

---

---

# Root Out Financial Deception

Detect and eliminate fraud or suffer the consequences.

BY W. STEVE ALBRECHT AND CONAN C. ALBRECHT

Employees and others who commit fraud have long relied on management's inability to see what's going on right under their noses. Why? Because it has been too difficult and expensive to sift through the enormous volume of business transactions taking place each day. Too often the intensive record-screening necessary to detect improprieties slows business processes and consumes funding and staffing. At some point, the "cure" becomes worse than the "disease." Practitioners' clients and employers need better antifraud weapons: This article explains several ways CPAs can respond by using technology to detect fraud—and even prevent it from taking place.

There are several reasons to make the effort. SAS no. 82, *Consideration of Fraud in a Financial Statement Audit*, requires auditors to assess the risk of material misstatement in financial statements due to fraud. And the payoff—for companies that beat fraud—is potentially great savings. In its 2002 publications, *Report to the Nation and National Fraud Survey*, the Association of Certified Fraud Examiners estimated that fraud and abuse costs U.S. organizations more than \$600 billion annually.

To control that financial hemorrhaging, business leaders have begun teaming up with fraud experts—in a recent trend—to quickly examine financial data, uncover evidence of possible misdeeds and prevent additional losses. Technology plays a central role in such strategies, and by combining their knowledge of business processes with forensic computing skills, CPAs can pinpoint and evaluate signs of possible fraud and, if further investigation reveals actual wrongdoing, take steps to recover losses and prevent more damage.

## HOW SMALL COMPANIES CAN FIGHT FRAUD

CPAs can choose from among several techniques to penetrate thickets of data and find the relevant bits of evidence necessary

to uncover and stop fraud. But to apply such methods effectively, practitioners first must consider the extent of the entity's auditable data, its available funding and the qualifications of its staff.

### The Tip of the Iceberg

Fraud usually reduces net income on a dollar-for-dollar basis. A \$10,000 fraud, for example, lowers net income by \$10,000. So, if a company's profit margin (net income/revenues) is 10%, the company must generate additional revenue—up to \$100,000 in this case—as much as 10 times greater than the amount of the fraud to restore net income to its pre-fraud level. That's why it's important to detect fraud as soon as possible.

Auditors looking for fraud in smaller organizations' data will find that most of the following technology-based methods—which rely on deductive analysis—will suffice. These techniques derive specific findings from general principles. For example, if an organization wants to find out why its purchasing costs are rising, its staff and its CPA could examine the records relating to each of its vendors. If a particular vendor's prices rose, but a purchasing manager ordered more of its products, the only legitimate explanation would be that the quality of the vendor's products had improved greatly, inducing the purchasing manager to both pay a higher unit price and increase the quantity of his or her order. But if the auditors then analyzed customer service records and found numerous complaints about the quality of that vendor's products, the *likelihood* of fraud would be sufficient to perform a thorough investigation, even

## Discovery Sampling Table

Sample size	Maximum percentage of sample containing signs of fraud							
	0.01	0.05	0.1	0.2	0.3	0.5	1	2
	Percentage of certainty that above percentage is accurate							
50		2	5	9	14	22	39	64
60	1	3	6	11	16	26	45	70
70	1	3	7	13	19	30	51	76
80	1	4	8	15	21	33	55	80
90	1	4	9	16	24	36	60	84
100	1	5	10	18	26	39	63	87
120	1	6	11	21	30	45	70	91
140	1	7	13	24	34	50	76	94
160	2	8	15	27	38	55	80	96
200	2	10	18	33	45	63	87	98
240	2	11	21	38	51	70	91	99
300	3	14	26	45	59	78	95	99+
340	3	16	29	49	64	82	97	99+
400	4	18	33	55	70	87	98	99+
460	5	21	37	60	75	90	99	99+
500	5	22	39	63	78	92	99	99+
800	8	33	55	80	91	98	99+	99+
1,000	10	39	63	86	95	99	99+	99+
1,500	14	53	78	95	99	99+	99+	99+
2,500	22	71	92	99	99+	99+	99+	99+

Note: Because of its minimal effect on sample size, population size is not included in the above table.

Source: From *Audit Sampling: An Introduction* (3rd ed.) by Dan M. Guy, D. R. Carmichael and O. Ray Whittington, John Wiley & Sons, 1994.

if—as is quite possible in such inconclusive circumstances—there turns out to be no evidence of wrongdoing. Generally, deductive techniques are simple and economical to apply but can lead to ambiguous findings, as the following examples will demonstrate.

**Discovery sampling.** This basic technique, which requires only a personal computer and inexpensive generic software designed for this kind of analysis, suits the capabilities of small organizations that don't have the budget or expertise to conduct more thorough and expensive investigations. Since discovery sampling requires only moderate skills and rudimentary technology, its cost is minimal.

For instance, if an auditor wanted to examine checks to see if someone in the company was making fraudulent payments to vendors, he or she would use random-number-generating software to select the serial numbers of checks to review. The auditor then would refer to a basic discovery sampling table (see "Discovery Sampling Table") available in any auditing textbook. Such a table consists of a probability matrix correlating the frequency of certain occurrences in a sample with approxi-

mations of the likelihood of their existence in the population from which the auditor drew the sample. Thus, the table would help the auditor—based on his or her examination of some of the checks—to infer reasonable conclusions about all of them.

If the auditor reviewed 300 of 6,000 checks and found no signs of fraud, he or she could be 95% confident that no more than 1% of all checks were fraudulent or 78% confident that no more than 0.5% were. Using the discovery sampling table above for example, the auditor could determine this by locating in the first column the sample size he or she is using and then looking along that row for the percentages of confidence that the value at the top of each column is correct. That value (1%, for instance, is at the top of the column containing 95%, and 0.5% is at the head of the column containing 78%) indicates the maximum percentage of the sample that may contain signs of fraud. To be more confident the sample accurately reflects the state of all the data, the auditor would have to increase its size.

The problem is that discovery sampling doesn't prevent auditors from selecting inappropriate or inadequate samples. Investigators simply search—in a random data sample—for

## EXECUTIVE SUMMARY

- **FRAUD COSTS U.S. BUSINESSES** \$600 billion each year.
- **CPAs CAN USE PROACTIVE FRAUD-DETECTION** techniques to determine when and where fraud is occurring in an organization. They and their clients then can focus on stopping current fraud and preventing it in the future.
- **DEPENDING ON THEIR EXPERTISE** and their clients' or employers' resources, needs and amount of data, CPAs use any of several investigative techniques that vary in cost, complexity and fraud-detection precision.
- **DEDUCTIVE ANALYSIS CAN HELP SMALLER** organizations fight fraud without exceeding their budget or technological resources. CPAs use such methods to conduct relatively unsophisticated searches for fraud symptoms. Data

mining, digital analysis or discovery sampling—three deductive techniques—require inexpensive, easy-to-use, generic software to search for possible signs of fraud. For small amounts of data and simple queries, these basic techniques work well. But large amounts of data and other demanding requirements often can cause them to return false leads.

- **FOR LARGER COMPANIES, INDUCTIVE ANALYSIS** is ideal for fraud detection, despite its complexity and expense. To perform it, investigative teams well-versed in fraud, in the organization's business and in database programming use custom software to estimate what types of fraud could take place in a specific situation. Deriving general principles from specific circumstances, they then conduct precise, usually fruitful searches for the kinds of fraud that most threaten a particular organization.

evidence of fraud. But because evidence of significant fraud often is clustered in only a few transactions, auditors' samples can be ineffective if they miss those records.

The task of ensuring the sample's relevance becomes even greater when auditing large databases. But, for companies that cannot afford other techniques, it is possible to improve the effectiveness of this method by examining the sample—to make sure it closely resembles all the data—before analyzing it for fraud.

**Inexpensive sampling software often produces “false leads” that appear to indicate fraud, but turn out to be irrelevant.**

**Data mining.** Auditors employ this user-friendly, low-cost technique to evaluate entire databases and, thus, avoid making inaccurate generalizations based on limited information. Unfortunately, inexpensive generic data-mining software can't efficiently process large volumes of information and doesn't allow programmers to focus their queries on specific types of fraud. This often results in numerous “false leads” that appear to indicate fraud but turn out to be irrelevant—so auditors waste time analyzing situations they ultimately determine to be innocuous.

In one case data-mining software made it possible for a small company, which believed it faced the risk of fraud involving kickbacks from vendors to the company's buyers, to sort purchasing records by vendor and purchase volume. The sorting revealed that total purchases from a particular vendor were increasing while those from all other vendors were falling. Data-mining software also helped auditors determine that prices of the favored vendor's products were rising faster than those of competing vendors. Such patterns often indicate kickback fraud. In this case, auditors discovered a scheme in which one

of the company's buyers accepted bribes in exchange for purchasing more than \$11 million worth of unneeded inventory and supplies.

Auditors should not, however, allow this type of success story to distract them from data-mining software's data- and query-processing inadequacies, which make it unsuitable for large-company use.

**Digital analysis.** Based on Benford's law, a theory of statistical probability, this method compares the expected frequency to the actual frequency of numbers that appear in a database. Although auditors can perform this technique on computerized records, it is not inherently dependent on technology. (For more information on Benford's law, see “I've Got Your Number,” *JofA*, May99, page 79, [www.aicpa.org/pubs/jofa/may1999/nigrini.htm](http://www.aicpa.org/pubs/jofa/may1999/nigrini.htm).) This approach requires auditors to examine for signs of fraud all records containing digits that occur more frequently than they should.

Although generally easy to apply and particularly useful when searching large, unsorted databases, this straightforward, economical technique does not enable auditors to match the symptoms they find with specific types of fraud. As a result, the leads it generates are only signs of potential problems; they are not detailed prognoses. So, once a fraud examiner identifies a suspicious item by means of digital analysis, he or she still must determine what kind of fraud is involved and who is committing it.

For example, one organization applied Benford's law to its supplier invoices, analyzing the first digits of dollar amounts from a total population of thousands of invoices. The patterns conformed nicely to Benford's law until the auditor started analyzing invoices company by company. Suspiciously, billing from three vendors followed patterns significantly different from those of other suppliers. Further investigation revealed that each of these three vendors had billed the company for products they never supplied. But if the auditors had ended their

analysis after seeing that, collectively, the numbers followed Benford’s law, they might erroneously have concluded the company’s purchasing was free from fraud.

## ZERO IN ON FRAUD AT LARGE COMPANIES

The three deductive analysis methods discussed above generally involve random searching of data for anomalies that could be signs of fraud. Alternatively, for more precise results, auditors—especially those working at bigger entities—can use the inductive method to focus on situations particularly susceptible to deception.

**Auditors—especially at bigger entities—can use inductive analysis to focus on situations particularly susceptible to deception.**

Knowing which areas to target isn’t self-evident, however, and CPAs and others using inductive analysis need to

- Become familiar with the business or operation to be studied.
- Understand the kinds of fraud that could occur.
- Determine what symptoms or signs the most likely frauds would display.
- Use queries to search corporate information systems for such symptoms.
- Evaluate the symptoms found to see whether fraud or other, harmless, factors caused them.

But doing that requires customized programming and other special skills of an investigative team consisting of at least the following three members, one of whom should be a CPA: a business process expert, a database programmer and a fraud expert. They should have the following qualifications:

- **Business-process expertise.** An employee with these qualifications is well-versed in the organization’s procedures and operations. He or she can identify the kinds of fraud that may exist, the symptoms they would produce and the information necessary to detect such signs.
- **Database programming expertise.** This team member is proficient in database design and operations and knows how to query various kinds of databases and write programs to automate such queries. He or she arranges retrieved data in forms useful to the other team members.
- **Fraud expertise.** This member understands the nature of fraud and knows which types are possible in a given industry. He or she also is familiar with the symptoms each type of fraud produces and knows how to detect them. Together with the business-process expert, the fraud expert evaluates information the database programmer retrieves from the organization’s computer systems.

Companies can’t employ the full range of inductive techniques without help from teams of such high-powered professionals. But this form of analysis delivers meaningful results that limit fraud losses and justify the extra cost of hiring specialists.

## Pick the Fraud-Detection Method Best for Your Company

Deductive Approach	Inductive Approach
Generic data mining	Custom data mining
Digital analysis	Analysis of all data
Discovery sampling	
Generic software	Custom software
For smaller organizations	For larger organizations
Basic features	Sophisticated features
Easy to learn	Required advanced skills
Relatively inexpensive	More expensive

## CASE STUDY: TRACKING DOWN FRAUD AT BP CORP.

Realistic executives don’t expect to keep their companies free of deception without funding the development of fraud-detection-and-prevention capabilities. At BP PLC, the British oil giant that absorbed Amoco in a 1999 merger, top management understood how seriously fraud could hurt the bottom line. So they approved the request of Gregory Dunn, CPA, BP’s Chicago-based deputy head of security, for an intensive, proactive search for possible signs of fraud among tens of thousands of vendor invoices stored in the company’s computer systems.

Earlier, Dunn’s group had come across an instance of employee and vendor collusion to bill BP for services never rendered. BP’s security division and its internal auditors worked together to detect and stop that fraud. But Dunn wanted to identify early warning signs that would enable the company to avoid future fraud losses. So, he and his colleagues researched fraud-detection techniques and began using deductive analysis to comb BP’s huge databases for useful evidence, such as the addresses of employees that matched those of vendors. Overwhelmed by the sheer volume of data, their deductive searches produced thousands of leads, almost all of which turned out to be false.

That’s when Dunn called in fraud-detection consultants to help develop more powerful tools and techniques. Using customized inductive analysis software these experts designed, BP’s auditors and security division compared electronic records of the contractors’ billing to those of their employees’ time-card-tracked entry into and exit from a certain BP facility. This revealed discrepancies between the hours billed and worked.

“In one test,” Dunn said, “we found billing for welders up to 3 standard deviations away from what we knew was reasonable. That showed us whom to focus on.” Such targeted results distinguish inductive techniques from deductive methods, which auditors use to look for any signs of fraud, with no particular specific search criteria.

Once Dunn and his colleagues targeted those contractors, they found what they had been looking for: fraudulent billing. The substantial discrepancies they found between billing and

timesheets provided incontrovertible proof, Dunn said. One contractor, on seeing the evidence, gave the company a \$50,000 refund that same day.

Dunn credited inductive analysis for the enormous improvement in the efficiency and effectiveness of BP's fraud-detection efforts. He said that his team would continue using such techniques to stop fraud before it grows.

"The question that keeps us going," he said, referring to fraud's direct impact on the bottom line, "is, 'How many barrels of oil do we have to refine to make up for that deception?'"

## EMBRACING THE FUTURE

As the cost of computing power and software drops, CPAs, their clients and employers are increasingly using some form of computer-based analysis to search for and prevent fraud. With an ordinary PC and inexpensive software, even a small organization can perform some form of deductive analysis to find and prevent fraud. But companies—both large and small—that can afford to hire employees or consultants with advanced fraud detection-and-prevention skills should make the necessary investment. As the incidence of fraud increases by leaps and bounds each year, more and more companies will realize that paying for the ounce of prevention—regardless of how costly it may seem now—is cheaper than the pound of cure they ultimately will need to conquer fraud. And by staying abreast of advanced techniques for fraud detection and prevention, CPAs can protect their employers and clients and lead successful campaigns to spot, terminate and prevent fraud, now and in the future.

## Fraud Resources

- American College of Forensic Examiners, [www.acfe.com](http://www.acfe.com).
- American Society for Industrial Security, [www.asisonline.org](http://www.asisonline.org).
- Association of Certified Fraud Examiners, [www.cfenet.com](http://www.cfenet.com).
- Association of Government Accountants, [www.agacgfm.org](http://www.agacgfm.org).
- AICPA, audit and attest standards team, [www.aicpa.org/members/div/auditstd/index.htm](http://www.aicpa.org/members/div/auditstd/index.htm).
- Information Systems Audit and Control Association, [www.isaca.org](http://www.isaca.org).
- Institute of Internal Auditors, [www.theiia.org](http://www.theiia.org).
- Society of Professional Investigators, [www.spionline.org](http://www.spionline.org).

W. STEVE ALBRECHT, CPA, PhD, CFE, CIA, is associate dean and Arthur Andersen Alumni Distinguished Professor of Accounting at the Marriott School of Management, Brigham Young University, Provo, Utah. Professor Albrecht lectures on fraud-detection-and-prevention techniques; his e-mail address is [steve\\_albrecht@byu.edu](mailto:steve_albrecht@byu.edu). CONAN C. ALBRECHT, PhD, is an assistant professor at Brigham Young University's School of Accountancy and Information Systems. Professor Albrecht designs fraud-detection-and-prevention systems; his e-mail address is [conan\\_albrecht@byu.edu](mailto:conan_albrecht@byu.edu).

---

From *Journal of Accountancy*, April 2002, pp. 30-34. © 2002 by the American Institute of Certified Public Accountants, Inc. Opinions of the authors are their own and do not necessarily reflect policies of the AICPA. Reprinted by permission.