudulently claiming that an item is under warranty and obtaining replacement goods under a warranty exchange. A typical scam involves multiple requests to replace the same piece of equipment--typically computers. (Perhaps surprisingly, most computer manufacturers don't keep track of hardware, such as by placing serial numbers on components.)

Here, too, the numbers indicate that the problem will get worse. By conducting benchmarking studies of seventeen companies in the computer hardware industry, one consulting firm has estimated warranty fraud in that industry as a $2.2 billion problem in 1997, up from $1.6 billion in 1995 and $1.9 billion in 1996. That firm, Asset Management Solutions, Raleigh, North Carolina, forecasts that warranty fraud will cause losses of $3.4 billion by the year 2000.

At Sun Microsystems alone, the consulting firm roughly calculated that warranty fraud costs $22 million

to $44 million a year, according to Don Greenwood, manager of international security. And Asset Management Solutions CEO Barry Wilkins says that several respondents to his company's study reported that more than 30 percent of warranty claims were fraudulent.

Detection/prevention.

While the information age has opened up a world of new fraud opportunities, it is also starting to provide business with some solutions. Software that performs exception reporting and brings up irregularities in online ledgers, cash disbursement records, and inventory records has been around for a while, but the market is starting to see more sophisticated products as well as software designed to retrieve deleted and hidden files. At least one product pinpoints signs of contract and procurement fraud and develops an investigative plan.

Still, many experts say that the best detection and prevention methods are the traditional ones, such as adequate reporting programs, regular and surprise audits, suspicious transaction monitoring, and communication of policies with staff.

The Federal Sentencing Guidelines for Organizations, in effect since November 1991, has created a strong incentive for companies to develop fraud prevention programs. The guidelines hold companies and their executives criminally responsible for fraud but reduce the penalties for companies with reasonable security programs.

KPMG's Taylor says that in the year and a half he's been with that firm, corporations are becoming increasingly aware of the need for a code of ethical conduct for employees, managers, and directors. Disney, of the ASIS white collar crime committee, adds that he's seeing more companies establish sound whistleblower programs.

But KPMG's Drum says that effective ethics policies are still wanting in many corporations, and that these businesses often lack reporting channels for employees. Instead of addressing fraud problems proactively, which requires a substantial time and cash commitment, she says, companies are acting after-the-fact, looking for quick fixes that cannot be rewarded by the federal sentencing guidelines.

"The biggest mistake is coming up with a code of conduct and an 800 [reporting] line and thinking you have a policy," says American Express's Alpert. "It has to be an ongoing thing."

A critical element in prevention and detection, says Alpert, is knowledge of the industry. Companies committed to combating white collar crime are learning the importance of knowing the particular conditions in the industry that make certain types of fraud likely. For example, an expert in healthcare fraud would know that certain types of billed procedures could only be performed by a specialist, not a resident.

Law enforcement is also trying to do its part. The FBI is forming joint partnerships with corporate America, such as a training program for companies in Philadelphia. Participating businesses receive periodic faxes from the FBI that supply fraud trends and advice.

As part of its annual crime survey, the FBI is also trying to reach out to the business community and gauge its concerns, says Harrington. The FBI tries to press its message through presentations, seminars, and conversations with auditors at major corporations. For example, via the local chamber of commerce, the Philadelphia office of the FBI is sending a warning to cash-strapped companies about advance fee schemes (fees for loans that are promised but never materialize), which are wiping out smaller businesses.

In the financial institution sector, the U.S. Secret Service has an Electronic Crimes Special Agent Program in which agents trained in forensic examination of computers provide technical assistance to investigators, such as retrieving evidence from hard drives. The Secret Service has also established a counterfeit instrument database, containing specimens of counterfeit instruments such as payroll checks and bank checks. Deputy Special Agent Brown has testified that the database has helped identify specific equipment used in counterfeiting.

For its part, the FBI helped create a subgroup of the Interagency Bank Fraud Working Group to focus on computer-related fraud at financial institutions. This body has been drafting interim guidelines for reporting computer crimes against banks.

The FBI is also promoting an inkless fingerprint system for use by nonbank customers. Owens recently testified that the program, promoted by more than twenty state bankers associations, has led to a 70 percent reduction in check fraud in states where it is in use. In addition, the FBI is due to come out with an international fraud prevention video, aimed at mid-level managers and executives in financial services operations.

In 1996, Congress acted on healthcare fraud by enacting the Health Insurance Portability and Accountability Act. Under the statute, the FBI received $47 million in fiscal year 1997 (up from $38 million in fiscal year 1996) for its healthcare fraud efforts, which bolstered staffing by forty-six agents. Funding under the statute is due to increase incrementally until 2003, when it will plateau at $114 million.

Other resources are being marshalled to battle fraud. Property-casualty insurers in the United States spent more than $650 million on fraud prevention and detection in 1996, as opposed to about $200 million in 1992, according to the Insurance Research Council. That group suspects that insurers will devote even more resources to the issue in coming years.

The ASIS white collar crime committee has taken its message of business ethics to business schools to raise awareness among the business men and women of tomorrow. It is beginning with about five New England-area business schools, says Chairman Disney, and has received a good reception. "Students for

the most part want to see what the pitfalls may be."

It remains to be seen whether these efforts will take some of the starch out of white collar criminals. But KPMG's Drum doesn't think so: "If there's an opportunity out there, people are going to take it."

Michael A. Gips is a senior editor of Security Management.
