1. Introduction to Forensic Accounting

The History of Forensic Accounting:

Fraud has become an industry, not just for the fraudster. Academics study it, investigators investigate it, lawyers litigate on it, and conference-goers debate it. But the industry is built on managing the consequences of fraud rather than on preventing fraud. The investigation of fraud is only one of the services offered by the professional forensic investigator. Equally important is the creation of a culture and environment which is aimed at the prevention of fraud and a response policy which is designed to respond to fraud detection as effectively as possible. According to a report released by Nedcor, crime cost South Africa R31 billion rends in 1994/1995. A large part of this amount can be attributed to white-collar crime. Fraud and its roots - greed and arrogance - are human nature. As business people, we must recognize fraud as a permanent risk, a risk we must take action to manage. Fraud is theft. It hits an enterprise in the pocket and has a direct effect on the bottom line. Despite the fact that statistics indicate a dramatic escalation in the incidents of fraud over the past decade, certain company executives still dismiss the suggestion that they may be victim of, or exposed to the risk of fraud. The extent of fraud and white-collar crime resulted in the formation of various specialized units in law-enforcement agencies. It also resulted in a major demand for accountants in the fields of forensic accounting as such crimes can only be proved with forensic reports and testimony by experts.

The outcome of fraud investigations may be critical to the survival of the business. Even the smallest engagement ay has serious consequences for individuals, innocent or guilty. It is accordingly vital that the appropriate experience is brought to bear. A specialist forensic accountant must always be consulted on potential engagements where fraud is at issue. General type investigation procedures are not adequate to investigate fraud. Different standards of evidence and of control and collection of material apply. There are no small fraud investigation engagements. Seemingly small frauds are frequently the tip of the major iceberg. All engagements must therefore be carried out to the same high professional standards. Fraud investigation work is wide ranging. The same investigation may be covered determining whether fraud has occurred and, if so, the nature of the loss and those responsible; tracing of assets lost and legal action against those responsible to obtain recovery; disciplinary proceedings; civil and criminal litigation. Few clients will have previous experience of fraud investigations and investigations will often be undertaken in an atmosphere of serious concern, and perhaps crisis. Effective assistance will be dependent on the forensic investigator's ability to help the client manage the crisis, shape his expectations and take action quickly and with discretion. It must be recognized that the outcome of investigations may rest not only on the quality of the investigation but on the decisions made by the client, and it is therefore vitally important that the client be accurately and correctly advised at the outset. It is thus of utmost importance that when fraud of any kind is suspected,
a experienced forensic team manage and investigate the matter. This can only benefit the client in the long run.

**What is Forensic Accounting?**

Forensic accounting can be defined as assistance in disputes regarding allegations or suspicion of fraud, which are likely to involve litigation, expert determination, and enquiry by an appropriate authority and investigations of suspected fraud, irregularity or impropriety which could potentially lead to civil, criminal or disciplinary proceedings. The focus is primarily on accounting issues, but the role of the forensic accountant may extend to more general investigation which includes evidence gathering. It is because of the fact that by definition, forensic assignments are related to judicial or quasi-judicial dispute resolution, that the forensic investigator requires a basic understanding of the applicable statutory and common law, the law of evidence and the law of procedure. The most competently conducted investigation will be of no value to the client should the evidence gathered be ruled to be inadmissible or the expert accounting witness be found to fall short in respect of the requirements of expertise, credibility, or independence.

**The Qualities of a Professional Forensic Team:**

It is essential that a professional forensic team has:

- Knowledge of the elements of economic crime;

- The ability to collect evidence and to exercise proper control over large volumes of documentary evidence;

- The appropriate skills and level of relevant experience;

- Investigation background;

- the ability to work in a team with instructing attorneys and police and have the ability to coordinate, manage and administer the litigation support, assemble the documents, and organize meetings;

- Knowledge of legal aspects such as the basic rules of evidence relating to admissibility of evidence and the drawing of inferences;

- an understanding of what needs to be proved so that evidence documented in his or her reports, letters and affidavits are compiled in a concise, logical and persuasive manner;

- The ability to testify and stand up to cross-examination in a court of law.

**Where Forensic Accounting can be applied?**

Forensic Accounting may be conducted into the following:

- Fraud and white collar crime investigations;
• Criminal and civil investigations;
• Preparation of expert reports, reviews and evidence;
• giving oral evidence in court;
• insolvency and liquidation support investigation;
• Fraud prevention and awareness strategies;
• Fraud and fund tracing;
• Civil and criminal actions regarding fraud and financial irregularities;
• Breach of contract;
• Breach of warranty, particularly on company acquisitions;
• Insurance claims;
• Liquidation support;
• Regulatory enquiries;
• Special and confidential investigations;
• Fraud and risk management surveys and reports.

A forensic accounting engagement and investigation is typically substantially longer than any other investigation. Continuity of staff on the part of the client is therefore often difficult to maintain. This makes it all the more essential that the forensic accountant conducts his work in a manner which is concise, detailed documented.

**Forensic Accounting as Prevention**

As regards an appropriate response to fraud which has been detected, every institution requires an integrated corporate strategy.

An amoral business environment corrupts honest employees.

The economy cannot afford business to become a facilitator for crime and dishonesty, merely because it has become convenient not to bring culprits to justice.

In developing an appropriate fraud response plan, it is essential that an institution considers the following steps:

What are the organization’s major risk areas and what is its policy stance on perpetrators of fraud?

What is the level of fraud awareness within an organisation?
Are controls effective?
Are customers or trading partners aware of the company's policy on fraud?
Do employees understand the company's attitude to fraud and dishonesty?
Can employees report fraud confidentially?
Are recruitment practices compatible with an honest workforce?
Do disciplinary proceedings dispense justice even-handedly and more importantly, are the seen to do so?

The Key areas of Forensic Accounting

✓ Fraud Investigation
✓ Resolving Commercial Disputes
✓ Family Law
✓ Insurance Claims
✓ Valuations
✓ Business Intelligence
✓ Data Recovery & Conversion

That's a big list of things, so let's give you a brief explanation for each of them:

**Fraud Investigation**

The bread and butter of Forensic accountants: this is where you become the detective, work out what went wrong, who did it, how they did it and how much money they've stolen.

And you're expected to present all your analysis in court or to the police.

You can go here for fuller details on forensic accounting and fraud investigation.

**Commercial Disputes**

The list is endless:

✓ legal contracts get breached (one party doesn't do what the other party expected)
✓ construction workers fall off buildings
✓ slanderous comments get made resulting in loss of business
✓ employees get sacked unfairly
Forensic accountants have to assess the impact of these disputes and in many cases tragedies.

As an example, let's say an aircraft maker is expecting a supply of engines from another company within an agreed timeframe. The engine supplier fails to meet the deadline and has now breached the contract.

Inevitably a huge fight will break out, the lawyers get called in and not long after so do we. And it could be for either side as they seek to justify their positions.

At the end of the day the job is to work out just how much money one party is expected to pay the other in compensation.

**Insurance Claims**

We're sure everyone can relate to this. You lose something. You claim it on insurance. Now imagine huge claims on complex transactions. There's work to be done to estimate just how much the loss actually is and to then convince the insurance company that it's accurate.

**Family Law**

When couples break-up the financial side of things usually turns nasty pretty quickly as each party lays claim to what is rightfully theirs.

The Forensic Accountant has to get in there and assess who has what, checking the assets/liabilities that exist, placing a value on them and then explaining all of that to the lawyers and the couples.

And of course, it may all to go court.

**Valuations**

Most people would think of this work arising where business and partnerships need to break-up, like any bad marriage unfortunately.

However, but it doesn't necessarily mean a dispute has caused it.

For example, a businessman retires and wants to sell his part of the company to a daughter, son or colleague.

Key work includes:

Valuing a company for a sale (in part or in whole)

Company valuations for bank purposes to borrow funds

Valuing the shares (or share options) in a company for potential sale or purchase
The challenge here is getting the various parties involved agreeing to the valuation. Not easy in the slightest as buyers want it cheap and sellers want it expensive.

**Business Intelligence**

Here's where things turn a bit brighter. Whilst the first five items on our list are mainly about the resolution of problems, Business Intelligence is all about providing - to management - insight into how their business is running which will help them to focus on where to deploy their resources.

For example, it will helps management discover where money is being lost so that a decision to divest (sell) a company can be made.

**Forensic Accounting and Forensic Investigation**

The concept of Forensic Accounting (never mind a fraud investigation) can be tricky if you've never heard of it before.

We explained on our "What is Forensic Accounting?" page that there were actually many different "things" that an accountant in the forensic field could actually do.

But fraud investigation is the original and best known area.

And if you're already working in this field we make no apologies for the level of simplicity we're using here to explain what it's all about.

Most people trying to find out information in this field usually get bamboozled with flowery jargon and big words.

Hopefully we're going to avoid that and give you the following:

An example of a simple fraud

Explain the concepts of Prevent and Detection Controls

Why Controls Fail

Why Big Companies = Big Frauds

Let's say you run a company. And you put your trust in your employee - Dave - to run the payroll for you every month.

That means he has to pay all your employees their monthly salaries.

You put some controls in place to make sure Dave is doing the right thing. That could mean Dave supplying you with a sheet of paper showing you which employees are being paid and how much. You review it and sign at the bottom.

Dave then goes off and pays all these employees correctly.
But, unknown to you, he adds in an extra employee to be paid that you don't know about.

Oh dear.

And it turns about to be Dave paying himself extra wages. And he ends up doing this for years.

And then one day Dave doesn't turn up to work and is now living on a beach in South America using his "extra" wages. Nice one Dave.

**Prevention and Detection Fraud**

There's two ways a company could have stopped this happening.

Welcome to the world of Prevention and Detection Controls.

And collectively they are sometimes referred to as Internal Controls.

Prevention Controls: had the company been smart enough they would have implemented controls to stop (i.e. prevent) Dave in the first place. For example, Dave prepares the list of people to be paid but someone else makes the payment. Or two people have to sign the payroll checks (or authorize on internet banking) before they are released.

Detection Controls: these controls come in after the payroll has been paid. For example, someone different from Dave (i.e. you!) gets the bank statements the following day and you check that the amount that's left the bank account ties back to the sheet of paper that you signed the previous day.

Hopefully you notice that the two amounts are different and you immediately investigate what's happened.

That way, you may not have prevented Dave's bad behaviour but you certainly would have detected it very quickly.

**Why controls fail?**

So, if you could have stopped the fraud happening in the first place (or at least limited it) then why do frauds by the truckload continue to happen?

You can design as many controls as you feel like, but if you forgot to stick with them then you have what are known as "control breakdowns"

The main reason is the human factor.

Or if we weren't being as nice - people are lazy, forgetful, too busy, didn't understand what was needed of them. Whatever the reason - the controls fail.

And in the worst case - fraud - someone deliberately ignores the control.
Big Companies = Big Frauds

Now, take our simple example and then think about a huge multi-national company with numerous processes around how their cash is spent and collected - which could be payroll, invoicing clients, stock control and operating expenses.

Imagine the sheer number of controls that need to be implemented to make sure that all the cash paid out or received is accurate and properly accounted for.

These controls will be a combination of complex computer systems and lots of people. And they can breakdown either unintentionally (system bugs, genuine human error).

Or a person (or a group of persons) can get together and maliciously set out to commit a fraud. That's called collusion.

And if they get away with it....then the numbers can be massive.

So, what is Forensic Accounting?

We're hoping you now have a better understanding of how frauds can be committed in any size of company and the importance of controls.

And we're now also hoping that our definition of Forensic Accounting will make more sense to you.

Forensic Accountants are usually called in after a fraud has already been committed.

The internal controls have failed. Money has been lost. Particularly in large companies it may not be clear (or they may not have a clue!) what happened.

The company needs to find out.

And that's when they call in the accountants, the lawyers, the police and other government organizations if things get really nasty.

And the role of the Forensic Accountants is to:

Investigate and gather evidence. Interview staff

Analyze that information. Review the controls and how they failed. Query the data systems

Work with the lawyers, police and anyone else who's involved from outside the company

Document their findings in a clear and concise format which is delivered to the Company

Prepare further reports/documents that will be used by the Company to launch a legal case against the fraudulent employees.

Appear in court to explain the investigation work that they've carried out and the conclusions they reached.
FORENSIC ACCOUNTANT AND AUDITS

It is important to define the term forensic accountant to ensure readers understand concepts and narratives throughout the book. One of the key points to understand about forensic accountants is the difference and roles of financial audits versus fraud audits. This section will discuss some of the issues and differences.

*Forensic Accounting Defined*

In this book, the term forensic accounting refers to the comprehensive view of fraud investigation. It includes preventing frauds and analyzing antifraud controls. Forensic accounting would include the audit of accounting records in search for evidence of fraud; a fraud audit. A fraud investigation to prove or disprove a fraud would be part of forensic accounting. It also includes the gathering of nonfinancial information, such as interviews of all related parties to a fraud, when applicable. Forensic accounting includes writing a report to management or court. Serving as an expert witness and litigation support are part of forensic accounting.

Although relatively new to the accounting profession, the role of a forensic expert in other professions has been in place for some time. Webster’s Dictionary defines the word forensic as “belonging to, used in, or suitable to courts of judicature or to public discussions and debate.” Accordingly, the term forensic in the accounting profession deals with the relation and application of financial facts to legal problems. Forensic accounting evidence, therefore, is oriented to a court of law.

*Financial Auditors, Fraud Auditors, and Forensic Accountants*

In the lexicon of accounting, terms such as fraud auditing, forensic accounting, fraud examination, fraud investigation, investigative accounting, litigation support, and valuation analysis are not clearly defined. Some distinctions apply between fraud auditing and forensic accounting. Fraud auditing involves a specialized approach and methodology to discern fraud; that is, the auditor is looking for evidence of fraud. The purpose is to prove or disprove a fraud exists. Historically, forensic accountants, however, have been called in after evidence or suspicion of fraud has surfaced through an allegation, complaint, or discovery.

Forensic accountants are experienced, trained, and knowledgeable in all the different processes of fraud investigation including: how to interview people (especially the suspect) effectively, how to write effective reports for clients and courts, how to provide expert testimony in court, and rules of evidence. The ACFE refers to this definition of forensic accounting as fraud examination. In recent years, the broadest of these terms in the antifraud profession is forensic accounting, which typically refers to the incorporation of all the terms...
involved with investigation, including fraud auditing; that is, fraud auditing is a subset of forensic accounting.

Fraud investigation usually encompasses about the same thing as a fraud audit except investigation typically involves a lot more nonfinancial evidence, such as testimony from interviews, than a fraud audit. So fraud investigation includes fraud audit but goes beyond it in gathering nonfinancial forensic evidence.

Litigation support refers to a forensic accountant assisting attorneys in prosecuting or defending a case in the legal system. That support can take on a variety of skills but ultimately is intended to conclude with the forensic accountant offering an opinion in a court of law as an expert witness on whether a fraud occurred.

Analyst [CVA]) has to establish a value on the loss associated with a fraudulent event, whether it is a spouse trying to hide assets in a divorce case, or a customer claiming exorbitant losses in an insurance claim, or a victim entity suffering from a bad merger/acquisition that ended in a bankruptcy of the subsidiary.

Financial auditing is a wholly different term that needs to be distinguished from forensic accounting and fraud auditing. Financial auditing typically refers to the process of evaluating compliance of financial information with regulatory standards, usually for public companies, by an external, independent entity. The well-publicized SOX incorporate concepts and procedures to deter and to catch fraud in audits of internal controls over financial reporting.

However, the focus of financial audits and financial reporting ultimately is concerned with providing reasonable assurance that a material misstatement to financial statements has not occurred, regardless of the reason.

**Financial Auditors**

The term financial auditor broadly applies to any auditor of financial information or the financial reporting process. The largest classification of financial auditors is those who work for public accounting firms and perform audits of financial statements for public companies. This classification is the most commonly used in this book when referring to financial auditors.

Financial auditors have expertise in their knowledge of accounting and financial reporting (such as in generally accepted accounting principles [GAAP], PCAOB standards, or International Financial Reporting Standards [IFRS]), auditing (generally accepted audit standards [GAAS]), and how those standards apply to business transactions. As expressed in the GAAS literature, the most important financial auditing attributes are independence, objectivity, and professional skepticism.

Financial auditors traditionally have been seen as, and to an extent have been, numbers oriented, and their processes have been driven by the audit trail. The financial audit procedures are designed to detect material misstatements, and thus financial auditors focus on
misstatements that singularly or in the aggregate are large enough to be material. Fraud auditors and forensic accountants are not constrained by materiality. The discipline of financial auditing has been thought to be almost a checklist of items to complete.

In reality, judgment is crucial in financial auditing and has progressively increased in the direction of more dependence on auditor judgment. SOX requirements involve auditor judgment to a large degree; auditors are to understand processes significant to financial reporting and to evaluate management’s controls over those processes. Additionally, auditors are to consider environmental, including soft, intangible, factors in that evaluation.

**Fraud Auditors**

Fraud auditors are generally accountants or auditors, who, by virtue of their attitudes, attribute, skills, knowledge, and experience, are experts at detecting and documenting frauds in books of records of accounting and financial transactions and events. Their particular attitudes include these beliefs:

- Fraud is possible even in accounting systems that have tight controls.
- The visible part of a transaction fraud may involve a small amount of money, but the invisible portion can be substantial.
- Red flags of fraud are discernible if one looks long enough and deep enough.
- Fraud perpetrators can come from any level of management or society.

The skills fraud auditors require include all of those that are required of financial auditors, plus the knowledge of how to gather evidence of and document fraud losses for criminal, civil, contractual, and insurance purposes; how to interview third-party witnesses; and how to testify as an expert witness.

Fraud auditors must know what a fraud is from a legal and audit perspective, an environmental perspective, a perpetrator’s perspective, and a cultural perspective. They also need both general and specific kinds of experience. They should have a fair amount of experience in general auditing and fraud auditing, but should have industry-specific experience as well (e.g., banking; insurance; construction; and manufacturing, distribution, and retailing).

Fraud auditing is creating an environment that encourages the detection and prevention of frauds in commercial transactions. In the broadest sense, it is an awareness of many components of fraud, such as the human element, organizational behavior, knowledge of fraud, evidence and standards of proof, an awareness of the potentiality for fraud, and an appreciation of the red flags.

Some of the functions of a fraud auditor follow.
In short, fraud auditing is the process of detecting, preventing, and correcting fraudulent activities. While completely eliminating fraud is the goal, it is simply not feasible. The concept of reasonableness is applicable here, and this concept is often associated with the fraud-related fields of financial accounting and auditing. Fraud auditors should be able to thwart a reasonably preventable fraud.

Accounting-type frauds are usually accompanied by the modification, alteration, destruction, or counterfeiting of accounting evidence. But accounting records can be either intentionally or accidentally modified, altered, or destroyed, by human error or omission. The first objective for the fraud auditor, then, is to determine whether a discrepancy in accounting records is attributable to human error. If it is, there may be no actual fraud. If the discrepancy (missing records, destroyed records, modified records, counterfeit records, errors, omissions) cannot be attributed to accidental or human error, further investigation should follow at an appropriate level.

**Forensic Accountants**

Forensic accountants may appear on the crime scene a little later than fraud auditors, but their major contribution is in translating complex financial transactions and numerical data into terms that ordinary laypersons can understand. That is necessary because if the fraud comes to trial, the jury will be made up of ordinary laypersons. Areas of expertise of forensic accountants are not only in accounting and auditing but in criminal investigation, interviewing, report writing, and testifying as expert witnesses. They must be excellent communicators and professional in demeanor.

The involvement of the forensic accountant is almost always reactive; this distinguishes forensic accountants from fraud auditors, who tend to be actively involved in prevention and detection in a corporate or regulatory in criminal matters, statements of claim arising in civil litigation, and rumors and inquiries arising in corporate investigations. The investigative findings of the forensic accountant will impact an individual and/or a company in terms of their freedom or a financial award or loss. The ACFE refers to this person as a fraud examiner.

The forensic accountant draws on various resources to obtain relevant financial evidence and to interpret and present this evidence in a manner that will assist both parties. Ideally, forensic accounting should allow two parties to more quickly and efficiently resolve the complaint, statement of claim, rumor, or inquiry, or at least reduce the financial element as an area of ongoing debate. Objectivity and independence of the forensic auditor are paramount for these purposes.

**Differences among the Three**

Forensic accountants, fraud auditors, and investigative auditors measure financial transactions in relation to various other authorities, such as the Criminal Code, an insurance contract, institutional policies, or other guidelines for conduct or reporting. The
accountant/auditor prepares the report rather than the client or subject and does not include an opinion on the findings.

In the investigation, one does not reject evidence as being immaterial; indeed, the smallest item can be the largest clue to the truth.

Fraud auditors, forensic accountants, and/or fraud investigators (i.e., all professionals involved with forensic accounting) put things together rather than taking them apart, as is the case in classic financial auditing or the modern method of systems analysis. The process of forensic accounting is also sometimes more intuitive than deductive, although both intuition and deduction play important parts. Financial auditing is more procedural in many regards and is not intended to work as effectively in detecting frauds as the tenets of fraud auditing and forensic accounting.

Q1: How would you distinguish forensic accounting, fraud auditing, and investigative auditing from financial auditing?

A. The distinction is related to one’s goals. Financial auditing attempts to enable the auditor to render an opinion as to whether a set of statements upon which the opinion is rendered are always the representations of management. The auditor is primarily concerned with qualitative values (hence the concept of materiality comes into play) and generally is not concerned about whether the financial statements communicate the policies, intentions, or goals of management.

B. Forensic accounting is a general term used to describe any financial investigation that can result in a legal consequence. Fraud auditing is a specialized discipline within forensic accounting, which investigates a particular criminal activity, namely fraud. Investigative auditing involves reviewing financial documentation for a specific purpose, which could relate to litigation support and insurance claims as well as criminal matters.

C. The objective of financial auditing is to provide the auditor with a degree of assurance in giving an opinion with respect to a company’s financial statements. The materiality level of an investigative auditing engagement is much lower and more focused than that of the normal financial auditing engagement.

Q2: How would you define what you do as a forensic accountant?

A. I think of myself as one who seeks out the truth.

B. I would define my forensic accounting responsibilities as follows:

(1) Investigation and analysis of financial documentation; (2) communication of the findings from my investigation in the form of a report, accounting schedule, and document briefs; and (3) coordination of and assistance in further investigation, including the possibility of appearing in court as an expert witness.
C. My role is that of an objective observer or expert. The final report that is issued as a result of my work will be used to negotiate some sort of settlement, be it financial or be it imprisonment. My role as a forensic accountant extends beyond the particular financial circumstances and seems to be one of an objective individual who provides the buffer between, in civil instances, the client and counsel, and, in criminal instances, the investigator and the prosecutor. Therefore, I am considered an integral member of the team of professionals assigned to any given case. Related to the specific work that I do, it has been described to me, and I agree, that the makeup of a given forensic accountant is one third business person, one-third investigator, and one-third accountant.

Q3: What qualities of mind and/or body should a forensic accountant possess?

A. Creativity: the ability to step out of what would otherwise be a normal business situation and consider alternative interpretations that might not necessarily make business sense; curiosity: the desire to find out what has taken place in a given set of circumstances; perseverance: the ability to push forward even when the circumstances don’t appear to substantiate the particular instance being investigated or when the documentation is very onerous and presents a needle-in-a-haystack scenario; common sense: the ability to maintain a “real-world” perspective; business sense: the ability to understand how businesses actually operate, not how business transactions are recorded; confidence: the ability to believe both in yourself and in your findings so that you can persevere when faced with cross-examination.

B. As with any other pursuit, a healthy mind in a healthy body is a solid foundation. Beyond that, one should have generous proportions of common sense, inquisitiveness, skepticism, and an ability to avoid the natural tendency to prejudice—that is, to be fair and independent.

In addition, because forensic work ultimately can lead to court appearances, good posture, grooming, vocal projection, and stamina can all be valuable attributes.

C. The foremost quality a forensic accountant requires is independence, because a forensic accountant is often forced to balance conflicting opinions about the same piece of documentation. The second major quality is an intense sense of curiosity coupled with a sense of order—a desire to put the puzzle back together.

D. Common sense/street smarts; sensitivity/understanding of human behavior; analytical; logical/clear; ability to simplify complexities and delete jargon; not be prone to lose the forest for the trees; ability to identify and assess alternative explanations and interpretations; ability to quickly assess cost-benefit of pursuing alternative avenues of investigation and reporting contents/formats.

E. The forensic accountant needs to be calm, cool, and collected; have good business judgment; and have a mind that can deal logically with esoteric issues and precise matters. A forensic accountant involved in litigation must be physically fit to withstand the long days and long nights of investigation and preparation for trial and the trial itself.
Forensic accountants need to have a pleasant appearance and demeanor so that they will not be offensive when in the witness box.

Q4: What skills are most important to the successful practice of forensic accounting?

A. Solid technical accounting and financial skills—the basis of your “expertise”; ability to quickly prioritize issues and map out a

“game plan”—good judgment; ability to communicate well—both verbally and in writing—is necessary to obtaining information, directing your staff, presenting your findings, and achieving your desired results. Even the best-planned and executed assignment can fail if you are unable to clearly and concisely present your findings.

B. A forensic accountant needs to be precise, pay attention to detail, and be a broad thinker; that is, not suffer from tunnel vision.

C. When looking at a given forensic accounting engagement, there are two major areas that come to mind in the completion of a given case.

First, there is the investigative aspect, and second, the communication aspect. I feel that investigative skills would include areas such as the ability to assimilate large volumes of information, general organization and administrative skills, use the microcomputer or understand the abilities of the microcomputer, and interpersonal skills.

Communication skills would include the ability to write a comprehensive report understandably.

D. Communications skills: oral/written; interpersonal skills; listening skills; ability to synthesize/integrate; ability to identify/prioritize objectives/issues.

Financial Audit versus Fraud Audit

Many in the public, and some in the U.S. Congress, have questioned why financial auditors do not detect more fraud. The general public believes that a financial auditor would detect a fraud if one were being perpetrated during the financial auditor's audit. The truth, however, is that the procedures for financial audits are designed to detect material misstatements, not immaterial frauds. While it is true that many of the financial statements and frauds could have, perhaps should have, been detected by financial auditors, the vast majority of frauds could not be detected with the GAAS of financial audits. Reasons include the dependence of financial auditors on a sample and the auditors’ reliance on examining the audit trail versus examining the events and activities behind the documents. The latter is simply resource prohibitive in terms of costs and time.

There are some basic differences today between the procedures of fraud auditors and those of financial auditors. Fraud auditors look behind and beyond the transactions and audit trail to
focus on the substance of the transactions instead. The fraud auditor doesn’t question how the accounting system and internal controls stack up against applicable standards but rather:

- Where are the weakest links in this system’s chain of controls?
- What deviations from conventional good accounting practices are possible in this system?
- How are off-line transactions handled, and who can authorize such transactions?
- What would be the simplest way to compromise this system?
- What control features in this system can be bypassed by higher authorities?
- What is the nature of the work environment?

Another difference is the current status of technical guidance combined with research on frauds. Frauds can be divided into three main categories:

Financial frauds are typically perpetrated by executive management and average millions of dollars in losses. According to a recent KPMG Fraud Survey, that average is about $258 million. Generally speaking, therefore, financial frauds are likely to be material, and thus financial audit procedures have the potential to detect them—because they would be a material misstatement, due to a material fraud. However, those who might be responsible for fraud audits internal to the firm could be constrained or thwarted in detecting the fraud because executives are in a position to hide the fraud or misdirect fraud auditors’ efforts. Cynthia Cooper argues that at WorldCom she was thwarted from doing her job as internal auditor, but she eventually did uncover the financial fraud being perpetrated there.

FORENSIC ACCOUNTANTS

The forensic accountant has skills, abilities, and knowledge related to the fraud cycle, including legal resolution. Because of the scope of fraud, the fact that fraud occurs in a lot of different arenas, there are a lot of different groups who could benefit from the services of a forensic accountant.

Who Needs Forensic Accountants?

The increased business complexities in a litigious environment have enhanced the need for the forensic accounting discipline. It is possible to summarize the range of application into the following general areas:

Corporate investigations Companies react to concerns that arise through a number of sources that might suggest possible wrongdoing initiated from within and without the corporate environment. From the anonymous phone call or e-mail from disgruntled employees and third parties, these problems must be addressed quickly and effectively to permit the company to continue to pursue its objectives. More specifically, the forensic
accountant assists in addressing allegations ranging from kickbacks and wrongful dismissals to internal situations involving allegations of management or employee wrongdoing. At times, a forensic accountant can meet with those persons affected by the allegations, rumors, or inquiries; they may view the accountant as an independent and objective party, and thus be more willing to engage in discussion.

**Litigation support** Litigation support includes assisting counsel in investigating and assessing the integrity and amount relating to such areas as loss of profits, construction claims, product liability, shareholder disputes, bankruptcies, and breach of contract. Obviously, litigation support is initiated by an attorney responding to some kind of legal action, whether criminal or civil.

**Criminal matters** Efforts to prevent white-collar crime have consistently used accountants and auditors in attempts to sort out, assess, and report on financial transactions related to allegations against individuals and companies in a variety of situations such as arson, scams, fraud (e.g., kickbacks or embezzlement), vendor frauds, customer frauds, investment scams, and stock market manipulations. In criminal matters, accountants and auditors as expert witnesses are increasingly important in court cases.

**Insurance claims** the preparation and assessment of insurance claims on behalf of the insured and insurers may require the assistance of a forensic accountant to assess both the integrity and the quantum of a claim. The more significant areas relate to the calculation of loss arising from business interruption, fidelity bond, and personal injury matters. Whereas certain of these cases require financial projections, many need historical analysis and other accounting and auditing-oriented services.

**Government/Regulation/Compliance** Forensic accountants can assist entities to achieve regulatory and contractual compliance by ensuring that companies follow the appropriate legislation, law, or contract terms. Grant and subsidy investigations and public inquiries form a part of this service to government.

**Forensic Accountant: Required Knowledge, Skills, and Abilities**

Many of the aspects of forensic accounting fall outside the traditional education, training, and experience of auditors and accountants. The following skills, abilities, and/or knowledge are necessary to serve as an effective forensic accountant:

**Ability to identify frauds with minimal initial information** Many times, the fraud investigation begins with minimal knowledge of the specifics of a potential fraud. The forensic accountant needs to be able to identify the possible scheme (i.e., fraud theory approach), the possible manner it was perpetrated, and potentially effective procedures to prove or disprove the potential fraud (i.e., the “theory”).

**Interviewing** Throughout the course of seeking evidence and information, the forensic accountant becomes involved in interviewing. For the forensic accountant, this function is
another art to master. There are many things about interviewing, including what is the best order in which to interview parties of interest that the forensic accountant must know. Most important, the forensic accountant must be prepared to handle a confession in such a way that the process ensures the evidence is admissible in a court of law.

**Mind-set** One of the critical success factors of forensic accountants, and one of the hardest to define or measure, is mind-set. A successful forensic accountant has a certain mind-set that includes several abilities. He or she is able to think like a crook. This attribute is basically counter to the average auditor who has lived a life with integrity and believes strongly in honesty. The successful forensic accountant knows almost instinctively that something “does not pass the smell test.” He or she is able to sense the anomaly sometimes before actually knowing the nature of the anomaly.

This person has a healthy skepticism at all times, neither fully trusting people nor fully distrusting them. They have a natural tendency to question the substance behind transactions, documents, and testimony (written or oral) that others do not have. They also know, and have, the following mind-set factors:

**Fraud can be detected as well as discovered by accident or tip**

*Financial audit methodologies* and techniques are not really designed to detect fraud but rather designed to detect material financial misstatements.

*Fraud detection* is more of an art than a science. It requires innovative and creative thinking as well as the rigors of science.

*Determination*, persistence, and self-confidence are more important attributes for a fraud auditor than intelligence.

*Logic and problem-solving* and detective skills are critical success factors for fraud auditors and forensic accountants.

*Knowledge of evidence* The forensic accountant must understand what constitutes evidence, the meaning of “best” and “primary” evidence, and the form that various accounting summaries can take to consolidate the financial evidence in a way that is acceptable to the courts. It is imperative that a forensic accountant understand the rules of evidence in court and how to conduct the investigation from the beginning as if all evidence will make it to a court of law. If these rules are ignored, evidence could be compromised and found inadmissible if it does get to court.

*Presentation of findings* The forensic accountant must have the ability to clearly communicate the findings resulting from the investigation in a fashion understandable to the layperson. The presentation can be oral or written and can include the appropriate demonstrative aids. The role of forensic accountants in the witness box is the final test of the findings in a public forum. By its nature, however, accounting and financial information is difficult for the average person to comprehend. Therefore, the forensic accountant as an
expert witness must have above-average communication skills in distilling financial information in a manner that the average citizen can understand, comprehend, and assess to reach a sound conclusion.

**Knowledge of investigative techniques** When the issues have been identified, it is imperative that further information and documentation be acquired to obtain further evidence to assist in either supporting or refuting the allegation or claim. It is a question of knowing not only where the relevant financial documentation exists but also the intricacies of GAAP, financial statement disclosure, and systems of internal control, and being aware of the human element involved in frauds.

**Investigative skills** Forensic accountants usually apply investigative skills at the appropriate time during the course of their investigations. For example, in dealing with criminal matters, the primary concern is to develop evidence around motive, opportunity, and benefit. Of equal concern is that the benefit of doubt is given to the other side to ensure that proper interpretations are given to the transactions. Other concerns, such as the question of method of operation and the issue of economic risk, must also be addressed.

Similarly, investigative skills are needed in litigation support. The forensic accountant must ensure that: a proper foundation exists for the calculation of future lost profits; all assumptions incorporated into the work product are recognized and identified; he understands his limitations as an expert; and the issue of mitigation of damages is considered.

**Investigative mentality** Along with their accounting knowledge, forensic accountants develop an investigative mentality that allows them to go beyond the bounds set out in either GAAP or GAAS. The following three tenets in forensic accounting are driven by the necessity to prove intent in court in order to prove there was a fraud. The investigative mentality develops in the search for best evidence, for competent and sufficient evidence, for forensic evidence. For example:

**Scope is not restricted as a result of materiality.** Often, especially in the early stages of a management/employee fraud, the transactions are small and accordingly are more easily conveyed to the court to show a pattern of conduct that is deceitful. As the dollar value of the transactions and their complexity increase, the ability to convey the essence of the transaction is hampered, and the forensic accountant’s task is made more difficult.

**For the most part,** the use of sampling is not acceptable in establishing evidence.

**A critical element** of corporate investigations in particular is the assumption of integrity by management, both personal statements and its documentation of financial transactions and events.

The investigative mentality is best developed by continued experience as a forensic witness. It is through this process that the forensic accountant’s eyes are opened, because counsel for the opposing side raises issues and possibilities the accountant may not have considered up to that point. Repeated experience as a forensic witness creates a greater awareness of what is
relevant and must be considered, so the expert witness can present financial evidence independently and objectively to reflect the reality of the situation.

**Identification of financial issues** When forensic accountants are presented with a situation generated by a complaint, allegation, rumor, inquiry, or statement of claim, it is important that they clearly identify the financial issues significant to the matter quickly. They base their decisions on experience and knowledge, and any resulting recommendations must reflect both common sense and business reality. For example, if documents are needed from a foreign jurisdiction, although the most obvious recommendation would be to obtain these records, it is usually not practical to do so. Other alternatives must be considered.

**Interpretation of financial information** It is unusual for a transaction or a series of events to have only one interpretation. The forensic accountant must be extremely conscious of a natural bias that can exist in the interpretation process. It is important that transactions be viewed from all aspects to ensure that the ultimate interpretation of the available information fits with common sense and the test of business reality. A proper interpretation of information can be assured only when one has looked behind and beyond the transaction in question without any scope limitations. In particular, a forensic accountant who is called as an expert witness must be aware of alternative accounting or financial formulas, rules, and interpretations.

**FRAUD AUDITORS**

Just as forensic accountant services are needed by a variety of groups, fraud audits also have a number of groups who could potentially benefit from their services, although it is somewhat less in scope than forensic accountants. The scope is less because fraud audits involve only a limited phase of the fraud cycle.

**Who Needs Fraud Auditors?**

The need for fraud-auditing talent is not related solely to compliance with new governmental regulations. In the private sector, fraud-auditing skills are also useful in most cases of financial crime, such as embezzlement; misrepresentations of financial facts; arson for profit; bankruptcy fraud; investment frauds of all manner and description; bank fraud; kickbacks and commercial bribery; frauds; and scams and shams by vendors, suppliers, contractors, and customers.

In the United States, the largest body of trained and experienced fraud auditors comes from government audit and investigative agencies like the Internal Revenue Service (IRS), FBI, Government Accounting Office (GAO), and the SEC. Police authorities on the state and local levels have few audit resources at their disposal; as a consequence, their ability to investigate certain white-collar crimes is limited. There is a need for fraud auditing in both public and private sectors of the economy.
Public accounting firms and other organizations in the private sector are developing fraud audit expertise. Although relatively few public accountants and internal auditors are specifically trained and experienced in this discipline, their numbers are rapidly increasing.

**Fraud Auditor: Required Knowledge, Skills, and Abilities**

More broadly, fraud auditing focuses on creating an environment that encourages the detection, prevention, and correction of intended or executed fraud.

The main thrust of this book is to provide auditors, investigators, and other persons in the fraud environment with the ability to establish and influence forces that effectively counter attempts at fraud. Ability comes from insight, knowledge, and experience in viewing fraud as an economic, social, and organizational phenomenon.

Fraud auditors should know the aspects of the common body of knowledge regarding fraud. That knowledge includes: fraud schemes, red flags and the ones associated with specific frauds, the fraud triangle, fraud research, emerging fraud issues, steps in a fraud investigation, legal aspects of fraud (especially evidence), fraud professional organizations, fraud certifications, behavioral characteristics of white-collar criminals, and so on. The fraud auditor, of course, needs to be able to apply that knowledge in the fraud environment.

The personal attributes of fraud auditors include self-confidence, persistence, commitment to honesty and fair play, creativity, curiosity, an instinct for what is out of place or what is out of balance, independence, objectivity, good posture and grooming (for courtroom testimony), clear communication, sensitivity to human behavior, common sense, and an ability to fit pieces of a puzzle together without force or contrivance.

Inevitably, accounting and investigative (legal) skills cross over and are inextricably tied together in the context of a forensic audit. Although auditors and investigators exhibit similar skills in some ways, when separated they demonstrate different abilities. As for accounting skills, an effective fraud auditor should be able to do the following competently:

**Establish accounting**, audit, and internal control (when, where, and how fraud is most likely to occur in books of account and in financial statements).

**Conduct a review of internal controls**

**Assess the strengths and weaknesses of those controls**

**Design scenarios of potential** fraud losses based on identified weaknesses in internal controls.

**Know how** to identify questionable and exceptional transactions (too high, too low, too often, too rare, too much, too little, odd times, odd places, odd people).

**Identify questionable** and exceptional account balances and variations.
**Distinguish** between simple human errors and omissions in entries and fraudulent entries (intentional error, such as recurring small errors versus unintentional random error and ignorance).

**Know how** to follow the flow of documents that support transactions.

**Follow the flow** of funds in and out of an organization’s account.

**Search for underlying** support documents for questionable transactions.

**Review such documents** for peculiarities like fake billings, destruction of data, improper account classification, irregularities in financial data, and substitution of copies for original documents.

A couple of notes with regard to these skills should be made. One of these is the “toos” and the “odds” method for identifying possibly fraudulent transactions.

Transactions are suspect if they are too high, too low, too often, too rare, too close, at odd times, in odd places, and so forth. A good example of the “too close” idea is the common check fraud perpetrated at a high dollar amount that bypasses the usually necessary high-level approval by paying the amount with multiple checks just under the threshold for (extra) approval. A mid-level accounts payable manager may be able to solely sign checks only for $1,000 and under, but can get $1,998 without additional approval with just two checks of $999 each, just below the approval threshold.
Fraud: An Introduction

INTRODUCTION

Fraud has several potentially ambiguous definitions, and is categorized in various ways. A proper understanding of these definitions and models is fundamental to preventing and detecting fraud. The fraud principles are the building blocks of an effective antifraud program, or of effective prevention and early detection of fraud.

First, it is important to establish a definition for fraud both for the profession and for an entity devising an antifraud program. It is good to be reminded of the possibility of fraud in order to avoid the “it-can’t-happen here” syndrome. Understanding effective models such as the fraud triangle is useful in understanding why fraud occurs. There are numerous classification models (taxonomies) for fraud schemes, but it is important to pick one that can be effectively applied in fraud prevention and early detection.

Lastly, an understanding of the profile of the white-collar criminal is helpful as well.

DEFINITION: WHAT IS FRAUD?

Fraud means different things to different people under different circumstances.

For instance, fraud can be perceived as deception. One might say that fraud in the form of intentional deception (including lying and cheating) is the opposite of truth, justice, fairness, and equity. Although deception can be intended to coerce people to act against their own self-interest, deception can also be used for one’s own defense or survival. Despite that rationale for deception, deception by current standards of behavior is generally considered mean and culpable, but deception can be intended for a benevolent purpose, too.

Benevolent deceivers in society are not looked on as harshly as are those whose intentions and motives are impure. Those who act out of greed, jealousy, spite, and revenge are not so quickly excused or forgiven.

Fraud can also be associated with injury. One person can injure another either by force or through fraud. The use of force to cause bodily injury is frowned on by most organized societies; using fraud to cause financial injury to another does not always carry the same degree of stigma or punishment.

Fraud is a word that has many definitions. Some of the more notable ones are:

**Fraud as a crime** Fraud is a generic term, and embraces all the multifarious means that human ingenuity can devise, which are resorted to by one individual, to get an advantage by false means or representations. No definite and invariable rule can be laid down as a general proposition in defining fraud, as it includes surprise, trick, cunning, and unfair ways by which another is cheated. The only boundaries defining it are those that limit human knavery.
Corporate fraud Corporate fraud is any fraud perpetrated by, for, or against a business corporation.

Management fraud Management fraud is the intentional misrepresentation of corporate or unit performance levels perpetrated by employees serving in management roles who seek to benefit from such frauds in terms of promotions, bonuses or other economic incentives, and status symbols.

Layperson’s definition of fraud as it is commonly understood today means dishonesty in the form of an intentional deception or a willful misrepresentation of a material fact. Lying, the willful telling of an untruth, and cheating, the gaining of an unfair or unjust advantage over another, could be used to further define the word fraud because these two words denote intention or willingness to deceive.

Specific Frauds and Categories

As stated earlier, fraud is intentional deception. Its forms are generally referred to as lying and cheating. But theft by guile (larceny by trick, false pretenses, and false tokens) and embezzlement sometimes are included as fraudulent acts. The element of deception is the common ground they all share. But fraud and deception are abstract terms. They go by many other names as well. For example, in alphabetical order, they might be called:

- Accounts payable fabrication
- Accounts receivable lapping
- Arson for profit
- Bank fraud
- Bankruptcy fraud
- Benefit claims fraud
- Bid rigging
- Breach of fiduciary duty
- Breach of trust
- Business opportunity fraud
- Bust out
- Cash lapping
- Check forgery
- Check kiting
✓ Check raising
✓ Collateral forgery
✓ Commercial bribery
✓ Computer fraud
✓ Concealment
✓ Consumer fraud
✓ Conversion
✓ Corporate fraud
✓ Corruption
✓ Counterfeiting
✓ Credit card fraud
✓ Defalcation
✓ Distortion of fact
✓ Double dealing
✓ Duplicity
✓ Electronic funds transfer fraud
✓ Embezzlement
✓ Expense account fraud
✓ False advertising
✓ False and misleading statement
✓ False claim
✓ False collateral
✓ False count
✓ False data
✓ False identity
✓ False information
✓ False ownership
✓ False pretenses
✓ False report
✓ False representation
✓ False suggestion
✓ False valuation
✓ False weights and measures
✓ Fictitious customer
✓ Fictitious employees
✓ Fictitious person
✓ Fictitious vendors
✓ Financial fraud
✓ Financial misrepresentation
✓ Forged documents
✓ Forged signatures
✓ Forgery
✓ Franchising fraud
✓ Fraud in execution
✓ Fraud in inducement
✓ Fraudulent concealment
✓ Fraudulent financial statement
✓ Fraudulent representation
✓ Industrial espionage
✓ Infringement of copyrights
✓ Infringement of patents
✓ Infringement of trademarks
✓ Input scam
✓ Insider trading
✓ Insurance fraud
✓ Inventory overstatement
✓ Inventory reclassification fraud
✓ Investor fraud
✓ Kickback
✓ Land fraud
✓ Lapping
✓ Larceny by trick
✓ Loan fraud
✓ Lying
✓ Mail fraud
✓ Management fraud
✓ Material misstatement
✓ Material omission
✓ Misapplication
✓ Misappropriation
✓ Misfeasance
✓ Misrepresentation
✓ Oil and gas scams
✓ Output scams
✓ Overbilling
✓ Overstatement of revenue
# Root causes of Typical Fraud

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Opportunity</td>
<td>Knowledge and opportunity to commit the fraud. Fraudster holds a position of trust, has tenure, and/or access to records or assets. Control weaknesses, lack of audit trail, lack of segregation of duties, no internal audit function, weak culture</td>
</tr>
<tr>
<td>2</td>
<td>Rationalization</td>
<td>Mentally juxtapose the crime against personal code of ethics to formulate intent without self-incrimination; e.g., “just borrowing the money,” entitlement</td>
</tr>
<tr>
<td>3</td>
<td>Commit The fraud</td>
<td>the fraud Execute a particular scheme, usually the fraud escalates as time goes by and fraud goes undetected—larger amounts or add more schemes</td>
</tr>
<tr>
<td>4</td>
<td>Convert asset to cash</td>
<td>Convert asset to cash If necessary (not necessary if already cash), an official check is same as cash, sell inventory at reduced prices in a “black market”-type venue; financial statement fraud leads to stock options, which leads to cash out of stock</td>
</tr>
<tr>
<td>5</td>
<td>Conceal the crime</td>
<td>Conceal the crime If necessary (not necessary if no one looking! Or if off the-books fraud), false refunds/credits, use large volume accounts, rely on apathy, alter documents, destroy documents</td>
</tr>
<tr>
<td>6</td>
<td>Red flags</td>
<td>Red flags In the process of commit, convert, and conceal, fingerprints are left that are known as “red flags”; behavioral red flags could be a lifestyle change—true even for off-the-books frauds; transactional red flags are missing data or anomalies (e.g., unfavorable variances, unusual increases)</td>
</tr>
<tr>
<td>7</td>
<td>Suspicion or discovery</td>
<td>Suspicion or discovery Tip, discovery of variance or anomaly including a sufficient analysis, discrepancies, internal controls, internal audit, external audit, accident</td>
</tr>
<tr>
<td>8</td>
<td>Predication determined Before a fraud</td>
<td>Predication determined Before a fraud investigation can begin, predication has to be determined to exist; a fraud professional believes a fraud has occurred, is occurring, or will occur because of circumstances</td>
</tr>
<tr>
<td>9</td>
<td>Fraud theory</td>
<td>Fraud theory Unless the specific fraud is known, the fraud theory approach helps to identify the most</td>
</tr>
<tr>
<td></td>
<td>likely schemes and how they are being perpetrated</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Fraud investigation</td>
<td>Fraud investigation Identify and gather forensic evidence, loss of assets confirmed, loss documented, interrogations performed, nonfinancial evidence acquired</td>
</tr>
<tr>
<td>11</td>
<td>Write a report</td>
<td>Write a report Almost all fraud investigations require a report at its conclusion, whether to victim’s management, insurance company, or court officials/lawyers</td>
</tr>
<tr>
<td>12</td>
<td>Disposition:</td>
<td>Disposition: Termination Most often, the victim company extricates itself from the fraudster employee and hopes that ends the episode, employee terminated for cause, where possible insurance claim is filed to recover some or all of the losses</td>
</tr>
<tr>
<td>13</td>
<td>Disposition:</td>
<td>Disposition: Prosecution Either criminal or civil prosecution is sought by the victim entity, prosecuting entities may not even take the case, and may not successfully prosecute the case</td>
</tr>
<tr>
<td>14</td>
<td>Trial</td>
<td>Trial Presentation of facts and testimony before trier of fact, use of expert witness, presentation of forensic evidence</td>
</tr>
</tbody>
</table>
FRAUD DETECTION AXIOMS

There are several axioms concerning fraud detection that are important to remember when designing an antifraud program or activities. A key to fraud detection is to remember that frauds are more often associated with the absence of controls rather than weak controls; that is, a weak control is generally better than none. They are also more often detected by reactive measures rather than proactive ones; thus there is a lot of room for improvement. There is an overreliance on external audit to detect fraud. Lastly, frauds are often detected by intuition, suspicion of investigators, managers, auditors, or an exception (anomaly) detected in the accounting records. However, frauds are most often detected by proven detection methods. This chapter is devoted to proven means of early detection of fraud.

COMMON DETECTION METHODS

Periodically, the Association of Certified Fraud Examiners (ACFE) conducts a study on frauds resolved in the previous 12 to 18 months and reports the statistics to the public in the form of a report entitled Report to the Nation (RTTN). The ACFE has issued a RTTN in 1996, 2002, 2004, 2006, and 2008. In each RTTN, the statistics show the more common detection methods. In all years, the most common detection method has been tips. In some years, tips accounted for about twice as much in percentage of detection as whatever method ranked second. In all years, the least effective detection method, other than law enforcement, is external audit. It is therefore not logical to rely primarily on external audit for an entity’s detection method yet that is exactly what most entities that experience frauds are doing; the 2008 RTTN shows external audit as the most popular control employed by the victim entities (almost 70 percent of the entities were using external audit, 61.5 percent a code of conduct, 55.8 percent internal audit).

Notably, the least frequently employed controls by fraud victims are those listed as the most effective; that is, fraud victims have their controls upside down.

This control information is a valuable source of knowledge in detecting frauds.

Effective General Methods

The ACFE’s RTTN classifies fraud controls by efficiency to detect or prevent fraud. Specifically, the 2008 RTTN asked respondents to identify which fraud countermeasures were in place when the fraud being reported was discovered, as well as the amount of the loss. Then a simple ratio depicting fraud loss reduction was calculated on each countermeasure, antifraud control, based on whether that control was in place (‘‘yes’’) or not (‘‘no’’), and the average loss for each of the two groups.
It depicts the analysis of the controls along with the ratio, which shows surprise audits as the most effective antifraud control, if measured in its ability to reduce the amount of losses incurred. It is followed by job rotation/mandatory vacation, anonymous hotlines (tips and complaints), employee support programs, fraud training for managers and executives, internal audit or fraud examination department, and fraud training for employees. Each of these controls reduced losses by at least 50 percent. Many of these methods would be considered detective controls, and would be useful in deploying antifraud controls that can provide early detection.

**Other General Methods**

Methods can be developed for frauds in general, or specific groups of frauds (e.g., a category), or even individual schemes. Some methods that could be used for general detection, regardless of the scheme, are:

- Internal audit function actively engaged in proactive antifraud activities
- Sarbanes-Oxley Act (SOX) section 404 results can lead to identification of weaknesses in internal controls that can cause a higher risk for fraud in that area or business process
- Horizontal and vertical analysis of financial reports, especially when comparisons are made between business units and their data
- Ratio analysis, especially trends over several years, and by business unit compared to other units and the entity as a whole
- Surprise audits and/or cash counts
- Anonymous tips and complaints system to which employees, vendors, and customers have access; comfortable, convenient, easy to use
- Data mining for applicable red flags using Computer-Assisted Auditing
- Tools (CAAT).

**SPECIFIC DETECTION METHODS**

This section describes some detection methods that are designed to detect specific schemes or groups of schemes rather than fraud in general.

**Financial Statement Schemes**

- Financial auditors’ application of SAS No. 99
- Horizontal and vertical analysis of financial reports
- Ratio analysis, especially trends over several years
✓ Beneish’s five earnings manipulation ratios (see Appendix 7A)

✓ Examination of generally accepted accounting principles (GAAP) tax rate versus cash tax rate

✓ Irrational price-to-earnings ratios: benchmark is 20 to 25, S&P average is about 36

✓ An audit committee that meets SOX requirements and is actively engaged in an antifraud program, especially in holding executives accountable

✓ Running background checks on executives

✓ External auditors maintaining a professional skepticism on every client

Asset Misappropriation Schemes

✓ Sending the bank statements to a person in the entity separate from accounts payable and any check-writing personnel, and having that person review the statement and cancelled checks, then forward them to the person responsible for the bank reconciliation

✓ Rotating duties or mandating vacation for key employees

✓ Examining all types of transactions that have a review/approval level, extracting all transactions just below that level, and classifying them by employee, vendor, and customer

✓ Reconciling inventory and confirming receivables regularly

Cash Larceny

✓ Investigating shortages in cash drawers, deposits, registers

✓ Investigating missing or altered sales records

✓ Having two people independently verify deposits on bank statements to postings in the general ledger

✓ Maintaining and reviewing daily cash availability amounts Having deposits delivered to the bank under dual control

✓ Secretly determining the deposit prior to its transmittal to the bank and then independently confirming with the bank the amount of the deposit

✓ Making sure deposits in transit are the first to clear on the next statement (flag associated with lapping deposits)

✓ Conducting surprise cash counts

✓ Reviewing cash and check ratio of daily bank deposits (for those who steal only cash)
✓ Reviewing timeliness of deposits from remote locations to central treasurer function
✓ Observing cash receipting at all points of entry

Billing Schemes
✓ Shell Company
✓ Sorting payments by vendor, amount, and invoice number
✓ Expense exceeds budget, especially if it is exactly double (i.e., possibly producing two checks, one for the legitimate vendor, and one for the fraudster)
✓ Examining charges in largest expense account, as fraudsters often charge billing schemes to the largest account in an attempt to hide the crime
✓ Horizontal analysis
✓ Verifying service-only vendors’ invoices
✓ Using a CAAT software tool to cross-reference employees’ addresses with vendors’ addresses
✓ Testing for turnaround time from receipt of invoice to payment
✓ Verifying that vendors are legitimate. While this test may appear daunting, it can become manageable by verifying only the vendors added since last audit and only ones specific to the applicable business unit. Look them up in the phone book or in the online white pages. Use Google to search for the firm. Check with the local chamber of commerce. Contact others in the same industry.
✓ Reviewing cancelled checks
✓ Not paying a suspicious invoice/vendor and seeing who follows up on payment
✓ Taking special precaution with those employees who can add a vendor to the authorized list (segregate that duty if possible from invoice approval)
✓ Data mining for as many of the red flags as possible Verifying the legitimacy of any vendor who uses Excel-generated invoices
✓ Printing the vendor list alphabetically and searching for two vendors with nearly identical names and data

Pass-Through Vendor
✓ Examining all invoices just below the approval level, sorted by vendor or employee who approved the invoice
✓ Comparing market prices for prices on invoices, using a CAAT and some research
✓ Reviewing invoices for what is being bought and the prices

No accomplice Vendor

✓ Sorting invoices by vendor and looking for unusual invoice numbers
✓ Classifying vendor by invoice amounts and looking for unusual amounts
✓ Verifying invoices that led to vendor refunds
✓ Requesting that the bank notify the proper person if someone endorses a check where the company is the payee, and use the stamp ‘‘For Deposit
✓ Only’’ for all endorsements

Personal Purchases

✓ Spot-checking expenditures on credit cards, looking for unusual vendors or items bought
✓ Surprise audits of employees who are authorized to use credit cards or sign checks
✓ Examining unfavorable balances on performance reports
✓ Vendor payment trend analysis
✓ Extracting all purchases with no purchase order, summarized by both vendor and employee
✓ Extracting all purchases just below the review/approval limit, summarized by both vendor and employee

Payroll Schemes

✓ Ghost Employee
✓ Where feasible, reconciling employees in the payroll database with
✓ employees in the human resource (HR) database; the ghost should be
✓ missing in HR
✓ Getting a copy of the Social Security number (SSN) file and, at least once a
✓ year, reconciling that file with your employees’ SSNs
✓ Periodically and unannounced, distributing checks manually, requiring ID
✓ to pick up check
✓ Investigating any payroll checks with dual endorsements (a sign that an
employee accomplice is working with a real person who is serving as the ghost

Rotating duties of handling printed paychecks, or requiring vacation timed with issuance of paychecks (pay day)

Data mining payroll data looking for these red flags:

Post office box versus a physical address

Physical address matches that of another employee (i.e., a “duplicate”)

Direct deposit account number that matches that of another employee

Missing phone number, or a phone number that matches either another employee or a work phone

Dates of paychecks compared to termination dates (employees being paid after terminated, and used as a ghost by an existing employee)

**Commissions**

Randomly spot checking all of the transactions involved in sales commissions for a pay period or a salesperson

Investigating higher rates of returns or credits for a salesperson

Creating and reviewing a linear correlation between sales and commission paid, by employee

Tracking uncollected sales by employee

Creating exception reports for employees whose compensation has increased over last year by some unusual percentage

Having a designated and independent official verify all changes in commission rates

**Falsified Wages**

Data mining all transactions over a certain number of overtime hours (e.g., more than 20 hours per week)

Creating exception reports for employees whose compensation has increased over last year by some unusual percentage

Randomly verifying the pay rates in a pay period or for an employee over pay periods

Having a designated and independent official verify all changes in pay rates

Maintaining careful custody of time cards—after approval, process them immediately
Check-Tampering

- Periodically rotating personnel who handle and code checks
- Requiring dual signatures for checks over a designated threshold
- Using a positive pay system at the entity’s bank
- Having the bank statement sent unopened to someone in management completely separate from accounts payable—in the case of smaller companies, perhaps the owner/manager. Review the statement and cancelled checks, even if it is online, before passing the statement on to the person who will do the bank reconciliation.

Skimming

Skimming frauds happen before a booking entry is made. Because it is an off the-books fraud, this type of fraud is one of the most difficult to detect. One methodology to detect skimming is to perform invigilation. Individual skimming schemes are related to sales (unrecorded sales, understated sales), receivables (write-off schemes, lapping schemes, unconcealed schemes), and refunds. Suggested methods to use for this type of scheme are:

- Surveillance of employees at point of sale (e.g., cameras above registers and meal tables)
- Discovery of ‘‘markers’’ near registers (fraudsters use markers to keep up with the amounts skimmed; for example, a penny for $100, a nickel for $500)
- Investigating gaps in pre numbered receipts
- Checking registers for excessive no-sale transactions, voids, or refunds
- Posting a sign at the register or in plain view of customers: “If you did not receive a receipt, please contact the manager and your meal will be free.” Using a trained secret shopper to look for signs of fraud
- Using an invigilation for an approximation of missing monies, or to determine if skimming is occurring
- Measuring variances in revenues by employee and by shift Creating a pro forma income statement, using cost of goods sold an standard markups to ascertain the level of sales that should exist, then comparing it to actual for an approximation of missing monies

Corruption Schemes

- Classifying transactions by vendor and examining unusual, unexplained
- higher-than-expected volumes
✓ Random investigation of all vendors, including owners, major shareholders, and any relationship with employees
✓ Reviewing contracts and approval of invoices periodically, even if only a sample during each audit
✓ Verifying the authenticity of vendors as part of internal audits, even if it is only a sample
✓ Looking for related-party transactions where the relationship has been hidden
✓ Reviewing approvals for transactions with related parties annually

Bribery and Economic Extortion

✓ Rotating duties of approving contracts and/or vendors, and bid responsibilities
✓ Segregating duties of approving vendors and awarding contracts or approving invoices
Financial Statements Analysis

What Is Financial Statement Analysis?

Financial statement analysis compares ratios and trends calculated from data found on financial statements. Financial ratios allow you to compare your business' performance to industry averages or to specific competitors. These comparisons help identify financial strengths and weaknesses.

Financial Ratios


Profitability Ratios

Profitability ratios measure profit realized from different financial sources. They are the profit margin, return on assets and return on equity. To calculate any of these ratios, divide net income by sales, total assets or stockholders' equity, respectively.

Asset Utilization Ratios

Asset utilization ratios determine how efficiently a company's assets are managed. These ratios are receivables turnover, average collection period, inventory turnover, fixed asset turnover and total asset turnover. Except for the average collection period, all of the above ratios are calculated by dividing sales by the asset category named in the ratio title.

Liquidity Ratios

Liquidity ratios measure what amount of assets can be immediately converted to cash. These ratios are often used along with cash flow statements to determine a company's ability to pay its creditors. Liquidity ratios are the current and the quick ratio -- current assets and quick assets divided by current liabilities.

Debt Utilization Ratios

Like asset utilization ratios, debt-utilization ratios measure how efficiently a company uses its debt. These ratios are debt to total assets, times interest earned and fixed charge coverage. Debt to total assets is calculated as it is stated, while the others are a little different -- income before interest and taxes divided by interest and income before fixed charges and taxes divided by fixed charges.
Trend Analysis

Trend analysis lets you compare companies’ performances over specific periods of time. For example, over five years, managers can compare how their profit margin has improved or worsened. Complete analysis must also include industry standards.

Financial Statement Analysis Limitations

Financial analysis is an important part of small business management. Business owners often review financial information to ensure their business is generating enough capital to pay for expenses and provide the owner with a profit. While many different types of financial analysis exist in the business environment, financial statement analysis is a common management tool. Financial statement analysis usually involves a personal review by the business owner.

Facts

Financial statement analysis usually includes quantitative and qualitative reviews by business owners. A quantitative review includes the use of various financial ratios. These ratios measure the company ability to meet short-term financial obligations, profitability of goods or services sold to consumers, use of financial assets to generate income and other information. The qualitative review uses personal judgment or inferences when making decisions based on the information.

Financial Ratio Limitations

Financial ratios provide a limited analysis of the company financial statements. These ratios calculate numerical indicators or percentage values based on the financial information contained in the statements. However, these indicators mean very little if not compared to a competing business or an industry standard. Small business owners may find it difficult to compare their information to another company with similar business operations or financial obligations.

Qualitative Review Limitations

Business owners using qualitative analysis on financial statements may be limiting their reviews to the final output of financial information. While financial statements usually indicate how much profit the company has generated during a certain accounting period, financial statements typically do not provide enough information about the efficiency of business operations. Small businesses often can turn a profit even though too much money was spent on generating this income.

Considerations

Small business owners with a limited knowledge of accounting or financial analysis may be unable to properly analyze their operations. Business owners also may create financial
statements that do not accurately reflect the company’s financial situation. Analyzing financial statements with incorrect information can distort the owner’s understanding and decision-making process. Incorrect financial statements also distort the company’s historical financial information, creating a difficult process for measuring business trends.

Expert Insight

Public accounting firms or individual certified public accountants, or CPAs, provide small businesses with information on setting up and analyzing financial statements. Small business owners can use these professional accountants for preparing their business tax returns. Professional accountants help small business owners avoid significant financial mistakes when recording and reporting the business financial information. Business owners also may use these individuals advice when making business decisions.

Introduction to Financial Statement Analysis

Financial statement analysis is a common technique that allows small business owners to review their company operational performance. Small business owners will need to create financial statements from their company business transactions before conducting a financial statement analysis. Financial statements represent an aggregate total of the company’s business information during a certain time period.

Types

Business owners can use two types of financial statement analysis: quantitative and qualitative. Quantitative analysis uses formulas or ratios to break down the company’s financial statements into indicators. These indicators provide business owners with benchmarks to compare the company’s information against the industry standard. Qualitative analysis involves business owners using personal judgment or inferences when reviewing financial statement information. Business owners use quantitative or qualitative analysis to make decisions regarding business operations.

Quantitative Analysis Features

Quantitative analysis features different financial ratios for analyzing financial statement information. Ratios include liquidity, asset turnover, financial leverage and profitability. Liquidity ratios indicate how well the business can meet short-term financial obligations. Asset turnover ratios provide information on the company’s ability to use assets when generating sales. Financial leverage ratios determine the long-term solvency of the business. Profitability ratios help business owners calculate the amount of profit from consumer goods or services.
Qualitative Analysis Features

Businesses conduct qualitative analysis by comparing several financial statements at one time. This financial statement review process commonly is called a horizontal or trend analysis. Business owners can prepare a single document containing the current month’s financial statement and that of several previous months. Reviewing individual accounts or line items can help business owners discover trends in company operations relating to sales, cost of goods sold or expenses.

Considerations

A computerized accounting system is useful in conducting financial statement analysis, and several inexpensive accounting software programs exist. Users can customize accounting software for capturing a company’s business information according to pre-programmed directives. A computerized system also can limit calculation errors made by business owners when reviewing financial statement information.

Misconceptions

Financial statement analysis is not always the best management tool for measuring a company’s performance. Although financial statement analysis may indicate positive performance indicators, other issues may exist in the company. Business owners also should review production output, employee productivity and other internal business functions to avoid a myopic business decision-making process.

Financial Statement Analysis for Managers

There isn’t just one best method for evaluating business performance. Every business may differ slightly in operation, environment and methodology, which leaves many trial and error opportunities. Financial statement analysis provides a primary foundation for evaluating business performance and adapts to every business. All owners and managers should be skilled in analyzing financial statements to understand the impact business decisions will have on the organization.

Cost-Volume-Profit

Cost-volume-profit analysis provides owners and managers with an understanding of the relationship between fixed and variable costs, volume of products manufactured or sold and the profit resulting from sales. The financial relationship includes contribution margin analysis, break-even analysis and operational leverage. Financial statements provide the data to perform cost-volume-profit analysis.

Contribution Margin

Contribution margin analysis allows managers to look at the percentage of each sales dollar remaining after payment of variable costs, including cost of goods, commissions and delivery charges. Managers and owners use this analysis to help determine the pricing, mix,
introduction and removal of products. Contribution margin analysis also aids managers with determining how much incentive to use for sales commissions and bonuses. Comparing each product offered affords the opportunity to look at product profitability and product mix.

**Break-even**

Break-even analysis considers the sales volume at which fixed and variable costs are even. Owners and managers must consider two primary figures when calculating the break-even. First, gross profit margin, which is the percentage of sales remaining after payment of variable costs.

**Operational Leverage**

Every business model contains slightly different operating leverage, which compares the amount of fixed costs to sales. Businesses with higher fixed costs will experience a larger multiplier in their operating leverage, indicating less sales growth results in more profit. However, the same is true for losses, where small reductions in sales exponentially increase net losses. Less operating leverage results in less growth of net income.

**Financial Ratios**

A financial ratio expresses a mathematical relationship between two or more sets of financial statement data and commonly exhibits the relationship as a percentage. Profitability, solvency, leverage, asset turnover and liquidity comprise the five standard ratio categories. Managers and owners should review the ratios period over period, determining where unfavorable trends exist. After reviewing trends, benchmark ratios against industry standards, which managers can acquire from a variety of sources including industry-specific organizations and the Risk Management Association, or RMA.

**Financial Statement Analysis Tools**

Financial statements are usually the final output of a company accounting operations. These statements contain information relating to the revenues, expenses, assets, liabilities and retained earnings of the business. Business owners often pay close attention to this information since the statements can provide detailed information about the company operational performance. Many business owners and managers use specific analysis tools to closely review their company financial statements for decision-making purposes.

**Financial Ratios**

A traditional financial statement analysis tool is financial ratios. These ratios take information from the company financial statements and calculate economic indicators for comparison to another company or the industry standard. Financial ratios include liquidity, asset turnover, financial leverage and profitability calculations. Liquidity ratios calculate the company ability to meet short-term financial obligations. Asset turnover ratios indicate how well the company uses its assets to generate profits. Financial leverage ratios calculate the long-term solvency
of a company. Profitability ratios help companies determine how much profit they are generating from the sale of various goods or services.

**Horizontal Analysis**

A horizontal financial statement analysis compares current financial statements to previous year financial information. Companies often conduct this analysis by putting several years of financial statements in a side-by-side comparison format. This enables business owners and managers to review the same month over several years to determine if revenues, expenses, assets or liabilities have increased, decreased or stayed the same. Companies can also use a horizontal analysis to compare changes in dollar amounts or a percentage change when comparing financial statements.

**Vertical Analysis**

A vertical financial statement analysis is conducted using common size financial statements. A common size financial statement shows each item on a financial statement in a percentage figure for each statement line item. A vertical analysis gives managers a different option for reviewing financial information; managers may be more comfortable looking at percentages rather than dollar amounts. The percentage figure represents how individual line-item amounts compare to the aggregate total of the financial statements. For example: business owners or managers may wish to know what percentage office supplies were out of the total expenses reported on May income statement. A common size statement would divide May total office supplies expense by the total expenses listed on May income statement. This percentage is then listed where the office supplies expense amount would be on the financial statement.

**Trend Percentage Analysis**

A trend percentage analysis is an enhanced horizontal analysis technique. Trend percentage analyses help companies identify consistent revenues or expenses from past accounting periods. These trends can help managers make business decisions regarding future operations. Companies will use a specific financial statement as a base year for comparing all future financial statements. Changes for each future time period are expressed as a percentage when compared to the base financial statement. Companies can conduct a trend percentage analysis at various times of the year or use different financial statements as the base during this comparison process.

**Advantages of a Financial Statement Analysis**

To meet their financial reporting obligations and to assist in strategic decision-making, firms prepare financial statements. However, “the information provided in the financial statements is not an end in itself as no meaningful conclusions can be drawn from these statements alone.” Firms employ financial analysts to read, compare and interpret the data as necessary for quantitative analysis and decision-making.
**Definition**

Properly comparing a balance sheet with the corresponding profit and loss account to determine the strengths and weaknesses of a business describes financial statement analysis. “In a technical sense, financial statements summarize the accounting process and provide a tabulation of account titles and amounts of money,” reports Reference for Business. Financial statements help communicate what financial decisions have been made and how they affect the bottom line.

**Significance**

Financial analysis determines a company's health and stability. The data gives you an intuitive understanding of how the company conducts business. Stockholders can find out how management employs resources and whether they use them properly. Governments and regulatory authorities use financial statements to determine the legality of a company's fiscal decisions and whether the firm is following correct accounting procedures. Finally, government agencies, such as the Internal Revenue Service, use financial statement analysis to decide the correct taxation for the company.

**Liquidity**

The balance sheet provides liquidity rations that show how much monetary worth the company has on a given day, which helps determine if the firm’s financial reliability. The current ratio shows “the 'working capital' relationship of current assets available to meet the company's current obligations,” reports Credit Guru. The quick ratio is similar, calculating those assets easily convertible into cash, determining the immediate working capital relationship. The debt to equity ratio establishes who owns more of the company, creditors or shareholders.

**Efficiency**

Efficiency ratios measure how efficiently the company turns inventory into revenue. The day sales outstanding ratio focuses on the time required to turn inventory into cash and the age of your accounts receivable. The inventory turnover ratio “indicated the rapidity with which the company is able to move its merchandise,” reports Credit Guru. Accounts payable to sales shows the percentage of sales funded with supplier's money.

**Profitability**

Profitability ratios reveal a firm's success at generating profits. “The profit margin of a company determines its ability to withstand competition and adverse conditions,” reports Credit Guru. Return on assets, reveals the profits earned for each dollar of assets and measures the company's efficiency at creating profit returns on assets. Net worth focuses on financial returns generated by the owner's invested capital.
Limits

It is important to know that financial statement analysis has limits; simply manipulating numbers hides the actual state of the company. Different accounting methods will look different on paper, and the method a particular firm uses can change the visible health and profit levels for either better or worse. Quantitative financial analysis is an art, and different analysts may get slightly different results from the same information, or may return different data about the same business.

Financial Statement Fraud: Detecting the Red Flags

Important: The red flags of financial statement fraud are distinctly different from those of asset misappropriation. Common general red flags of financial statement fraud:

• Accounting anomalies.

• Unusually rapid revenue and/or profit growth.

• Readily noticeable internal control weaknesses.

• Noticeably “aggressive” financial actions by senior management.

• Personality or character flaws of the CEO and/or other “C-level” executives.

PERSONALITY ALERT

Important: Of these general indicators, top management personality and character are by far the most compelling with regard to financial statement fraud. Typically, a senior executive who is inclined to “cook the books” possesses low ethical standards, though this trait may often be difficult to detect prior to the commission of a crime. However, most executives with ethical weaknesses also exhibit very noticeable signs of aggressiveness in almost everything they do—including making critical financial decisions. Examples:

• Overly domineering, disrespectful or abusive management style vis-à-vis subordinates.

• Actively “steering” internal and external auditors away from financial reports that could reveal the fraud.

• Secretive or distinctly evasive attitude regarding critical financial information.

Detection methods for general financial statement frauds:

• Internal audit is consistently engaged in substantive anti-fraud activities.

• Auditors aggressively apply standards of SAS No. 99.

• Frequent and thorough fraud-oriented ratio analysis—focusing in particular on long-term trends and on comparisons between business units.
• Surprise audits and/or cash counts.

• Implementation of an anonymous, user-friendly tip hotline for use by employees, vendors and customers.

• Data mining using one of the common auditing software applications such as ACL or IDEA.

SPECIFIC RED FLAGS

As with asset misappropriation, there are also specific red flags of financial statement fraud that are present in many of the common varieties of such accounting violations. Examples:

• Complex or unstable organizational structure.
• Unusually intricate or confusing financial transactions with third-party entities.
• Sudden or gradual increase in gross margin compared with the company’s prior performance, and with industry averages.
• Cash flows that is negative for the first three quarters and suddenly positive for the fourth quarter—not by just a little, but by more than all losses to date. (This scenario is exactly what happened at Enron. It is why Sherron Watkins said, after the company’s demise, that if anyone had been paying attention to the cash flows they would have known that Enron's statements were suspicious and/or fraudulent.)
• Significant sales to companies or individuals whose identity and business track record are questionable.
• Sudden above-average profits for specific quarters.
• Executives or board members have direct personal dependence on the company’s performance.
• Conspicuously lax board oversight of top management.

FRAUD CATEGORIES

Also similar to asset misappropriation, financial statement fraud has distinct categories. Each has its unique red flags and detection methods. Examples…

• Revenue recognition or timing schemes—also known as improper treatment of sales. This fraud category is possibly the most common form of financial statement fraud—usually employed when management seeks to conceal the real numbers for a weak quarter or two. Red flags:
  • If a sale is legitimate, but is posted prematurely, the red flag would be a GAAP violation by early recording of the sale. Similarly, channel stuffing—where sales are recorded before they’ve actually been made—would be indicated by an excessive number of subsequent period returns of merchandise, accompanied by an unusual jump in credits.
Fictitious revenue. One of the oldest financial statement schemes around—this involves posting sales that simply never occurred. Red flags:

- Unusual increase in assets—the other side of the entry to mask fictitious revenues.
- “Customer” records are missing key data such as physical address and phone number.
- Unusual changes in ratio patterns—such as a spike in revenues with no commensurate increase in accounts receivable.

Concealed liabilities. (improper or under-reporting of expenses and other liabilities). By shifting expenses from one entity to another or reclassifying liabilities as assets, which is what got WorldCom into trouble when it improperly reported $3.8 billion in expenses as capital expenditures, management can make the company’s financial condition appear much rosier than it is. Red flags:

- Use of different audit firms for different subsidiaries or business entities.
- Recurring negative cash flows from operations or an inability to generate cash flows from operations while reporting earnings growth.
- Invoices and other liabilities go unrecorded in the company’s financial records.
- Writing off loans to executives or other parties.
- Failure to record warranty-related liabilities.

Inadequate disclosures. This tactic is used after a financial statement fraud has occurred—in an attempt to cover it up. Red flags:

- Disclosure notes are so complex that it is impossible to determine the actual nature of the event or transaction.
- Discovery of undisclosed legal contingencies.

Improper asset valuation. Fraudulently inflating asset valuations is a common form of profit manipulation. Red flags:

- Unusual or unexplained increases in the book value of assets such as inventory, receivables, long-term assets, etc.
- Odd patterns in relationships of assets to other components of the financial report, such as sudden changes in the ratio of receivables to revenues.
- GAAP violations in recording expenses as assets.

DETECTION METHODS...

To reduce the risk of having these frauds occur—or continue undetected—auditors should use such practices as:

- Horizontally and vertically analyzing all financial reports.
- Conducting frequent ratio analysis, including assessment of trends over periods of several years.
- Using Bonefish’s Ratios which pinpoint anomalies in year-to-year measures of gross margins, sales growth, receivables levels and other key accounting ratios.
- Rigorously applying the guidance of SAS 99 to all audit exercises.
Schemes, red flags and questions to ask

While the opportunity for misstatement exists on each line of every financial statement, a handful of culprits account for the majority of cases. It is incumbent upon managers to be familiar with these culprits and know which red flags might indicate their presence. Of course, red flags are not surefire signs of fraud. Rather, they are signs that questions need to be asked and that reasonable answers need to be found.

To help managers know when to raise eyebrows and start asking questions, the Association of Certified Fraud Examiners has developed a list of common accounting fraud schemes and associated red flags. More details are available in the ACFE’s publication Fraud and the CPA: Understanding Why Employees Commit Fraud. the ACFE’s schemes and red flags are listed below, along with a series of questions that managers should ask when the red flags appear.

Overstating revenues

Starting literally at the top of an income statement is always a good idea. Overstating or improperly recognizing revenues is a common form of financial statement fraud.

Schemes

- Recording gross, rather than net, revenue
- Recording revenues of other companies when acting as a “middleman”
- Recording sales that never took place
- Recording future sales in the current period
- Recording sales of products that are out on consignment

Red flags

- Increased revenues without a corresponding increase in cash flow, especially over time
- Significant, unusual or highly complex transactions, particularly those that are closed near the end of a financial reporting period
- Unusual growth in the number of days’ sales in receivables
- Strong revenue growth when peer companies are experiencing weak sales

Questions to ask

Why did revenues increase sharply during the end of the period compared with prior-year and current-year results and the budget forecast?

- How does revenue growth compare with that of peers during the same period? If substantially higher, does the explanation make sense?
• Did receivables increase due to a particular customer? If so, should a reserve be established?

**Understating expenses**

Another common number-fudging technique is understating expenses, which leads to increased operating income and net income.

**Schemes**

• Reporting cost of sales as a no operating expense so it does not negatively affect gross margin
• Capitalizing operating expenses, recording them as assets on the balance sheet instead of as expenses on the income statement
• Not recording some expenses at all, or not recording expenses in the proper period

**Red flags**

• Unusual increases in income or income in excess of industry peers
• Significant unexplained increases in fixed assets
• Recurring negative cash flows from operations while reporting earnings and earnings growth
• Allowances for sales returns, warranty claims, etc., that are shrinking in percentage terms or are otherwise out of line with those of industry peers

**Questions to ask**

• Why did gross margin (by location, product and geographic area) increase during yearend or period-end compared with the prior year\ and current-year budget forecast?
  ✓ Does the explanation make sense?
  • How does the company compare to competitors in terms of net income during the same time period?
  • What were the major additions to fixed assets during the year? Is the treatment of recording assets consistent with that of prior years?

**Improper asset valuations**

Highly publicized asset write-downs following the disclosure of faulty reserve reports should make all company managers pay special attention to how they report their most important hard assets.

**Schemes**
• Manipulating reserves
• Changing useful lives of assets
• Failing to take a write-down when needed
• Manipulating estimates of fair market value

Red flags

• Recurring negative cash flows from operations while reporting earnings and earnings growth
• Significant declines in customer demand and increasing business failures in either the industry or the overall economy
• Assets, liabilities, revenues or expenses based on significant estimates that involve subjective judgments or uncertainties that are difficult to corroborate

Questions to ask

• How is the overall economy affecting customer demand and business? Declines in both could be a signal that there might be an asset impairment issue involving inventory or allowance reserves.
• For areas where there are significant estimates, what is the method used to determine the estimate?
• Is this method consistent with that of prior periods?
• What supporting documentation is available to support the calculation?

Other common areas for financial statement fraud

The following are also schemes used frequently to “cook the books” and make results look better than they really are.

Schemes

Smoothing of earnings: • Often referred to as using “cookie jar reserves,” this involves overestimating liabilities during “good “periods and storing away funds for future use against declining revenues

• Disclosing information improperly, especially concerning related-party transactions and loans to management
• Executing highly complex transactions, particularly those dealing with structured finance, special-purpose entities and off-balance sheet structures, and unusual counterparties

Red flags

• Domineering management
• Decision to “fix” accounting in the next period
• No apparent business purpose
• “Reality” of transaction differs from accounting or tax result
• Significant related-party transactions
• Counterparts that lack economic substance
• Multiple memos rationalizing an aggressive accounting treatment

Questions to ask

• Is there an overly aggressive push by management to meet previously disclosed revenues or earnings targets?
• Can management explain the business purpose for entities that are outside the consolidated financial statements?
• Were there significant adjustments made at the end of the period?
• Has there been an unusual focus on achieving a certain accounting treatment?
• Does the business purpose make sense?
• Does the preferred accounting treatment allow the company to meet certain targets?
• Has there been a change in the method of calculating the reserve estimates for any item from that used in the prior quarter or prior years? If so, why?

When fraud is suspected

Ideally, questions that are prompted by red flags will result in answers that make perfect sense. But when they don’t, it’s time to consider two actions: notifying the audit committee and calling in the forensic accountants.

Forensic accountants are the crime scene investigators of the financial world. They have extensive experience examining the DNA of financial statements; sifting through email records, documents and data entries; and conducting extensive interviews to uncover and explain the most complex financial statement fraud. They are also trained to uncover and preserve evidence to make it admissible in court should the need arise.

When engaging forensic accountants, it is important to consider three qualifications.

The first is forensic accounting experience.

The abundance of corporate scandals in the last few years has created a forensic accounting boom, and many accountants with backgrounds other than forensics have established themselves as forensic accountants. It is important for companies seeking the help of forensic accountants to find out how long they have been practicing forensic accounting and whether the personnel who will be examining potential red flags have appropriate credentials. The second qualification is industry experience. A forensic accountant fluent in financial statements for a manufacturing or retail company might be lost trying to navigate the engineering and geophysical components of an investigation into the possible overstatement of oil and gas reserves.
The third qualification is the breadth of services offered by the accounting firm and its global reach. While a forensic accounting specialty shop might be able to conduct a solid, professional investigation of a small matter, it may not be able to address the issues that led to the fraud in the first place — issues like inadequate financial controls, insufficient or nonexistent processes or weak information technology infrastructure and security. A full-service firm, on the other hand, can move from a fraud investigation to the fraud prevention initiative that should follow. For energy companies operating internationally, use of a firm that can operate seamlessly on a global basis is critical to make certain that all elements of activity can be included in the investigation.
Evidence Created By Forensic Accountant

What does a Forensic Accountant do?

A Forensic Accountant is often retained to analyze, interpret, summarize and present complex financial and business related issues in a manner which is both understandable and properly supported.

Forensic Accountants can be engaged in public practice or employed by insurance companies, banks, police forces, government agencies and other organizations.

A Forensic Accountant is often involved in the following:

- Investigating and analyzing financial evidence;
- Developing computerized applications to assist in the analysis and presentation of financial evidence;
- Communicating their findings in the form of reports, exhibits and collections of documents; and
- Assisting in legal proceedings, including testifying in court as an expert witness and preparing visual aids to support trial evidence.

In order to properly perform these services a Forensic Accountant must be familiar with legal concepts and procedures. In addition, a Forensic Accountant must be able to identify substance over form when dealing with an issue
How can a Forensic Accountant be of assistance?

A Forensic Accountant can be of assistance in various ways, including:

**Investigative Accounting**

- Review of the factual situation and provision of suggestions regarding possible courses of action.
- Assistance with the protection and recovery of assets.
- Co-ordination of other experts, including:
  - Private investigators;
  - Forensic document examiners;
  - Consulting engineers.
- Assistance with the recovery of assets by way of civil action or criminal prosecution.

**Litigation Support**

- Assistance in obtaining documentation necessary to support or refute a claim.
- Review of the relevant documentation to form an initial assessment of the case and identify areas of loss.
- Assistance with Examination for Discovery including the formulation of questions to be asked regarding the financial evidence.
- Attendance at the Examination for Discovery to review the testimony, assist with understanding the financial issues and to formulate additional questions to be asked.
- Review of the opposing expert's damages report and reporting on both the strengths and weaknesses of the positions taken.
- Assistance with settlement discussions and negotiations.
- Attendance at trial to hear the testimony of the opposing expert and to provide assistance with cross-examination.
Who retains a Forensic Accountant?

Forensic Accountants are often retained by the following groups:

- Lawyers;
- Police Forces;
- Insurance Companies;
- Government Regulatory Bodies and Agencies;
- Banks;
- Courts; and
- Business Community

What should I consider when retaining a Forensic Accountant?

The following issues should be considered on retaining a Forensic Accountant:

- The experience and qualifications of the Forensic Accountant;
- A Forensic Accountant should be retained as early as possible in order to obtain maximum benefit. The assistance that a Forensic Accountant can provide early in the process can be significant in reducing the overall cost and maximizing the benefit. If retained early, a Forensic Accountant can assist with the Examination for Discovery, identify additional areas of damages, assist with settlement negotiations and provide a preliminary assessment of the quantum of damages;
- If a Forensic Accountant is engaged as an expert witness then he or she should be given access to all of the relevant documentation. If restrictions are imposed upon the scope of the investigation there may be an impact upon the acceptance of the findings; and
- In situations where counsel is involved, the Forensic Accountant should be retained by counsel so that the privilege which exists between the client and counsel will be extended to the work product of the Forensic Accountant.
Digital Evidence Importance:

Digital evidence or electronic evidence is any probative information stored or transmitted in digital form that a party to a court case may use at trial.

The process of handling digital evidence or electronic evidence must be conducted in a forensically sound manner to ensure court admissibility.

We are experts in IRS forensic accounting with specialized knowledge and training in IRS digital evidence and examination of that evidence.

Digital evidence or electronic evidence is having a profound effect on the future practice of law, as standards for obtaining managing and using information gathered through this process continue to be established.

While many courts have applied the Federal Rules of Evidence some courts notice that digital evidence or electronic tends to be more voluminous, more difficult to destroy, easily modified, easily duplicated, more expressive and more available and sometimes treat digital evidence or electronic evidence differently for purposes of authentication, hearsay, the best evidence rule, and privilege.

In December 2006, strict new rules were enacted within the Federal Rules of Civil Procedure requiring the preservation and disclosure of electronically stored evidence. However, a more comprehensive foundation is required. The American Law Reports lists a number of ways to establish the comprehensive foundation and suggests the proponent demonstrate:

- The reliability of the computer equipment
- The manner in which the basic data was initially entered
- The measures taken to insure the accuracy of the data as entered
- The method of storing the data and the precautions taken to prevent its loss
- The reliability of the computer programs used to process the data
- The measures taken to verify the accuracy of the program

Digital evidence and electronic evidence will continue to be a critical element of all types of legal matters as well as non legal.

Forensic Accountants are trained to examine massive amounts of evidence and question seemingly benign documents. Forensic Accountants look behind the facade and do not accept the records at their face value because the documents may not be what they appear to be.
Your questions are important to us. It only takes a minute to call and ease your mind.

**About Evidence in Forensic Accounting**

Forensic accounting is the science of finding evidence using investigative and accounting practices together. The goal in all forensic accounting cases is the evidence, so it is most important topic of discussion when talking about forensic accounting. It is this evidence that lawyers and government officials rely on for very important and high profile cases. Learn more about the evidence that forensic accountants are looking for and how they obtain it.

**Methods**

- Forensic accountants have several methods they use to find evidence. What these professionals do is find statistical correlation between numerical data found in paper and electronic documents. One technique that has been used, and proven successful in the past is Link Discovery (LD). This is when the forensic accountant use statistical and practical tasks to develop deterministic graphical evidence. Using Bayesian probabilistic and other techniques, investigators are able to find hidden links amongst documents to put together to form evidence. A new approach has been raved about is the Hybrid Evidence Correlation (HEC). Still relatively new, this technique uses first-order logic with probabilistic semantic inference to find suspicious patterns that aren't easily noticed.

**Benefits**

- The evidence forensic accountants find are beneficial in criminal and civil courts. Evidence can either prove or disprove the presence of wrongdoing. After combing through thousands of transactions and finding patterns or links, forensic accounts put their finding in reports and charts. These reports and charts accompany the correlated documentation to create evidence that would be allowed in court. This evidence can be used to solve shareholder disputes, find employee fraud, assist in matrimonial disputes, determine damages and losses in insurance claims and help litigation in obtaining a conviction.

**Process**

- While conducting an audit, a forensic accountant has only one goal in mind; to find evidence of fraud. Their job is to look for fraud; it is what they were hired to do. In order to do this, they follow certain procedures to complete their task. The first thing that they must do is to meet with the client. Most people that hire forensic accountants are business owners, lawyers or government officials. After the meeting, the forensic accountant starts to collect records--credit card statements, journals, bank statements, databases, emails, memos and ledgers are all types of records that are considered as records. Not only do they go over the records with the intent on discovering fraud, but they also conduct interviews just like any other type of investigator. They thoroughly go over the information they have (interview taps and records) to find holes in it.
Then they decipher patterns and find hidden links between the documentation and interviews. After completing the investigation, the client is presented with a report that verifies whether fraud was committed or not.

**Warning**

- The evidence that is collected by forensic accountants is valued and fragile information. The reality is that the evidence is only as valid as the investigator that collected it. Because of this, forensic accountants must adhere to the same laws as police detectives during an investigation. The information is sensitive and the reputations of everyone involved are at jeopardy. The forensic accountant must protect the rights of everyone by being discreet during and after the investigation. If the evidence was collected illegally, or individuals feel as if their rights were violated, the forensic accountant will have to face the repercussions and the evidence will be discredited, thus making it useless in court.

**PROVING CASES THROUGH DOCUMENTARY EVIDENCE**

We prove all cases through evidence. In general, we divide evidence into two categories—direct and circumstantial. In addition to these two categories of evidence, we classify evidence according to its nature. For example, we classify actual witness testimony on the stand in open court as testimonial evidence.

The statements that you obtained during your investigation are documentary evidence, as are canceled checks, bank statements, and photographs of suspect transactions. Additionally, since hundreds of canceled checks are often difficult to comprehend as they sit in piles, attorneys prepare charts and schedules to assist jurors in understanding the big picture. We call these schedules and charts demonstrative evidence. Finally, we refer to physical objects, like guns, knives, and fingerprints, as real evidence. It is through these different classes of evidence that attorneys prove that something did or did not occur.

The difference between financial crimes and nonfinancial crimes is the composition of the evidence. Prosecutors often use real evidence such as fingerprints and tool-mark comparisons to prove crimes such as murder and burglary. Sometimes, documentary evidence like pawn receipts and photographs become important in these cases, but generally, they are non document-based cases. Conversely, financial crimes are very document heavy.

Because of this difference, investigators must often confront huge volumes of evidence. In the typical murder investigation, more than 500 pieces of evidence would be considered exceptionally high. Conversely, in major financial crimes, 500 individual pieces of evidence would be much more common.

For example, the number of canceled checks belonging to a single account for a single year could easily exceed 500.
As we proceed through this chapter, we will prepare you to deal with this unique aspect of financial crime investigation. As we begin, we will focus on the basics of document collection. From consensual searches, to subpoenas, to search warrants, you will be exposed to the various methods of securing documentary evidence. At the same time, we will offer some tips on what types of documents you might expect to encounter.

Next, we will offer some guidance on organizing your efforts. Because you are likely to encounter an unmanageable number of documents in your investigation, a system for organizing and collating them is very important. In the next section, we will offer a framework and some tips for creating an evidence tracking system that will serve you well regardless of the size of the investigation.

Finally, we will discuss how to prove your case. Using the framework of logic and inference, we will explain how you can apply the organizational techniques you developed in the first two sections to prove cases. Marshalling the evidence toward proving one ultimate thesis—guilt—is an art; becoming good at it requires you first understand the process of legal proof.

**DOCUMENT COLLECTION**

All cases require submission of the best evidence. The term best evidence does not refer to the most appropriate piece of evidence for a particular claim. Instead, it means that all evidence submitted to prove a claim must be the original.

1. Where the original is not available, the offering party must generally offer both evidence to show why it is unavailable and proof that the offered copy is accurate.
2. There are some exceptions to this rule; however, it is wise to view it as being inflexible.

This rule is of particular importance to financial crime investigators. When attempting to prove that suspect “A” killed the victim by shooting him, production and introduction of the actual gun is usually a given. Conversely, when seeking to prove that CFO “A” embezzled money from the pension fund, introducing copies of bank statements and other documents might appeal to prosecutors. While under certain circumstances courts will allow this, proper collection and submission of the original is usually required.

Therefore, proper handling of documents from the very beginning is your primary concern. From the moment documents come into your possession, regardless of how they were obtained, you will be ultimately responsible for their safekeeping and for their production. If you take the necessary precautions beforehand, this responsibility should be a simple matter to fulfill.

**Sources of Documents**

Although you will probably find documentary evidence in a number of locations, we have decided to divide them into three categories. First, you will obtain documents from the victims of the financial crime. Whether it is an investor swindled out of his pension or the multinational conglomerate that lost a million dollars, this is usually the first place you will
look for documentary evidence. Next, you will seek to obtain records and documentary evidence from third parties. Finally, you will probably attempt to collect evidence from the suspect herself.

Collecting your documentary evidence in that order is usually advisable. As with everything we have discussed up to this point, when and from whom you first seek to collect evidence may vary depending on the operational circumstances; however, we have found that this logical sequence usually works very well.

Documents from the Victim As soon as you receive the complaint or allegation, you should begin collecting documentary evidence. When you meet with the complainant, she will probably have some documentation available to substantiate her claim. If she does, collect it. While you may be tempted to instruct the complainant to hold onto the evidence until you make a more clear determination of viability, this could be problematic later on. Although it is rare, documents sometimes get lost. If you allow the victim to hold on to the evidence and she misplaces, or worse, destroys it, the basis for your case may be gone. Likewise, there is the remote possibility that the original reporting party was complicit, but for some reason chose to initiate a complaint—perhaps to divert suspicion. If you allow the complaining witness to retain the evidence, destruction is possible if she later becomes a suspect.

Finally, even if the complaining witness is not involved, the suspect may have accomplices in the company who have access to the documents. If so, removal, alteration or destruction is a real danger.

Make copies and issue receipts. Sometimes, the complainant may be reluctant to release the documents. This is often the case with sensitive financial data or trade secret information. Nonetheless, it is important that you explain to the victim the need for proper evidence handling procedures so that the court system can bring the guilty party to justice. Assure the victim that your evidence handling procedures are as secure as or better than his own; then make the appropriate copies for his files and issue him itemized receipts for everything you take.

Be meticulous in your paperwork. While we have seen cases in which the investigator who collected documents took shortcuts and got away with it, do not test the limits of your liability insurance coverage. When the task of collecting hundreds of documents at a time confronts you, the natural inclination is to list groups of documents in bulk and lump everything together. Not only does this make identification of specific documents difficult, it could trigger liability when the victim claims she released the company’s most valuable trade secret to you and you cannot disprove it. The best advice is to take the time and list everything.

At the very minimum, you should leave with a statement. Even when the complainant has no documentary evidence to back the claim, you can still leave with something. Request that
complaining witness complete a written, signed statement. By doing this, you are establishing a basis for investigation as well as protecting yourself from future confusion. If the complaining witness recants, for whatever reason, you have something to verify the nature of the original complaint. Likewise, if the original witness is unavailable in the future, the statement, while unlikely to be admissible in court, can serve as a reference in her absence. Finally, even if the witness does not recant, she may alter her story or forget pertinent details. If you have them in writing, from the beginning, you have lost no ground.

**TYPES OF DOCUMENTS TO EXPECT**

- **Signed statements.** Besides the original complainant, you should anticipate taking written statements from all witnesses at the victim business.

  These documents, while not substitutes for the actual testimonial evidence that the witnesses will offer later at trial, can serve as your outline of their likely trial testimony. In addition, the same cautions regarding complainant statements apply here.

- **Transactional paperwork.** This is another place where your pre investigation planning will benefit you. Each business victim you encounter is likely to operate in a different manner. While most businesses have the same general flow of paper documents, there will be differences. Always be on the lookout for paperwork generated by the business that documents the various transactions that occur within its business cycle. Invoices, payment vouchers, and other original records of transactions are invaluable for tracking the flow of money.

- **Intranet sources.** In today’s business world, more and more companies are establishing intranets that connect all employees and departments together.

  While this is a boon for productivity, it can also be a boon for you. Pay particular attention to chat facilities, weblogs, and other semipublic areas where suspects and witnesses may both lurk. While transactional information may not be available through these sources, they are often the unofficial communications channel in a firm. Background information, rumor, and gossip might prove to be a valuable place to begin looking for other clues.

- **E-mails.** Again, the rise of the company intranet and the growth of computer based operations in business can be a boon to investigators. One area that has received considerable attention from the legal community recently is e-mail communications. Lawyers have quickly realized the value of e-mail communications, and more than one e-mail message has served as the smoking gun in civil cases. Many people treat e-mail correspondence with surprising flippancy considering the longevity of most messages on the corporate server. Their carelessness can be your windfall.

Even though this list is not exhaustive, it is a good place to begin. As we mentioned, the record-keeping systems and paper trails generated will differ from business to business.
However, preplanning and intelligence gathering should serve as a guide to knowing exactly what you are looking for. Whether the suspect religiously uses e-mail, or simply sends out traditional paper memos, both can be valuable sources of evidence. The key is remaining flexible, and tailoring your search to the specific circumstances of each business.

Documents from Third Parties As a rule, in financial crime investigations the majority of documentary evidence you collect will come from third-party sources. In order for a financial criminal to be successful, he or she must interact with the traditional business world. They must deposit money into banks, secure the advice of financial and legal professionals, and generally, engage in the same type of conduct that noncriminal do. As a result, third parties become a very valuable source of information. Banks, accountants, and business and government organizations all have the potential to provide key pieces of evidence linking the suspect to the crime.

Remember, the diverse nature of business means that many different sources exist. Every business has a particular pattern of activity, and each has a circle of influence. In some cases, the contacts a business has may be limited to financial professionals. In other cases, their contacts will extend well beyond the financial sector into the community. Either way, keep in mind that the diversity of contacts the business has may dictate where you may find potentially incriminating documents.

Notwithstanding this diversity, we believe that a suspect’s contacts can be broken down into five basic categories. First, the business or suspect will undoubtedly have contacts in the financial sector. These contacts can include banks, brokerage houses, and insurance professionals. Second, the suspect may have contacts within the professional community including lawyers and accountants. Third, the suspect will have industry contacts such as business organizations, associations, and networking groups. Fourth, there will be contact between the suspect and the government, and finally, every suspect will have personal contacts, which, while not necessarily integral to the suspect’s illegal activities, may still be a valuable source of information.

Because of the diversity we discussed earlier, instead of discussing the various sources of documents individually, we will address them by category. We will offer you some basic guidance about what you may expect to find, and we may even offer some tips about particular documents that are available.

However, in terms of tailoring your search, we will leave you to your own devices, since there are, as we mentioned, an endless number of permutations of the information that you are likely to find.

**FINANCIAL CONTACTS** Banks are often a great place to begin. Most criminals, if not all, will need to have some contact with organized financial institutions.

Whether they need a simple checking account, or utilize the full panoply of financial services most banks now provide, there will be paper trails from which you can construct a picture.
Access to some bank records may be restricted. For example, Currency Transaction Reports (CTRs) and other Bank Secrecy Act documents are a much lesser extent local and state criminal investigators, will be limited in their ability to use these powerful tools. On the other hand, there are many bank and bank-related documents that civil investigators can obtain through civil summons and pretrial discovery tools. Likewise local and state law enforcement investigators can obtain the majority of these documents through investigative and grand jury subpoenas and search warrants.

Do not overlook the non-obvious clues that banking records can reveal.

Some inexperienced investigators may be tempted to focus immediately on the value that bank records have in proving income, or even documenting payments to business associates. As experience grows, an investigator will routinely find that bank records are valuable for many more things.

In addition to explicit information like amounts of cash flows, bank records hold metadata. Investigators loosely define metadata as a component of data that describes data: in other words, data about data. The metadata of a bank record set then is the data surrounding the transactions and their origin. For example, an item deposited into the suspect’s account is more than an increase in cash. On the contrary, we can extract much more than that. By examining the date, time, teller information, and format of the transaction, we can extrapolate many important clues.

Taken together, metadata can establish our pattern of activity. By analyzing, either digitally or manually, all the transactions, we can build patterns that can give direction to the investigations. These patterns may lead us to other associates, or other assets, or even allow us to make predictions about future illegal acts.

The metadata generated by each transaction can help reconstruct a suspect’s movement. In addition to American Banking Association routing numbers, each check that goes through the clearing process collects additional clues. For example, during a counter transaction the teller will stamp the check with a unique transaction code, a time, date, and the teller’s information. Each of these codes may differ from bank to bank, but the bottom line is that each transaction is uniquely identifiable to a particular point in time. Included among these numbers are clues to the disposition of the funds and, in the case of deposits, the source of the funds. Exhibit 10.1 shows an example of some of this metadata.

As you begin to evaluate banking transactions, it may be helpful to remember that there are essentially two categories of transactions. The first category, flow-through, is transactions that relate to the holder’s account. For example, deposits, withdrawals, and debit/credit memos are all considered flow-through transactions. The second category encompasses the remainder of the banking transactions you are likely to encounter and we refer to them as non account transactions, since they are not directly tied to a holder’s account.
Some of examples of common no-account transactions are loans, CD transactions (excluding conversions of CD proceeds into an account deposit), third-party transactions, and safety deposit box transactions.

In order to extract the metadata necessary to formulate a hypothesis, it is also important to understand the basic progression of a flow-through transaction.

Exhibit 10.2 shows the flow of an average transaction through the system.

Although you will often encounter loan files, securities statements, and other, no-account documentation, the greater portion of your analysis will involve flow-through transactions. Each transaction flows in generally the same way. First, there must be a transaction entry point. Usually, this is a window transaction where a suspect presents either an item for deposit or a draft for withdrawal, but it could just as easily take some other form such as an ATM or point of sale (POS) transaction. From the transaction entry point, the items proceed to the proof department where the teller’s mathematical calculations are checked and the items are encoded with the bank’s discrete identification numbers and the transaction-specific MICR information. From the proof department the transaction items are transferred to the microfilm department where all items are recorded and entered into the bank’s computer system.

From the microfilm department, the bank separates the transactions and then sends them to different departments for clearing.

Clearing is where the money changes hands. Depending on whether the transaction is an in-house transaction, meaning the item is presented against the institution on which the claim is held, or an outside transaction, the process may be more or less complicated. However, the general purpose of the clearing process is to ensure that at the end there is an exchange of claims between the payer and the payee. In the case of an in-house transaction, where the payer and payee institutions are the same, the transaction data are sent to the in house clearing department, and then on to the bookkeeping department where the customer records are updated.

If the transaction involves a local institution, the bank sends the transaction items to the local clearinghouse. When the parties to the transaction are local, usually within the same city, and the payer and payee institutions are not the same, the transaction items go to the local clearing department. These local checks are then usually cleared through the Fed wire funds transfer system or the Clearing House for Interbank Payments System (CHIPS).

**PROFESSIONAL CONTACTS** You should always interview professionals with whom the suspect has dealt. Attorneys are not known for their liberality when it comes to discussing their clients. Even so, there are occasions when a lawyer may be both forthcoming and enlightening. Notwithstanding the attorney–client privilege and work product doctrines, there are matters within the knowledge of an attorney that they may in fact be able to tell you. While these times will be rare indeed, it is important to leave no stone unturned.
In addition, the attorney’s fellow professional, the accountant, is often a much more fruitful target. In many jurisdictions, the accountant–client relationship falls outside the privileged information doctrine. As a result, you absolutely must question accountants, and if necessary compel them to produce all written documents pertaining to the client. The following is a list of a few of the documents that may be in the possession of your suspect’s accountant:

- Working papers; these often identify sources of income, expenditures, hidden accounts, and loans.

- Corporate minutes and other corporate documents leading to the identification of shell companies.

In short, nearly any financial document within the control of your suspect might also be available through his accountant. Rely on the meticulous recordkeeping nature of most public accountants to provide a source of evidence.

Real estate professionals may also have records. Both real estate agents and title companies may have copies of contracts identifying real property that your suspect owns. Likewise, real estate and title companies commonly retain copies of insurance documents, settlement sheets, and copies of financial instruments used in consummating the transaction. These documents will show buyer/seller information as well as price, down payment, and the distribution of money at closing. Additionally, do not overlook the possibility that the real estate agent may be acting as a property manager. In the event the suspect retained the realtor in such a capacity, the realtor will have copies of items such as leases and tenant information.

**INDUSTRY CONTACTS** Industry organizations can provide information to which you may compare your suspect. Most industry-based organizations maintain vast amounts of marketing and sales information for their industry.

While the data they have will not likely be specific to your suspect, it may be valuable in determining things such as actual sales, expenses, and COGS. By obtaining the proper industry information, you can arm yourself with a yardstick by which to measure both the timing and amount of cash flows in the suspect’s account. For example, while an association of video retailers will not have the specific number of monthly rentals your suspect transacted, they can tell you what the industry average is. In some cases, their information is specific to each region or city. Armed with that information, you are prepared to spot overstated revenues when examining your suspect’s books.

Persons with whom the suspect does business have records, too. Both suppliers and customers will have transaction records documenting their relationship with the suspect. The nature of the relationship, frequency of contact, and general cooperativeness of the third party may determine the value of the documentation to the investigation. Do not overlook it. In some instances, you must take care to avoid eliminating a vendor/customer as a suspect too early in the investigation. Assuming the business contact is legitimate, there are a number of
documents of value in their possession. For example, purchase orders and invoices are a great way to disprove claimed sales figures or expenses.

Likewise, unusual timing of invoices and unusually generous credit terms may tend to establish less-than-arm’s-length transactions and sham asset transfers. Do not hesitate to seek support for the vendor’s documentation.

For example, just because the suspect’s supplier produces a paid invoice for 3,000 pizza boxes do not mean the transaction actually occurred. Backup data should exist in the vendor’s file as well, indicating the depletion of inventory, reorder, and similar activities.

Sometimes what you do not see is just as important as what you do. As we said, information from invoices and purchase orders could be great evidence; however, do not overlook the ramifications of no evidence. If the suspect’s office supply account reflects $35,000 in purchases over the course of the year, and the supplier of record has no invoices reflecting such purchases, you have just proven that the suspect inflated the business expenses—a manipulation often used by local money launderers.

**THE LOGIC OF ARGUMENT**

**Deductive Argument**

Deductive reasoning is a form of argument that works from the general to the more specific; we often refer to this as “top-down” logic. Inductive reasoning, on the other hand, works from specific observations to the broader and more general; we sometimes call this “bottom-up” reasoning.

An argument stated deductively offers two or more rules or assertions that lead automatically to a conclusion. This syllogistic form of argument, first propounded by Aristotle, is designed to produce mathematical certainty. The use of syllogisms, or mathematical statements, ensures that the lines of argument lead logically to the conclusion.

A deductive argument has, at a minimum, three statements: the major premise, the minor premise, and the conclusion. The first statement, or the major premise, is a statement of general truth dealing with categories rather than finite objects. Contained within the major premise are two sections: the antecedent and the consequent.

The antecedent phrase is the subject phrase, and the consequent phrase is the predicate. For example, the statement “all men are mortal” contains the antecedent phrase, “all men” (the general category), and the consequent phrase, “are mortal.”

The second statement, the minor premise, is a statement about a specific instance encompassed by the major premise. For example, the phrase, “Socrates is a man,” is a statement of truth dealing with a specific instance governed by the major premise.
The third statement, the conclusion, must follow naturally from the relationship of the major and minor premises to one another. If no deductive fallacies exist, this statement will be the inescapable result of the first two statements. In the above example, “Socrates is mortal” is the natural and inescapable conclusion to the major and minor premise.

In forming deductive arguments, we can relate the minor premise to the major premise in four different ways. Only two produce sound logical arguments; the other two produce deductive fallacies.

The structure in our illustration is an example of affirming the antecedent.

In this form, the minor premise asserts that a particular instance is an example of the major premise’s antecedent. In our example, we are asserting that Socrates is indeed a man. We are affirming that Socrates and the state of being a man are equal.

We refer to the converse of this form as denying the consequent. In order to construct a deductive syllogism in which we deny the consequent, we must assert that a particular instance does not equal the consequent. Our major premise, “all men are mortal,” may remain the same. However, the minor premise must change.

If, instead of asserting that Socrates is a man, as we did in affirming the antecedent form, we deny that a specific object is mortal—“my car is not mortal”—we have constructed the second

**Inductive Argument**

In contrast to the mathematical precision of deductive reasoning, inductive reasoning is not designed to produce certainty. This form of logical argument uses a series of observations in order to reach a conclusion. We combine these observations, often referred to as a chain of observations, with previous observations to reach a defensible conclusion.

Of the three basic forms of inductive reasoning, induction by enumeration, or generalization, is the most common. In this form, you make a general statement regarding some predicted outcome based on observations of a specific instance of a class. For example, the statement, “all lawyers are sleazy,” when based on your observation of the last three lawyers you have encountered, would be induction by enumeration.

Because inductive logic is less precise than deductive logic, fallacies are often less easily identified. The fallacy most commonly associated with inductive reasoning is the hasty generalization. When an argument fails as a hasty generalization, the inductive leap that the proponent asks the decision maker to make is too remote. Sufficient evidence does not support it. The following statement suffers from the fallacy of hasty generalization:
Inductive versus Deductive in Case Proof

As you can see, inductive and deductive reasoning are very similar, the greatest difference being the manner in which we express the argument. When you argue from the general to the specific, deductive reasoning is in play. When you reason from the specific observation to broader generalizations, inductive logic is in play. It is important to note that we may recast all inductive arguments as deductive syllogisms and vice versa.

As an investigator, you will encounter both forms of logical reasoning.

However, the offering of evidence in the legal system will most often expose you to inductive logic. In the process of proof, it is common to allege and prove specific isolated facts and build to a general conclusion. Therefore, the inductive process of moving from the specific observation to the general conclusion just seems to feel right.

We should note that some readers may argue that deductive reasoning, being the more mathematically certain, should be the more favored logical form in legal proceedings. Keep in mind that the law, and the system for legal resolution of disputes, is concerned with probabilities, not certainties. It is not absolute proof that we seek; it is proof beyond a reasonable doubt. Because inductive reasoning is ideally suited to reason from specific facts (evidence) toward broad generalizations (guilt or culpability), induction is the more natural form of legal argument. In truth, it does not matter greatly which form the argument takes. As stated earlier, we may form all arguments as either inductive or deductive premises.

That is not to say that deductive reasoning is useless in the legal context.

Quite the opposite is true. When we choose the deductive over the inductive, the inferential focus shifts. There are still inferential leaps that you must make; we simply make them in a different location.

For example, we can formulate our argument regarding XYZ Company’s activities either way. To state the argument inductively: XYZ Company is involved in money laundering since it is an import-export company operating in Miami, Florida.

Stated as syllogisms: (1) All import-export companies operating in Miami, Florida, are involved in money laundering. (2) XYZ Company is an import-export company located in Miami, Florida. (3) Therefore, XYZ Company is involved in money laundering (deductive).

Obviously, these examples are oversimplified, exposing the fallacies of logic quite quickly. In reality, the inferential links in a logical chain will be much more subtle, and the facts often obscure the fallacies of logic that can cripple the argument.

Both arguments, as they stand, are legally indefensible. In the inductive example, the inferential leap may not be as evident as in the deductive, requiring the reader to infer that all import-export companies operating in Miami,
Florida, are engaged in money laundering. Although the reader undoubtedly senses that something is not quite right, specifically pinpointing the source of the illogicality may be difficult.

In the deductive example, the breadth of the inferential leap required of the reader is much more apparent. By breaking the proposition down into deductive form, we more easily expose the fallacies of logic inherent in the inductive process.
DATA MINING: COMPUTER-AIDED FORENSIC ACCOUNTING INVESTIGATION TECHNIQUES

Data mining uses software to assist the forensic accounting investigator in identifying and reviewing unusual data trends, patterns, and anomalies. Regardless of size, many of today’s organizations maintain the majority of business transaction data in electronic formats. That is also true for many of the other primary sources of data potentially relevant to a forensic accounting investigator: customer and supplier information, product and price documentation, telephone logs, building security and access details, and employee data, to name but a few sources. The likelihood is high that most of the data the forensic accounting investigator is engaged to review will exist electronically.

As a result of the use of small-business management programs such as QuickBooks in smaller firms and enterprise-wide accounting packages in national or global firms, today’s computer systems are vast warehouses containing data from finance, operations, marketing, and personnel. While small companies engage in hundreds or thousands of transactions, large-company transactions number in the tens or hundreds of millions, even billions. Given such volume, relying exclusively on manual investigation skills (without using computer aided techniques) to uncover suspect transactions is too expensive and likely to overlook key data. Within those thousands or millions of records could be fraudulent activity that may remain hidden unless the right tools and know-how are applied to bring the issues to light.

Data analysis is often the fastest and most effective tool at the forensic accounting investigator’s disposal for gathering much of the evidential material needed to support findings. Much of the data, particularly the no accounting data, is never used directly by the organization in question, but any of it may hold the key to an investigation. In cases in which the forensic accounting investigator has been engaged on the basis of a suspicion or an as yet unsubstantiated allegation, the results of data mining may provide the forensic accounting team with that all-important place to start.

Auditors too often use software tools—some of them generic or homegrown—to query accounting systems, gain assurance with respect to data integrity, and in some instances, identify so-called unusual transactions. American Institute of Certified Public Accountants Statement on Auditing Standards (SAS) 99, Consideration of Fraud in a Financial Statement Audit, refers to such measures as computer-assisted audit techniques. These tools form part of the forensic accounting software tool set. The tools can uncover anomalies and patterns that might go undetected by an approach that relies on testing samples.
Data mining is the process of looking for trends, patterns, and anomalies within a data set. These trends, patterns, and anomalies—or exceptions to them—may be completely innocuous and can be verified as such. However, unusual transactions—those falling outside expected norms—may signal the need for an investigation by forensic accounting investigators who will apply their experience in data mining and in investigative techniques to the overall situation that appears to be emerging.

The technical process by which data mining is carried out is often complex. The analyst must be a competent user of the relevant tools. While a full description of the complexities of the data-mining process is beyond the scope of this book, this chapter can usefully focus on the ways in which the forensic accounting investigator can utilize data mining to maximize its contribution to an investigation.

**EFFECTIVE DATA MINING**

At the planning stage of any forensic accounting project, the project manager should consider three key questions when deciding whether and how to gather electronic evidence:

- What relevant data might be available?
- What skills are available within the team?
- How will the data analysis fit in with the wider investigation?

**WHAT RELEVANT DATA MIGHT BE AVAILABLE?**

When computers store information for later retrieval, the operating systems necessarily create certain data about the stored information in order to facilitate ongoing processing. Some programs also allow users to add their own metadata to a file, such as a document title, the subject of the file, the name of the author of the document, the name of the manager responsible for the document, and the name of the company that owns the document. In addition, some programs permit a user to assign metadata to a document in order to facilitate later retrieval. This type of metadata can include assignment of the document to a particular category, inclusion of searchable keywords, or a description of the document’s contents.

In addition to these types of metadata, there are other, less obvious variations. For example, spreadsheets and databases can contain complex mathematical formulas and links among fields, which play key roles in calculating the numbers that appear in various cells. Typically, the printed spreadsheet will show only the result of the calculation, not the formula used to calculate the result. Similarly, modern word processing documents can contain links and references to other types of electronic files such as pictures, charts, spreadsheets, and sound files.

These linked files may be stored either in the same location as the main document or halfway around the world on another computer linked by a proprietary network or by the Internet.
printed document may show the content of the other files without revealing that those elements are not integral parts of the electronic document but are really borrowings from other electronic sources.

The electronic document will necessarily contain the code needed to connect to the data in the linked files and may give a forensic accounting investigator point-ers to additional sources of relevant information. This in turn may lead to additional witnesses, such as the author of a linked document in a remote location.

**AUDIT TRAILS (TRAFFIC DATA)**

In addition to metadata created at the file level, many computer systems generate significant amounts of traffic data when information is manipulated within a computer or across a computer network. Such traffic data, often referred to as audit trails, may be useful when trying to tie activity back to a particular user or set of users and may give clues as to its authorship. Network traffic data (if it is being stored) may indicate which user account was responsible for storing the document to that location.

Many types of traffic data may be available to the forensic accounting investigator.

For example, most general ledger systems can be configured to record the user name associated with the most recent change to any value in the system.

Some systems allow users to record the user names responsible for every change to a value over time. Similarly, many e-mail systems retain information about the dates and times associated with transmissions of each e-mail and attachment.

Some of these systems also record the date and time of message deletions. Operating systems may maintain dates associated with accessing, moving, or deleting files. All of this information can be useful in the course of an investigation.

Yet traffic data can take an investigation only so far. It is sometimes said that the last inch in a cyber investigation is the hardest. Electronic audit trails may indeed lead a forensic accounting investigator back to a particular computer as the one responsible for a given set of activities—for example, a particular change to a general ledger system.

**FASTER/BETTER/CHEAPER**

A computer can search, sort, and manipulate an electronic document in a fraction of the time necessary for a human to perform the same tasks. In a case involving hundreds of thousands or millions of pages of printed materials, human review and search for specific information can be tedious, imprecise work. But computer searches across the same volume of electronic files can reliably discover—and in short order—every instance of a particular word or combination of words. Similarly, a computer can instantly sort a large volume of information by date, file name, author, storage location, or any number of other criteria, thereby
highlighting key documents in what could otherwise be an extremely time-consuming manual review.

ACCESS TO RELEVANT DATA

The existence of information does not guarantee that it will be readily available to the forensic accounting investigator. There may be technical, organizational, or legal barriers that potentially prevent the forensic accounting investigator from gaining access to that data. For example, in many investigations, forensic accounting investigators find that the organization’s archiving system restricts access to data they need, particularly historical data. Depending on the format and media to which data has been archived, the forensic accounting team may find that the cost of restoring the archived data is prohibitive.

In one engagement, a forensic team found that detailed transactional data were copied to microfiche six months after the transactions occurred. The original documents were then destroyed. Because of the cost involved in restoring the data to a usable format, the forensic accounting investigators had to develop an alternative approach to analyzing the transactions, which included searching for a sample of transactions on the existing microfiche—an incomplete and extremely time-consuming process.

Many organizations archive only the information they are required by law to keep. When this is so, information on historical transactions may be available only in summary or overview form. It may also be that the needs of the forensic accounting team conflict with the organization’s security policy concerning access to especially sensitive information. While such factors may not ultimately prevent the forensic accounting investigator from accessing relevant data, they need to be considered, particularly when the project is subject to time or other constraints.

In recent years, difficulties have arisen because of organizations’ outsourcing of their data management function. Consider this example: a forensic technology team was called in, at an outsourcing agency, to review the work of a technology team from another firm. The review team members noted that they were dealing with an accounting system that contained over 1,400 tables with multiple links among many of them. Complicating the situation even further, only one contract engineer at the outsourcing agency possessed a thorough understanding of the system. While forensic technology professionals could have spent time piecing together an understanding of the multiple links, in this particular engagement that would not have been the best use of professional time or client money. The investigation was delayed until the engineer could be released from other projects to assist the forensic team with the data extraction. Only in this way could the team be sure of performing the task correctly the first time around.

Having this specialized knowledge on the team is more than likely to add value in determining the course of action.
One factor that forensic accounting investigators ignore at their peril is the potential for legal restrictions governing access to the data they need to review.

Data protection legislation is often in place, particularly in Europe, where such legislation is stricter than in many other parts of the world. Forensic technologists and others who are asked to investigate or evaluate such data should familiarize themselves with the relevant legislation, which may be complex and is sometimes untested. In addition, while the team might legally be able to obtain and access certain information within a particular geography or country, restrictions may exist on transporting that information beyond country boundaries. Example, forensic accounting investigators might request data only from individuals who cannot be personally identified. Solutions can often be found that comply with the requirements of the legal environment. When an investigation requires the use of customer, staff, or other personal details, access to such data may still be possible. Each country or jurisdiction may have laws that protect privacy and even dictate whether computerized files can be removed from the premises or out of the country. A good practice is to always seek appropriate legal advice before attempting to acquire any personal data.

**ASSESSING DATA QUALITY AND FORMAT**

Early assessment of the quality and format of available data is vital to ensure that the forensic accounting team’s technological resources will be used effectively.

If data is potentially unreliable or extremely difficult to extract or format, the team may be better off concentrating on other investigation methods. However, cases in which no tool can be found to deal with system output are rare, and in most instances at least some of the data is reliable.

A person experienced in data management should perform the initial assessment of data quality and format; this is important. Additionally, if the data is of a highly specific nature, it may be necessary at this stage to involve individuals with specialized industry and technical skills and knowledge. The person assessing the data sources should have good background information about both the operational activities of the client and the nature and purpose of the investigation.

Close coordination between the forensic technologists and the organization’s systems administrator is highly recommended. Generally, the systems administrator should be the forensic technologist’s first point of contact and often provides considerable input about the structure of the system, relevant input controls, and potential formats for extractions.

Clearly, such coordination would be inappropriate if the systems administrator is the probable focus of the investigation. As well, forensic accounting investigators should be aware that systems administrators’ objectives might differ from those of the forensic accounting team. Administrators may be concerned about their own or their team’s workload; or there may be a desire to make data validation controls seem tighter than they actually are; or administrators may attempt to persuade the forensic team that their team’s technical competencies are more
robust than they actually are. Because administrators are frequently more cooperative when dealing with other data management specialists, using such an individual to carry out the assessment will make it less likely that the team will be put off by an uncooperative systems administrator.

The initial assessment should cover:

• Scope of available data

• Quality of available data

• Time required and data requests

SCOPE OF AVAILABLE DATA

Given the breadth of data that is available, a clear understanding of the investigation is useful in guiding the forensic accounting investigator to the relevant data. Data can come from many different sources within an organization, and while financial reporting systems are frequently the main data sources, less obvious sources may exist from which supplementary information can be gathered.

In one case, management of a bank alleged that certain mortgages were being falsely attributed to an intermediate broker instead of to the customers who had directly applied for the mortgages. The purpose of the alleged fraud was to generate additional broker’s commission. In gathering evidence, the forensic team matched the names of bank customers found in the branch’s daily appointment diaries to details taken from the bank’s mortgage portfolio. The diaries proved to be unusual but effective sources of data. Other useful data sources for forensic accounting investigation engagements might include bank statements, supplementary accounting systems, and logs from telephone networks or electronic security systems.

The integration of data from such sources can be one of the most productive investigative methods for the forensic analyst. Fraudsters rarely manage to cover all traces of their activity. The forensic accounting investigator’s ability to crosscheck various data sources against common key fields and to identify potential inconsistencies between sources can be a most valuable investigative tool.

In their search for data, forensic accounting investigators should not focus exclusively on digital sources. Paper records can be scanned and converted into usable files with optical character recognition tools. For example, bank statements are often scanned and then matched against the accounting system, creating, in effect, electronic bank reconciliation. In environments in which checks are used, another option is to request that the bank provide a tape of cleared checks. By comparing this information with the client’s disbursement file, the forensic accounting investigator can create a list of outstanding checks.
Every forensic accounting investigation engagement is different, and for each, the key sources of data may vary. However, the following are among the most useful and readily available records:

- Vendor master file
- Employee master file
- Customer master file
- General ledger detail
- Cash disbursements
- Customer invoices
- Other data or data sources, depending on the circumstance, including receiving and purchasing information, telephone data, voice mail, e-mail, personal digital assistants, BlackBerrys, and computer hard drives.

In most cases, system input controls will determine the quality of the data available within an organization. On certain systems, particularly nonfinancial systems, few such input controls may exist. Together with the systems administrator or another internal information technology (IT) professional who has detailed knowledge of the system’s functions, the forensic technologist should first assess these input controls and their potential impact on data quality. In addition, forensic investigators should check their conclusions against discussions with actual system users, who may be inputting particular data items even though the system does not require them to do so.

When the system does not perform internal validation checks—such as checking a tax code against amounts input or restricting the range of values that can be input into a field—the quality of the data will in most circumstances be lower.

The forensic accounting investigator should consider this important detail before requesting a data extract that can often require several days’ work on the part of a systems administrator and the forensic technologist. If it is determined that no—or relatively few—controls over system input are in place, or if key fields can be left blank, the forensic technologist should assess how much value the data will add to the investigation.

TIME REQUIRED AND DATA REQUESTS

Data can be extracted from a system in a variety of formats. In descending order of convenience for the forensic accounting team, the formats include database files, delineated text files, and headed report files. While the use of software is an important aspect of any investigation, the challenge is to obtain accurate and complete data in the proper format the first time. Awareness of common pitfalls and mistakes can avoid frustration and erroneous conclusions.
The forensic technologist and systems administrator should jointly prepare an estimate of the
time it would take to produce extracts in each available format and should review that
estimate in light of both the risk of extraction errors and the estimated cost of cleaning the
data.

At this juncture, a compromise is usually reached as to the degree of effort the systems
administrator expends to extract the data and the degree of effort the forensic technologist
expends to prepare the extract for analysis. For example, the systems administrator may be
able to provide standard reports that with very little effort, can be made available in the form
of text files. Even using powerful cleanup tools such as Monarch, the forensic analyst may
spend considerable time cleaning out headers and expanding multidrug data. As a general
rule, whenever possible the forensic technologist prefers data in no report format that can be
accommodated within the investigation plan.

The number of available data formats may be restricted by the technical expertise available
within the organization. A significant number of smaller organizations outsource their IT
function and receive very little nonstandard support from the external contractor. Before
conducting any of the data-mining techniques, forensic accounting investigators need to
ensure that they are requesting the correct computer files for the assignment. The
investigative team should meet with appropriate IT personnel to confirm that it has searched
all potentially relevant sources. Especially with multinational companies, the team should not
assume that transaction processing is maintained at the location where the transactions occur.
Such transaction processing or other elements of the process may have been outsourced or
may be located at a central service center. For example, the data required for an operation in
Pittsburgh may actually reside at a shared services center in India.

The team should document in writing the information it is requesting, speak to
IT and finance personnel, and ask probing questions so that information is correct and
complete the first time around. See the appendix immediately following this chapter for an
example of a data request.

The team should establish a protocol for requesting specific information b combining
requests and by speaking to IT and finance/accounting personnel to verify completeness. The
requests should be in writing and include requirements regarding the format in which the
information should be received—for example, text, tab delimited, or ASCII. Lack of clarity
and precision in the request can cause additional work and problems associated with cleaning
up or scrubbing data, which can be avoided by planning and clear communication at the time
that files are requested.

A clear understanding before beginning any analysis can avoid false starts and erroneous
preliminary conclusions. Requesting a data dictionary can be helpful to an understanding of
what types of information are captured in a system or in a database of information. The data
dictionary specifies which files have the data and fields required for analysis. This approach
is preferable to asking for specific fields and thereby running the risk of not obtaining all
required information the first time around. If in doubt, the forensic accounting investigator should err on the side of asking for more data rather than less. Even after receiving the computerized information, the investigative team should determine the completeness and accuracy of all information received.

There are two key requirements for the preparation of a comprehensive data specification: a good understanding of the structure of the data source and clarity as to the aims of the forensic accounting investigation. By way of illustration, consider a hypothetical investigation at a manufacturing plant in Matamoros, Mexico. The company’s corporate headquarters is located in the Midwest.

Embezzlement and kickbacks have been alleged. The investigative team’s assignment is to determine where the money has gone and who is involved. In this hypothetical situation, the team must ask where payments are processed and what level of detail can be obtained from the system. The answer may be twofold:

(1) Payments to vendors are processed in Mexico, sometimes in pesos and sometimes in cash, and (2) payments to vendors are processed in the United States in U.S. dollars. Both sets of data may be necessary to the investigation.

The team must not rely solely on the data from Mexico or from the United States. By obtaining both data sets, the team might determine, for example, that the same vendors are paid in pesos and in U.S. dollars for the same services, with both sets of payments approved by local Mexican management.

As noted earlier in this chapter, the cooperation of the systems administrator can be invaluable in determining and understanding the system structure. However, circumstances may exist in which systems administrators are unable or reluctant to help or in which they themselves are suspected of being complicit in the fraud. In such circumstances, the forensic technologist will need to seek out other ways to obtain this information. A helpful source in this regard often is the system documentation itself. Alternatively, if the system type is familiar to the analyst, inspection alone might yield valuable information.

The forensic technologist should spend time with the forensic accounting investigator in charge of the investigation to determine which data could be relevant to the analysis or to the collection of evidence. Close coordination between the forensic accounting investigator leading the review and the forensic technologist during the initial stages of the investigation, prior to the extraction of data from the organization’s systems, can save all parties valuable time and effort.

In the design of the data specification to be submitted to the organization, it is important to build in certain flexibility in terms of the upcoming data analyses.
In many cases, requesting extra data fields will require minimal additional extraction work. However, once an extraction has been prepared, requesting an extended data extraction can often be difficult. Doors should not be closed at the early stage of an investigation.

Another reason the scope of the data specification request should be as broad as possible has to do with the processing time required for extraction. For example, extracting data from an organization’s systems that relates to all customers who have made more than three payments in the past month may take considerable processing time. Requesting data on all customers and all payments and, subsequently, identifying customers relevant to the analysis may actually take less time.

The investigation will rely on the data extracted by administrators. Minimizing the likelihood of errors will save time and money. The team should discuss the extraction process with the systems administrator to identify exactly what that process will entail. Taking this step not only provides a clearer idea of what will be received and how but also reduces the risk of error.

In one investigation, the systems administrator had to prepare the data extract from archived tapes that covered overlapping periods. In order to try to correct for this factor within the data extract, the administrator deleted all duplicate records. Unfortunately, no unique key had been included in the extract. As a result, many genuine records were accidentally erased.

Once the team decides which data are relevant to the investigation, it should convert that decision into a detailed written data specification. Care should be taken when drafting this document. In all likelihood, the systems administrator will provide the forensic technologist with only those fields for which the team explicitly requests data specifications. The document also should include requirements about how the information should be received—for example, as database files, as delineated text files, or as headed report files. When requesting e-mail files, the forensic technologist should consider asking the systems administrator for super user passwords or user passwords to gain access to password protected or encrypted files.

On one occasion, a bank prepared a data extract for an internal investigation that occurred before engaging forensic accounting investigators. As part of the internal investigation, the investigator requested information on the date, amount, currency, and narrative of all transactions. The systems administrator did not include a transaction ID—which would be useful in providing a link between debits and credits for internal transactions—because it was not requested in the data specification.

The specifics of any data request typically depend on the nature of the organization and its systems and on the nature of the potential fraud. A general checklist should include the following:

- Primary key. The most vital element of any data extract, the primary key is the field that uniquely identifies each record in the data set.
• Foreign keys. These keys are present when the data provided consists of more than one table. In a well-managed data source, they provide the link from their own table to the primary key of another table.

• Lookup tables. While foreign keys are often present in the main data extract, the relevant look-up table is absent. For example, branch codes may exist but not a list of the specific branch to which each code relates.

• Row count. Comparing the number of records received with the number of records that the client thinks it has extracted is an apparently simple but nonetheless important step.

• Hash totals. With large-scale data extracts, hash totals requested from the client should be compared with totals computed from the data used in the investigation. These are sums generated by totaling data items such as transaction IDs or product codes. They provide an additional check that the data has not been compromised as it passed from the client's system to the investigation database.

• Data specification/data dictionary. The systems administrator should provide a short description for each field within each table. This avoids the possibility of inaccurate calculations if the forensic accounting investigator must make assumptions about the contents of key fields.

• Extraction specification. All data requests should be submitted in writing to avoid confusion. E-mailing such requests is a perfectly acceptable method of communication. Knowing exactly what the extracted data represents and the period it covers is important. For example, if the forensic accounting investigator has requested “invoices over $100,000 from the eastern division from 200X to 20XX,” then the investigator should seek written confirmation that the data has been delivered. If possible, the person who actually produced the data extracts should provide the confirmation

DATA CLEANING

This process involves removing page headers and footers from files, expanding data with more than one row per record, stripping out nonnumeric characters from number fields, and a host of other procedures aimed at standardizing the data to make it suitable for use with the analysis tool selected as most appropriate for the data analysis exercise.

The data-cleaning stage is critical to the data analysis process. It is the only point at which alterations are intentionally made to the extracted data, and it is imperative that amendments made at this stage not affect the accuracy of the information. A documentation log should be maintained of all alterations undertaken.

The log may be needed at a later date to prove the integrity of the analyzed data and its relation to the information extracted directly from the organization’s systems. We strongly advise that only forensic technologists with relevant and up-to-date experience undertake complex data-cleaning exercises.
Data cleaning can also involve the standardizing of common abbreviations within a data set and removing extraneous information. These steps make useful information available to the forensic accounting investigator. Not all software programs may be capable of this type of cleaning, and special programming may be necessary. In the long run, particularly for matches that are performed frequently, the cleaning procedure can increase efficiencies and improve consistency.

In Exhibit 20.1 on the next page, all directional components of addresses—that is, north, east, south, and west—and extraneous words and characters such as street and suite are removed. Additionally, spaces for characters such as periods, commas, and apostrophes are deleted. For example, compare the address from the vendor file, column D, with the cleaned address in column F. If the cleaning process were not performed in this way, lines 4 and 8 would result in a potential match because each address is “123 W. Main St.” When the cleaning process is applied, the addresses do not match because the comparison is then between “123MainIL” and “123MainOK.” In practical terms, designating long strings of characters to obtain matches does not make sense—for example, to identify multiple entities or individuals at the same address. Instructing the software program to match on the street number, the street name, and the state would yield results far different from instructing it to match only on the street number and street name. Similarly, matching street addresses based on the first few characters plus the state will yield results far different from matching street addresses based on the street number, street name, and state.

Exhibit 20.1, an excerpt from vendor and employee addresses, indicates when data has been cleaned and when it has not. With proper data cleaning, all line items would be street-address matched; however, line 8 would be an exception because the state was OK, not IL.

Using this data helps the forensic accounting investigator focus on which data to request for additional review; otherwise, some may resort to manual techniques to identify matches. The latter is a time-intensive and potentially inefficient process.

**ELIMINATING DUPLICATE INFORMATION**

One of the problems forensic technologists encounter is that multiple copies of various materials may be recovered as part of the investigative process. Because of the expense involved in reviewing such duplicative materials, elimination of duplicates (duplication, or deducing) in the recovered data sets is often the first order of business after the data has been acquired and the documentation has been completed.

One might suspect that duplication would be a straightforward process; however, several variations of the process need to be considered before work can begin. First, the examiner must decide what qualifies as a duplicate. Do all of the fields of data need to match exactly, or should two e-mail messages be considered duplicates if the subject and body are identical without regard to the date and routing information? If you require all of the data to match exactly, then any message with a bcc will appear at least twice because the bcc field will
show up time stamp is off by a second, the message will appear more than once in the review data.

Second, the practitioner must decide which universe of documents should be subjected to deducing. Consider an investigation involving the e-mail of 25 employees, one e-mail server, and four sets of backup tapes. There are likely to be at least six sets of data available for each employee—four sets of mail from the backup tapes, one set from each individual’s office computer, and one from the active server—and there could be many more depending on a variety of variables such as data from one or more additional laptop or desktop computers, BlackBerry devices, pagers, e-mail-enabled cell phones, and home PCs. DE duplication of this data could proceed on (1) the basis of the entire universe of data, so that each message would be reviewed by forensic accounting investigators only once, or (2) across the data related to each user, so that each message would appear only once in each user’s mailbox but might be reviewed up to 25 times by forensic accounting investigators if all 25 targets received a copy of the same message; or (3) across a subset of the entire universe, such as all employees in a certain department.

Each of these choices has advantages and disadvantages. DE duplication across the entire universe of messages may be the most efficient process in terms of limiting the amount of time it will take to review the data, but it also poses challenges. For instance, if the reviewers are divided into teams, with each team focusing on the activities of one of the targets (a typical arrangement) and only one copy of a message sent to seven people will appear in the review data, then which team will see the message? Should one target be considered the prime suspect such that all messages sent to that target and other targets will appear only in that target’s data? And if so, won’t that make the review of the other targets’ data nonsensical because many of the messages will appear out of context, with all duplicated messages not appearing in the secondary subjects’ data set?

As a practical matter, these issues require the examiner and the entire investigative team to map out their approach in advance and choose a process that is consistent with the particular project’s needs. DE duplication can dramatically reduce the cost of reviewing a large data set.

In one recent investigation, 5 terabytes (nearly 21 million files) of e-mail and user file data recovered from backup tapes was reduced to less than 900 gigabytes of data (less than 5 million files) through the DE duplication process, thereby cutting the review time by over 75 percent.

**TESTING THE DATA FOR COMPLETENESS AND ACCURACY**

How does one ascertain the completeness and accuracy of the information?

The files requested determine the approach. Sometimes the situation is complicated by incomplete, inaccurate, inconsistent, and incorrect information. In if not impossible and supplementary reasonableness checks may need to be performed.
The completeness checks can include confirming that the totals and rows extracted from the system are the same ones that the forensic accounting investigator received from the company. Other tests for reasonableness include the following:

- Comparing total payments, payroll, and profits with annual revenues
- Comparing total payments with debits on the bank statements: this may be done initially at a high level and then at lower levels of detail. Multiple accounts and/or numerous transfers that are not accounted for on the check register make this procedure more difficult.
- Comparing sub ledger and/or general ledger postings
- Testing selected transactions to determine whether they have been posted to the general ledger
- Discussing potential exceptions with management to confirm appropriate inclusion or exclusion of known problem cases

Forensic accounting investigators who are dealing with multiple currencies and multiple years may have to deal with more than one currency within the same payment information file. The data analyst will need to test to confirm that the currency conversion is functioning properly. Some currencies have undergone large fluctuations in value relative to others. For example, prior to 2002, Argentina’s currency tracked with the U.S. dollar; however, this is no longer the case due to dramatic fluctuations in the Argentine peso that occurred in 2002. A 50,000-Argentine-peso payment in 2001 may be equivalent to $50,000, while the same payment in 2003 may be equivalent to less than $20,000.

During a recent investigation in the Middle East, a forensic team requested check disbursement data in U.S. dollars for the branch office under investigation to facilitate comparison to data from other branches worldwide. Upon receiving the data, the team tested the currency conversion and found errors totaling as much as $70 million in a data set of $270 million—more than 25 percent of the total payment amount.

Discussed below are some additional false starts commonly encountered when an investigative team attempts to obtain data? They serve to illustrate the point that even when experienced investigators obtain computer files, miscommunications can occur.

**UNDERSTATED AMOUNTS**

After receiving payments data from a location in Mexico City, the investigative team quickly determined that the payments file was significantly understated.

The vendor payments file had been requested numerous times both verbally and in written form and in both English and Spanish. The request specifically highlighted the importance of
providing complete data. The team attempted to work together with the controller to determine the cause of the understatement.

However, the controller said he did not realize the request also included payments for inventory suppliers. In his mind, he did not consider an inventory supplier to be in the same category as a vendor. The complete file was obtained after the second attempt, and in the course of its analysis, the investigating team was able to identify several payments as possible bribes and kickbacks.

**OVERSTATED AMOUNTS**

On another cross-border assignment, a member of the investigative team observed that Ms. X had received 10 million pesos in a recent year—a significant sum for that person. The payment register files had totals that were a multiple of the annual revenues, a sign that data was probably incorrect. Upon closer examination, each line item had had two zeros added to the end of every payment that occurred during the data conversion. While Ms. X had received substantial payments, the magnitude was far less than originally surmised. This reinforces the fact that verifying the completeness and accuracy of the data is an important step before undertaking any analysis.

**INCOMPLETE RESPONSES**

When requesting a payroll file from a government entity, the investigative team noticed that the payments amounted to only a fraction of the payroll expense when compared with the general ledger. Upon inquiry, the IT department staff member responsible for fulfilling the team’s request commented that the request was for “payments,” which he interpreted to mean a physical check. All payroll direct deposits—those not paid with a physical check—were not included in the data file he had provided.

**INCOMPLETE DATA SETS**

While reviewing files to ascertain completeness, an investigative team may discover heretofore unknown or undisclosed transfers to other bank accounts. The team may use these transfers to uncover additional bank accounts and check registers, thus revealing many suspect transactions that could have gone unnoticed had the completeness and accuracy test not been performed.

**SKILLS OF THE FORENSIC TECHNOLOGIST**

Investigative data analysts should possess strong technical skills and a good understanding of the relevant tools. However, beyond the tools, the analysis process usually involves many other skills, such as accounting skills and an understanding of investigative methods. The process also requires communication between the analyst investigating the data and other members of the team.
TECHNICAL SKILLS

Most obviously, a forensic technologist should possess technical IT skills, which are fundamental to the performance of data cleaning and analysis and the presentation of results. Many data-cleaning and data analysis tools are available. While some are noticeably more powerful than others, all require that users possess a good understanding of how they work. Many such tools require that users be able to write code in one language or another, and a simple mistake such as putting a bracket in the wrong place could lead to distortion in the results. Forensic technologists will often not perform all of the analysis or presentation of results themselves. Rather, they will prepare the information in a format that the forensic accounting team can use to perform additional analysis. Nonetheless, the forensic technologist should continuously support the forensic accounting team throughout this process in an overview or advisory function by providing needed IT technical expertise.

Data analysis is an explorative technique. As with any non-IT-based investigation, approaches to investigating a particular set of facts or circumstances can vary. The process is iterative, and both accounting and investigative skills may be necessary to respond to results and to design the next investigative steps to be taken—or, in the case of data analysis, the next set of data queries to be run.

Forensic technologists who have knowledge of accounting mechanisms usually are able to highlight unusual items and recognize the various ways in which a transaction might be reflected in the system. Such knowledge is clearly useful.

Anyone undertaking a forensic accounting exercise is likely to need specialist technical support from an experienced forensic technologist. Coordination is essential to avoiding misunderstandings with regard either to the analysis requirements or to the results produced.

COMMUNICATION SKILLS

Forensic technologists should possess good communication skills, both verbal and listening. During the investigative process, the forensic technologist should liaise with the systems administrator and share information with the investigation team. The forensic technologist is also frequently called upon to explain the data analysis process to in-house or external counsel.

Throughout the forensic data analysis process, decisions must be made about which data to acquire, what tools to use, and which data queries to run. To make these decisions, the forensic technologist should have up-to-date knowledge of all significant factors relevant to the investigation. Only if analysts are thoroughly aware of the results or evidence identified in the manual investigation can they best respond to the interim results of the data analysis process. In cases in which the forensic technologist does not possess the accounting and investigative experience necessary to make such decisions, members of the forensic accounting team should be fully informed about all stages of the data analysis results so that the team’s requirements can be fed into the next stage of the process.
Close coordination will lead to a process of efficiently integrating the technologist’s work product into the forensic accounting team’s work and vice versa, or script indicating which queries to perform may be more efficient.

Results presented to the forensic accounting team must be fully understood. At the very least, data given to the forensic accounting team might well be accompanied by a narrative explaining what that data represents. Even if the forensic accounting investigators believe the team understands the information they have presented to the team, the team may benefit from this explanatory paragraph. Mistakes should be identified before incorrect data becomes the basis for further investigative procedures. This technique may be useful in cross-cultural teams.

**EFFECTIVE USE OF DATA ANALYSIS RESULTS**

A powerful method of gathering evidence, data analysis becomes most effective when it is integrated into the wider forensic accounting project. If the end results must cohere with findings from other sources, forensic data analysis should not be performed as a separate investigation. This section looks at the role of forensic data analysis methods in a forensic accounting project, including typical data analysis tests, typical data analysis tools, and methods of presenting results.

**ROLE OF DATA ANALYSIS IN THE INVESTIGATION**

Data analysis can serve many functions within a forensic accounting project. On some occasions, it is the main engine of an engagement. When such is the case, data analysis is used for highlighting potentially unusual items and trends. More often, however, data analysis is a complementary part of a wider forensic accounting investigation that involves several other methods of information analysis or evidence gathering, including document review, physical inspection, and investigative interviews.

The timing of the data analysis work depends on the extent to which the forensic accounting team needs to work with the results. In some cases—for example, once the method of a fraud has been established—data analysis is conducted to estimate the amount of damages. If the team knows that several branches of an organization were affected by a fraud scheme, that team may be able to compare these results with those derived from analyses of unaffected branches and after adjusting for other relevant factors, provide management with a broad estimate of the total effect on the financial statements. When such an approach is used, the comparison should be performed after the investigation has determined the characteristics of the fraud scheme. However, in most cases, the purpose of data analysis in an investigation is to identify suspicious activity on which the forensic accounting team can take action.

Suspicious transactions can be identified in a number of ways: comparing different sources of evidence, such as accounting records and bank statements, to find discrepancies between them; searching for duplicate transactions; or identifying sudden changes in the size, volume, or nature of transactions, which need to be explained. While data analysis often is a fast and
effective way of highlighting potential areas of fraud, it will never capture every detail that a forensic accounting investigator can glean from reviewing an original document. If data analysis is performed to identify suspicious activity, it should be performed before any manual review is carried out. This will help ensure that investigative resources are targeting suspicious areas and are concentrating on confirming fraudulent activity rather than concentrating on a search for such activity within a sea of legitimate transactions.

On one occasion, forensic accounting investigators spent two weeks creating a list of suspicious payments from source documentation before any data analysis was carried out. Within an hour of importing the data into its system, the investigative team had created a list that contained over 90 percent of the transactions that appeared on the manually prepared list, plus a few additional transactions that had been overlooked. Having this list at the start of the investigation would have been more efficient.

However, the role of the analyst goes beyond manual inquiries. Frequently, the results of manual inquiries need to be fed back into and incorporated in the analysis process. For example, if inquiries show that the fraud is limited to one or two suppliers, further analysis can concentrate on transactions in those accounts. While data analysis alone can be the focus of some investigations, most projects require an iterative analysis, alternating between input from the investigation team and feedback from analysis results. When this is the case, the infrastructure used in performing the analysis and communicating results to the team should support that level of interaction.

DELETED/SLACK/UNALLOCATED SPACE

Up to this point, our discussion has centered on active files stored on a computer system, backup tape, server, or other electronic media. One of the beauties of computer forensics is that a forensic accounting investigator is not limited to examining these so-called active files. When files are “deleted” from a computer hard drive, the operating system typically just removes references to the data in the file system. The actual file data is typically not removed from the drive until the operating system needs the space to store other data. Although this unallocated space generally cannot be seen by normal operating system tools—such as Windows Explorer—it can be seen, searched, and sorted by computer forensic tools. Some data in unallocated space will be fully recoverable as if it had never been “deleted.” Other data may consist of file fragments that have been partially overwritten. While such data may not be fully recoverable, it may still provide clues about the computer user’s activities.

Such tools can also search through the space at the end of files between the end-of-file marker and the end of the cluster in which the active file data resides.

This slack space, not being used by any active file, may contain bits of data from files long ago marked for deletion from the hard drive. Forensic tools can search and find data stored in these spaces that might otherwise go undetected if drives are simply copied rather than imaged.
There are several potential limitations on the use of data discovered in slack and unallocated space. First, it may not always be possible to attribute dates accurately to such information because the normal operating system dates will not typically be available. Second, highly fragmented data found in slack or unallocated space may be hard to place in context. For this reason, drawing conclusions about the data may be difficult in some cases. Third, it may be hard to attribute data found in slack or unallocated space to a particular user, especially if the computer under investigation was used by more than one person.

Notwithstanding these potential limitations, the ability to review data that has been marked for deletion by a user is one of the key advantages of a forensic approach to the review of electronic data.

**DATA SORTING**

Although the ability to sort investigative data is mundane, it may also be essential to the project goal, especially when millions of e-mail messages or pages of file documents must be reviewed. Data sorting enables the forensic accounting investigator to separate the data into more manageable subsets for review and analysis.

As mentioned previously in the chapter, attributes such as date/time are examples of metadata, which, depending on the matter at hand, can be useful information to the forensic accounting date accessed prior to a creation date is not possible. Examining this item of metadata may raise a red flag for the forensic accounting investigator.

**Date/Time**

Date and time sorts are common criteria in the sorting of data as part of an investigation.

In such sorting of computer data, many dates may be associated with a single document or data point. It is important to understand exactly what a particular date means before drawing conclusions about the data. For instance, in a typical Windows environment, one may find up to five dates associated with each file: file created, last accessed, last written, deleted, entry modified. All of these dates will not necessarily be available for each file. And each date has a different meaning. Following are the general meanings of these date references.

**FILE-CREATED DATE**

This is a record of when a particular file was created at the particular location where it is found. Thus, a file actually created before the end of December may have a file-created date in January of the following year if it is found by forensic accounting investigators on the desktop hard drive to which it was copied in the New Year.

**LAST-ACCESSSED DATE**

This date refers to the most recent time the file was accessed—by viewing, dragging, or even right mouse clicking. A file does not have to be changed for the last-accessed date to change.
It is important to note that certain automated processes, such as backup routines and virus-checking software, can change last accessed dates.

**LAST-WRITTEN DATE**

This date refers to the most recent time a file was opened, changed, and saved. Merely accessing the file without making changes will not change the last-written date.

**ENTRY-MODIFIED DATE**

Some file systems (notably NTFS [New Technology File System] and Linux) can store the date when the size of a file last changed. Changes to the file that do not affect its size will not change the entry-modified date.

Different programs may use different criteria when assigning dates of various types. It may therefore be necessary to research the particulars of a given set of dates if timing is important to an investigation. The above-mentioned dates are created independently of each other and can be quite useful in a review of documents. For example, Sarah Finch creates a document on July 27 and saves it on her computer. The system automatically ascribes the date saved: July 27. Two days later, on July 29, Sarah decides to make changes to the document, but she wants to backdate the changes made on July 29 to July 25, two days prior to the actual date of the primary document. With this in mind, on July 29 she changes the system date to July 25. She opens the document, reviews it, and closes it without making any changes. The following values will show for the four date fields:

**PRESENTING RESULTS**

The art of presenting results resides in one’s ability to communicate a message effectively to a specific audience. This is not always easy, particularly when information will be passed on to several different groups with different information needs and different levels of financial knowledge.

Lawyers and forensic accounting investigators are likely to need to see the full detail of all relevant transactions. Such data is most easily communicated in electronic tables, which can be queried and sorted as necessary. Any such tables must include the relevant primary keys to facilitate accurate referencing of transactions in subsequent communications. Files containing analysis results should be write-protected to prevent accidental alteration.

For planning purposes, a high-level overview is likely to be more appropriate.

The investigation leader should discuss his or her requirements with the analyst and decide on suitable grouping levels and on the types of aggregate figures required. The reports can then be designed to order and can include tables, graphs, and charts as necessary. Such summaries may also be appropriately given to clients or to prosecutors.
Any official report should include an appendix, detailing the source of the data and summarizing the data analysis process from extraction to reporting. The appendix should be referenced on all tables and charts.

Visual analysis programs usually work very well when they are incorporated into investigation support systems. In this way, the results of data analysis can be charted automatically, together with related findings from other investigative methods.

**REVIEWING THE ESSENTIALS**

In many data investigations, the principal forensic accounting investigator will manage the forensic technologist and ensure that the data analysis work gets integrated into the wider investigation. While playing this role does not necessarily require knowledge of technical procedures, the forensic accounting investigator should possess a good understanding of factors that affect the analysis: availability of data, specification of data extracts, skills required to prepare and analyze the data, and possible formats for the output of results.

One key factor to be determined at the planning stage is how the results should be incorporated into the investigation. To ensure a full and consistent audit trail through the evidence gathered, forensic accounting investigators should not work on stand-alone copies of results that must be updated every time an amendment is made to the analysis criteria. At the very least, primary keys should be retained so that any necessary updates do not have to be executed manually.
WORKING WITH ATTORNEYS

IN THE COMPANY OF LAWYERS

The first person to be contacted when there is a suspected fraud is typically in-house counsel. Depending on the apparent severity of the matter and its apparent location in the company, other internal resources to be alerted at an early stage, in addition to the board typically through its audit committee, may include corporate security, internal audit, risk management, the controller’s office, and the public relations and investor relations groups. Investigations usually begin with extensive conversation about who should be involved, and the responsible executives may naturally wish to involve some or all of the functions just mentioned.

Depending on the circumstances, the group of internal auditors can in fact be a tremendous asset to an independent forensic investigative team. As participants in the larger team, internal auditors’ knowledge of the company may improve both the efficiency with which evidence is gathered and the forensic team’s effectiveness in lining up interviews and analyzing findings. Our advice to client executives and in-house counsel is to engage an external team but to consider making available to that team the company’s internal auditors and other internal resources for any investigation of substantial size.

Forensic accounting investigators can expect to work with or for attorneys in a number of circumstances, including:

- Internal investigations with respect to accounting or reporting matters, generally triggered by:
  - Anonymous tips
  - Audit committee concerns
  - Internal audit concerns
  - External auditor findings
  - Media or regulatory reports or communications
- Regulatory investigations such as investigations by the U.S. Securities and Exchange Commission (SEC)
- Tax authority subpoenas or inquiries
- Civil litigation such as contract issues, shareholder lawsuits, wrongful termination claims, and fraud recovery actions

The number and kinds of attorneys are broad and varied. The forensic accounting investigator may work with the general counsel for the company; SEC counsel; special independent
(external) counsel to the board of directors or the audit committee, often referred to as 10A counsel1; attorneys for specific board or audit committee members; counsel for specific employees or groups of employees2; civil or criminal counsel; counsel for personnel who may be under suspicion or who hope to avoid that unwanted designation; and still others. The attorneys may be positioned as your client’s adversary or your client’s advocate, or they may be positioned as independent, as in the role of 10A counsel. It would not be at all unusual to have attorney representation of the following groups in a typical 10A investigation:

- The audit committee of the board of directors
- The company, defending against a potential SEC enforcement action or a U.S. Department of Justice (DOJ) indictment
- Officers or employees of the company, especially those named as “subjects” or “targets” enforcement actions or investigations. Each could have separate counsel.

Each attorney serving a client in this roster generally has varying interests to protect, timetables to work against, and different views as to the significance of specific documents, interviews, and theories. The forensic accounting investigator should keep in mind these varying perspectives throughout the investigation in order to avoid unintentional sharing of privileged information, loss of confidential points of strategy, and the like.3 While lawyers must adhere to ethical and legal guidelines, it is possible to communicate information accidentally, especially when working in physical proximity or with the same documents and personnel.

CONFIDENTIALITY REQUIREMENTS

A potentially material overstatement of asset values or understatement of liabilities is often the focus of investigation, and there may be an urgent need to inform stakeholders and markets that previously published financial statements may be unreliable. The extent of the problem should be determined and corrective action taken. In that scenario, a multitude of questions often swirl around the company:

Was the misstatement deliberate? Who knew or should have known of the misstatement?
What needs to be done?

In such investigations, confidentiality is usually very important. Leaks of information to the press or competitors may be particularly damaging. If the investigation is to be successful in uncovering the facts, the number of people within the company who are aware of day-to-day developments should be properly limited to avoid such leaks. The company may, however, voluntarily disclose information to regulators during such investigations. On occasion, the forensic accounting investigator may become involved in an external investigation in support of various law enforcement or government organizations such as the SEC, the DOJ, the Federal Bureau of Investigation, the Internal Revenue Service (IRS), or even state or local
prosecutors. This can come about in a variety of ways but typically occurs when the forensic accounting investigator’s client has decided to refer the matter for prosecution and offers the forensic accounting investigator’s assistance to the investigating agency. In such situations, attorneys for the government may find it useful to seek a 6(e) designation for the forensic accounting investigator. That designation grants the forensic accounting investigator access to grand jury or subpoenaed documents; forensic accounting investigators do not have subpoena powers, but they can review documents obtained through subpoena if working under a 6(e) order. While access to such information can be very helpful to the investigation, a 6(e) designation may require some modifications to the investigation process, which should be discussed with the investigating team, including counsel. When retained in such instances, the forensic accounting investigator should have a thorough initial discussion with counsel and the government agency to ensure that the ground rules are understood and that the forensic team is fully aware of required modifications to the investigation process or methods. Later in this chapter, we return in more detail to the topic of working with law enforcement or government organizations.

FORMING THE INVESTIGATIVE TEAM

Forensic accounting investigators are frequently called upon to investigate potential financial statement manipulations or misstatements and asset misappropriations.

For purposes of this discussion, we refer to such engagements as internal accounting investigations. When investigating asset misappropriation, company or by the outside attorney who represents the company.

The forensic accounting investigator conducting an asset misappropriation investigation typically receives excellent cooperation from company executives, who perceive themselves and the company as the victim. Experience has shown, however, that an investigation focused on asset misappropriation may produce evidence suggesting other schemes, in which the company may have been benefiting from illegal acts. Once the forensic accounting investigator picks up on a loose thread and follows it, there often is no telling where it might lead.

- Identification of an independent committee—generally a subset of the board of directors and typically the audit committee—to lead the investigation

And determine the company’s approach

- Initial communications with stakeholders, including employees, the market, stockholders, bondholders, lenders, and regulators

- Formation of an investigative team, generally through retention of appropriate counsel and other experts such as forensic accounting investigators and other specialists

- Urgent personnel decisions such as arranging for paid leave, restriction of duties or access, and termination
• Data stabilization and security to avoid any loss of critical information
• Notification of insurance providers at the company and board levels

The investigating team often includes:

✓ Independent counsel
✓ Forensic accounting investigators
✓ Forensic technology experts
✓ External auditor partner and key staff
✓ Based on the specifics of the investigation, the team may include other
✓ experts or specialists such as:
✓ Engineers
✓ Actuaries
✓ Tax experts
✓ Investment bankers
✓ Valuation or appraisal specialists
✓ Damages experts

How involved will the attorney be in the planning and execution of the investigation?

On one hand, the forensic accounting investigator may find that the attorney gives the forensic accounting investigator free rein to devise and execute a strategic investigative plan, subject to the attorney’s approval. That scenario is particularly likely in cases of asset misappropriation. On the other hand, some attorneys insist on being involved in all phases of the investigation. It is the attorney’s call. When engaged by counsel, forensic accounting investigators take direction from counsel. They should advise according to their best judgment but in the end they work at counsel’s direction.

Forensic accounting investigators bring a special skill set, perspective, and experience to the internal accounting investigation, complementary to the skills of auditors, counsel, and other experts typically involved in these investigations.

Capable forensic accounting investigators can be found within most large accounting firms as well as in boutique, or specialist, firms. Whether approached by counsel or directly by the company to participate in an internal accounting investigation, forensic accounting investigators should immediately assess their independence Once independence has been determined and forensic accounting investigators have been retained, those investigators
should obtain a thorough understanding of the respective roles and responsibilities of the various team members to allow for efficient and effective coordination across the team. Failure to clearly establish and fulfill roles and responsibilities may lead to wasted time and money—or worse, to gaps in the investigation process and incomplete or inaccurate results. These shortcomings may reduce the value of the investigation and may even subject the company and its officers and directors to adverse publicity or liability.

While it usually is easy enough in theory to delineate the team members’ responsibilities and to set up procedures that ensure communication across the team, it often is much more difficult to accomplish those things in practice.

Forensic investigations are often conducted in a crisis atmosphere that disturbs communication and allows duplication in the investigative process to slip through. In spite of deadline pressure and extensive work to be performed, time must be found to coordinate and share the information being obtained. When working with attorneys, forensic accounting investigators should specifically understand:

• Their expected role and responsibilities vis-à-vis other team members
• What other professionals are involved (current or contemplated)
• The extent and source of any external scrutiny (SEC, IRS, DOJ, and so on)

Any legal considerations (extent of privilege, expectation that the company intends to waive privilege, expectation of criminal charges, and so on)

• Anticipated timing issues, if any
• Expected form, timing, and audience of interim or final deliverables
• Specifics of the matters under investigation, as currently understood by counsel
• Any limitations on departments or personnel that can be involved, interviewed, or utilized in the investigation process

As noted at the beginning of this chapter, prudent forensic accounting investigators typically perform their assignment under the presumption that any deliverables, work product, or work process may become publicly available or accessed and utilized in civil or criminal litigation proceedings. That being said, when a company employs an attorney to represent it, the attorney’s work product usually cannot be subpoenaed. Attorneys enjoy a number of privileges that are necessary to ensure that their client can be completely honest with them without fear of disclosure.

The forensic accounting investigator who is employed directly by the attorney is considered an extension of the attorney, and the forensic accounting investigator’s work product may be protected from subpoena, unless the adverse party in litigation can prove, among other things, that there has been a “waiver of the privilege.” If work product or other privileged
information is intentionally shared with individuals outside the privileged group, the privilege may be lost.

The forensic accounting investigator should be careful to protect the privilege and should mark each and every individual document prepared with the caption “Privileged and Confidential—Attorney Work Product” or words to that effect.

This caption serves as a reminder and notice that the documents are privileged and not subject to subpoena or discovery. In practice, it is true that the privilege may be waived by the company and that the forensic accounting investigator’s spreadsheets, documents, and other working papers, as well as testimony, will be volunteered or subject to subpoena. It should also be understood that privilege is a jurisdictional issue and decisions can fall either way. However, when privilege is contemplated, it is still good practice to mark all documents with the privilege disclosure, so that they can be readily identified as privileged later on. It also makes it easy to determine documents prepared by the forensic accounting investigator as opposed to ones prepared by client staff.

Independent counsel, with the help of forensic accounting investigators, often takes the lead in setting up, organizing, and managing the investigative team. This process may include the selection and retention of other parties who make up the team. Independent counsel’s responsibilities typically encompass the following:

• Preparing, maintaining, and disseminating a working-group list (very helpful in sorting out which law firms or experts represent whom)

• Establishing the timetable in conjunction with the board of directors or management, disseminating the timetable to the investigating team, and tracking progress against it

**Forming the Investigative Team**

• Compiling, submitting, and tracking the various document and personnel access requests that the investigating team members will generate

• Organizing client or team meetings and agendas

• Preparing the final report with or for the board or its special committee, or doing so in conjunction with other teams from which reports are forthcoming

• Establishing and maintaining communication channels with the board of directors and other interested parties, generally including internal general counsel, company management, regulatory personnel, law enforcement or tax authority personnel, and various other attorneys involved

Although the attorney may lead the investigation formally, the forensic accounting investigator frequently is the cornerstone of a successful investigating team. The forensic accounting investigator may provide the following type of assistance and support for the larger team directed by the attorney:
• Ability to plan and conduct a proper financial crime investigation

• Expertise in accounting, in regulatory (such as SEC) auditing, in internal controls, and in financial analysis

• Interviewing skills, both fact-finding from witnesses and admission seeking from targets

• Expertise in performing data mining and data interrogation of the company’s books and records, including e-mail

• Experience in document authentication and knowledge of a network of subspecialists trained in highly technical authentication procedures such as typewriter/printer analysis and authentication through forensic laboratory science

• Ability to review and interpret internal accounting transactions and their compliance with various rules

• Ability to accumulate public financial and nonfinancial information, including SEC or company registry filings, if applicable

• Forensic imaging and other information technology (IT) expertise such as e-mail search tools

• Support of counsel in developing various hypotheses and investigative procedures and techniques

• Background checks on relevant personnel

• Vendor validity checks on the basis of publicly available information

• Preparation of specific sections of the draft and final reports or support of counsel for report sections that focus on accounting, reporting, or financial information

• Coordination with both internal and external auditors and the audit committee

• Review and critique of financial, accounting, or reporting analysis and advice provided by other specialists

• Among larger firms, a global network of investigators to assist in multinational investigations

Particularly when investigations include review and analysis of accounting and financial information, the forensic accounting investigator is often a critical member of the team. Some attorneys do not have extensive accounting or auditing experience, and certain accounting concepts may be foreign to them. In a recent investigation, counsel contacted the forensic accounting investigators as the final draft of the report was being prepared because counsel was uncertain about the concept of a “reserve”—its significance and how to explain it in the report. The forensic team gave an instant tutorial on how reserves can be manipulated and
then helped draft the relevant section. In another instance, counsel coordinated interview schedules with the forensic accounting team to ensure that an experienced SEC accounting specialist was available to participate with counsel in the interview of the company’s controller and chief financial officer (CFO). The SEC specialist’s participation turned out to be critical because the interview agenda included discussion of the adoption of two new accounting rules as well as discussion of the extent to which the external auditor was familiar with the new rules.

Forensic accounting investigators are frequently conversant in areas related to financial accounting and reporting such as valuation, tax, and financial aspects of human resource management, but “conversant” does not necessarily indicate a sufficient level of knowledge to guide a complex investigation. For complex investigations or investigations that involve public companies, it is often wise for the lead forensic accounting investigator to assemble a team that includes the following skills and experience:

• Ability to conduct or assist with the investigation

• Knowledge with respect to generally accepted accounting principles relevant to the applicable time period of the investigation

• Knowledge with respect to SEC-compliant accounting, financial disclosure, and other reporting

• Familiarity with the regulatory investigative process

• Knowledge with respect to generally accepted auditing standards and procedures

• Ability to immediately access industry or specialist knowledge as required—for example, expertise in derivative financial instruments, bank regulation requirements, and long-term contract accounting

• Familiarity with the uses and abuses of offshore companies and trusts

• Ability to identify departures from customary commercial behavior and business practices

• Relevant language skills and ability to meet the challenges of a geographically diverse investigation, as required

Each of the foregoing skills represents an area in which independent counsel frequently requires guidance and support by the forensic accounting investigator.

**Documentation**

While forensic accounting investigators often are critical components of an effective internal accounting investigation, it is important to remember that they are engaged as fact finders. Forensic accounting investigators may need to educate or remind counsel about the
limitations of the forensic accounting investigator’s expertise and scope of service. In particular, the forensic accounting investigator should take care to avoid:

• Providing legal advice or making legal assertions in their work or deliverables
• Providing actuarial or valuation guidance unless appropriately credentialed and trained
• Acting as a judge or jury by making judgments as to the guilt or innocence of particular people or groups
• Expressing an audit opinion on financial statements or internal control effectiveness.
• Creating legal exposure as a result of comments that may lead to claims of defamation, libel, slander, and the like

On occasion, the forensic accounting investigator may need to remind staff, other parties, and counsel of those limitations.

The board or special committee of the board, in conjunction with counsel, frequently issues a written report following an internal investigation, especially if the focus of investigation is a public company. The report may include work performed or evidence reviewed by the forensic accounting investigator, sometimes with an explicit reference to the forensic accounting investigator. For example, a report of the Special Investigative Committee of the Board of

• Information from the external auditor

CIVIL LITIGATION

If civil litigation is ongoing, the investigating team can utilize the discovery process to gain access to various types of personal information from the charged individuals not typically available to the team in the normal course of most investigations, including:

• Financial records
• Bank statements and account information
• Tax returns
• Asset ownership details
• Purchase, sale, and investment documentation
• Travel records or other data of interest to the investigation

In many investigations it is extremely helpful to learn whether the target has sources of income that cannot be explained. How to go about this? Courteously asking the individual to produce bank statements is usually unlikely to result in the individual’s compliance with the request, and from a strategic perspective, you will have tipped off the target that an
investigation is under way. The target may also decide to document for you only accounts that show benign and perfectly normal transactions.

INTERVIEWING

A few points should be summarized here about working with attorneys. It is not an uncommon practice for the investigating team to conduct a large number of interviews. Interviewing is a valuable tool in understanding an organization and individual roles, responsibilities, and perspectives. Interviews may extend beyond company personnel to include suppliers, customers, legal counsel, business partners, ex-employees, and still others.

When the investigation includes accounting issues, interviews typically encompass accounting and reporting personnel, management with responsibilities for the financial statements, the internal audit department, audit committee members and staff, external auditors, and perhaps others. The background and expertise of the forensic accounting investigator often are well suited to support counsel during these interviews. Unlike external investigations conducted by the SEC, DOJ, or IRS, internal investigations face a number of limitations, including:

• Lack of subpoena power. Interviews are voluntary, and the person being interviewed can walk away at any time.

• Testimony not under oath. The individuals being interviewed are not under oath to tell the truth, but lying to the forensic accountant may trigger liability under statutes that preclude such conduct.

• Interviews that is more informal than depositions. The output consists simply of interview notes taken by counsel or others participating.

EXTERNAL AUDIT FIRM

Before accepting a forensic accounting investigation engagement, the forensic accounting investigator should assess whether there are independence issues that disallow the engagement or limit its scope.

While it is true that one of the goals of the Sarbanes-Oxley Act is to mitigate independence concerns by identifying services that the external auditing firm is precluded from performing for audit clients, Congress did not want to restrict audit committees from engaging those professionals whom such committees regard as fully competent to perform investigations into allegations of financial improprieties. It may be entirely appropriate to engage forensic accounting investigators from the company’s external audit firm in some but not all situations.

The decision to utilize or to refrain from utilizing the external auditor firm to investigate allegations of fraud usually depends on several key factors, discusses later. When an audit committee is made aware of indicia of fraud or even the slightest suspicion of fraud, it
usually wants answers fast. Assembling a competent investigative team to fulfill the board’s responsibilities as quickly as possible is generally a high priority. In some cases, the quickest way to find valid answers to the questions asked by the company’s directors is to bring in forensic accounting specialists from the external audit firm. Are the allegations true? And if they are true:

• What are the financial implications?
• Who is involved in the alleged improper act?
• How significant and pervasive is it?
• How did it occur and go undetected until this time?
• What actions need to be taken to remediate the system of internal controls so that this does not happen again?
• Are we vulnerable in any other areas?

Those who would argue for a forensic accounting team from a firm other than the external auditors do so for reasons other than Sarbanes-Oxley, because Sarbanes-Oxley specifically allows for this. There may be a belief that the auditing firm cannot be independent; however, it has already been established that the external public auditing firm is independent: under no other circumstances could it perform the audit. There may be a belief that engaging the external audit firm would generate a conflict of interest. This may in fact be a valid concern—for reasons explored in Chapter 6. If there is a conflict, the appearance of objectivity may be impaired. When there is a concern that the allegation may lead to a potential restatement of the financial statements, a conflict of interest is entirely External Audit Firm possible. In that case, a forensic team independent of the external auditor would need to be retained—probably by counsel.

During a 10A investigation, counsel may be assisted by an independent forensic team. It is possible that the audit firm will deploy its own group of forensic accounting investigators in a specialist role, consulting with the audit team. The group will shadow the investigation conducted by company’s counsel to aid in bringing the investigation expeditiously to completion. This is not to imply that the audit team should in any way instruct the 10A investigative team on procedures that should be performed. It is the audit committee’s investigation. However, close and timely communication between the investigative team and the auditors is a good way to ensure that all parties, including the auditors, are comfortable that the investigation was conducted in an appropriate fashion and that findings were communicated to the auditors timely enough for them to react to the findings appropriately. Absent this level of cooperation, the auditors would not be informed of the investigative team’s findings until communicated by the investigative team to the audit committee and therefore could not begin their independent review of the support or bases for conclusions.
reached until subsequent to that communication. Alternatively, audit committees may retain a forensic accounting team from the company’s auditing firm to investigate, provided—as prescribed by SEC rules—that no regulatory proceeding or investigation has been initiated.

Under both scenarios (the audit firm’s forensic team is engaged or the audit firm shadows a forensic team engaged from another firm), the auditor is more than likely to require attorneys leading the investigation (10A counsel), on behalf of the company, to disclose the investigative findings and supporting evidence.

The auditor will be well-advised to inform the audit committee and its counsel in advance that the auditor needs to be kept fully informed. Notifying in this way may avoid difficulties at the conclusion of the investigation, which could delay the timely filing of SEC reports.

If a formal proceeding is initiated or the company is notified that it is the subject or target of an investigation by an enforcement agency such as the DOJ, the company should consider engaging a forensic accounting team independent of the auditing firm. It is still likely that the audit firm’s forensic accounting investigators will shadow the investigation for reasons mentioned earlier. The findings of that shadow team may be shared with the company and its counsel.

Duplication of efforts may be avoided or at least somewhat mitigated in this manner. For example, e-mails can be reviewed by the forensic team from the auditing firm and findings communicated to 10A or other counsel at the company’s direction. However, certain limitations would need to be well understood and respected. The auditing firm may not, for example, provide litigation support, a service specifically precluded by the Sarbanes-Oxley Act when a regulatory proceeding is under way.

Most auditing firms take the view that counsel appointed to conduct a 10A investigation must be independent of the company. This requirement does not mean that counsel is not permitted to have ever worked for the company before, but attorneys playing this role cannot be drawn from the company’s law firm of choice for prior litigation. Similarly, while knowing that it will shortly act as an advocate for the company in any enforcement action, 10A counsel cannot be expected to render an objective opinion on the possibility that an illegal act has been committed. Also, a forensic accounting team selected to support the company’s legal defense must likewise be independent of the forensic accounting team that assists 10A counsel. These are obviously intricate issues—with extended implications concerning who can do what while remaining strictly within regulatory guidelines.

It is possible to make available certain of the auditor’s working papers to the forensic accounting investigators assisting either 10A counsel or the company’s defense counsel. This may be accomplished through an access letter.

Before permitting access to the working papers, the incumbent accountant may wish to obtain a written communication from the firm providing forensic accounting investigative assistance regarding the use of the working papers.
These letters are not required by professional standards but certainly make good business sense. Why give voluntary access to a party that may later use what it finds as a basis to bring a claim against you?

Even with the client’s consent, access to the incumbent accountant’s working papers may still be limited. Experience has shown that the incumbent accountant may be willing to grant broader access if given additional assurance concerning the use of the working papers. Accordingly, the forensic accountant might consider agreeing to the following limitations on the review of the incumbent accountant’s working papers in order to obtain broader access:

Because your review of our working papers is undertaken solely for the purpose described above and may not entail a review of all of our working papers, you agree that (1) the information obtained from the review will not be used by you for any other purpose; (2) you will not comment, orally or in writing, to anyone as a result of that review about whether our engagement was performed in accordance with Statements on Auditing Standards; (3) you will not provide expert testimony or litigation services or otherwise accept an engagement to comment on issues related to the quality of our engagement.

Such letters will likely enable the recipients to review by sight only selected working papers. The access letters should restrict the use of the information and prevent both counsel and the independent forensic accounting team from assisting the company in any action against the audit firm.

WORKING FOR OR INTERACTING WITH LAW ENFORCEMENT OR GOVERNMENT AGENCIES

In the course of a forensic accounting investigation, the forensic accounting investigator often encounters law enforcement agents and prosecutors. Both will inevitably ask for information regarding the investigation. The forensic accounting investigator should determine from the client—and often, client’s counsel—what information the client wishes to turn over voluntarily. The client may decide it is advantageous to assist the prosecutor and may wish forensic accounting investigators to assist the prosecutor by turning over the results of their investigation, sharing information, or conducting additional investigation procedures as requested by the prosecutor. However, investigation processes often become more complex if the prosecutor makes grand jury material available to forensic accounting investigators for review.

Grand jury rules vary depending on whether it is a state or federal grand jury, but there are broad similarities. The grand jury conducts an investigation to determine whether there is sufficient evidence to indict. The prosecutor drafts an indictment, and the grand jury votes as to whether the evidence reviewed is adequate to support the indictment. Grand jury materials and information are confidential, and criminal and civil penalties are imposed for grand jury secrecy violations. However, the prosecutor may turn over subpoenaed information to authorized individuals, including law enforcement. Grand jury material may be shared with
other individuals in some circumstances in order to obtain information that furthers its investigation. Normally, an administrative process lists everyone who is authorized to access grand jury material. That list is detailed and precise, and only those listed are granted access.

If the prosecutor has requested that the forensic accounting investigator review documents obtained by the grand jury and if the client has agreed to such an arrangement, an interesting situation is created. The client is paying the fees of the forensic accounting investigator, but the forensic accounting investigator will in most instances be barred from giving any of the new information to the client. The client must be content that assisting the prosecutor corresponds to also assisting itself, even though that client will have no knowledge of the information to which the forensic accounting investigator now has access. When authorized to work with grand jury material, the forensic accounting investigator must make sure that the client understands the restrictions. The forensic accounting investigator must also (1) discuss in detail with the prosecutor how to ensure that there is no violation of the rules of access and (2) keep an open line of communication with the prosecutor for inquiries as to whether said accountant’s actions fit within the rules.

In some instances, state and federal prosecutors have hired forensic accounting investigators to conduct entire investigations, generally in situations in which the available law enforcement officers do not have the requisite resources. In such instances, the forensic accounting investigators’ involvement with the grand jury may be extensive and ongoing, and those investigators will be exposed to the full range of rules governing grand jury procedures and documents: the access rights of outsiders, the rights of subjects under interview, chain-of-evidence requirements, and the like. The forensic accounting investigators should work very closely with the prosecutor throughout the investigation and fully understand the rules and guidelines in advance.

**DISAGREEMENTS WITH COUNSEL**

From time to time, disagreements with counsel will arise when forensic accounting investigators are shadowing a 10A investigation. They are advising the auditors as to the conduct of the investigation and likely sufficiency to satisfy the auditor’s responsibilities under Section 10A of the Exchange Act. Such differences usually focus on the scope and strategy of the investigation. The authors have been fortunate to work with many bright, experienced, and informed attorneys who conduct their investigations with the expert skill and proper independent mind-set required of professionals charged with the responsibility of determining all the facts. On occasion, however, we have also found ourselves working with attorneys who are inexperienced at serving as independent

A recent SEC action has brought to the forefront the commission’s concerns about the conduct of some investigations. SEC enforcement director Stephen Cutler said in a September 20, 2004, speech that he is “concerned” that some lawyers hired to conduct financial crime investigations might actually have helped “hide ongoing fraud, or may have taken actions to actively obstruct such investigations.”
Judging by threatened enforcement actions and other communications, it appears the SEC is reviewing the quality and robustness of investigations, in which most decisions about procedures to perform and whom to interview are under the judgment of the lawyers charged with conducting the investigation.

There will no doubt be more to come on this issue, but early signs from the SEC should serve as warnings to lawyers that they should conduct financial crime investigations in a rigorous and robust fashion as an expected part of doing their job. The issue of the quality of investigation will continue to evolve, as evidenced by the SEC’s notification to a lawyer that he may face civil sanctions for his role in an investigation at a medical-device maker in Irvine, California. The unusual action of the SEC’s suing a lawyer over allegedly mishandling a corporate probe sends the message to lawyers that they must choose between serving as defense counsel and conducting a thorough investigation as independent professionals responsible to the audit committee, which serves investors’ interests.

Here are some examples to illustrate our point about selecting appropriate investigative procedures and executing them well.

• Gathering electronic evidence: Either electronic evidence should ideally be gathered by the forensic accounting firm’s own IT specialists or those specialists should closely supervise the company’s IT personnel. In addition, in some cases, forensic images should be made of hard drives and the like rather than merely copying them. And it is best to be more, rather than less, aggressive in choosing the number of personnel whose electronic data you select to examine. For example, the hard drive of a controller who has been accused by a whistle-blower of manipulating earnings is an urgent subject of forensic examination. It might be prudent to image the hard drives and examine the e-mail of some of those reporting to that controller as well as the controller’s administrative assistant.

• Interviewing: Chapter 18 explores this complex investigative procedure in depth. The complexity of the interviewing procedure is not always understood or respected. For example, we have seen certain lawyers approach interviewing as a simple note-taking exercise: put the documents in front of the subject, and write down what the subject says in response. That is clearly the wrong way to conduct an interview in these matters. Imagine you have discovered an e-mail in which the CFO writes, “Don’t tell the auditors about this transaction.” Before showing this email to the CFO, you would want to probe the subject through questioning:

“Have you ever instructed anyone to withhold information from the auditors?” This would be just one of many questions you would ask. You want to nail this issue down before producing the e-mail. Yet some lawyers would begin the interview by simply handing over the e-mail and asking the CFO to explain it. That gives the CFO ample time to come up with some inane explanation for making the comment.
Consider another example. A shipping clerk says in a preliminary interview that the supervisor said to record the goods as shipped, even though the goods were still on the dock. In order to get to the bottom of the matter, the lawyer decides to interview both the clerk and the supervisor together. Not surprisingly, the shipping clerk now changes his story to agree with the supervisor’s. The two should have been interviewed separately and instructed not to discuss the matter with anyone.

In situations in which you believe the lawyers are not conducting a robust enough investigation, it is wise to take your concerns directly to those charged with oversight of the investigation. It is ultimately their responsibility to ensure a thorough and proper investigation.
TEAMING WITH FORENSIC ACCOUNTING INVESTIGATORS

Forensic accounting investigators can make significant contributions to a financial crime investigation, provided that they can work effectively with the company’s internal and external auditors, as well as with other constituents involved in resolving allegations or suspicions of fraud. In addition to a thorough knowledge of accounting and auditing, the forensic accounting investigator brings to bear a variety of skills, including interviewing, data mining, and analysis.

Some auditors assume that auditing more transactions, with the use of standard procedures, increases the likelihood that fraud will be found. While this can prove to be true in some cases, when there is suspicion of fraud the introduction of competent forensic accounting investigators may be more likely to resolve the issue. This chapter explores how forensic accounting investigators can work effectively with internal and external auditors and considers the interests of other parties to an investigation.

Forensic accounting investigators work in a highly charged atmosphere and often present their findings in forums ranging from the boardroom and the courtroom to hearings before government agencies such as the U.S. Securities and Exchange Commission (SEC). Within the boundaries of an investigation, they typically deal with numerous constituencies, each with a different interest and each viewing the situation from a different perspective. These parties to the investigation may well attempt to influence the investigative process, favor their individual concerns, and react to events and findings in terms of individual biases. Forensic accounting investigators thus often have the task of conveying to all constituencies that the results of the investigation will be more reliable if all participants and interested parties work together and contribute their specific expertise or insight with truth-seeking objectivity. In the highly charged environment created by a financial crime investigation, the forensic accounting investigator usually bears much responsibility for displaying and encouraging level headedness.

All parties with a stake in the process—management, audit committee, auditors, and legal counsel—should consider including forensic accounting investigators in the process of decision making about the investigation. One of the key, usually, is the degree to which the forensic accounting investigators can work with and rely on the work of others—specifically, the internal and external auditors. Another common decision is whether forensic accounting investigators—with their knowledge of accounting systems, controls, and typical fraud schemes—may be added to the team that evaluates the organization’s business processes to strengthen the controls that allowed the fraud to occur.
Management may at first be inclined to push for a quick result because it feels the company will be further damaged if it continues to operate under a shadow. Senior executives may be unable or in some cases unwilling to see the full scope of issues and may attempt to limit the investigation—sometimes as a matter of self-protection—or they may seek to persuade the forensic accounting investigators that the issues at hand are immaterial. Whatever happened, it happened on their watch, and they may understandably be very sensitive to the forensic accounting investigators’ intrusion into their domain. Any defensiveness on the part of management should be defused as quickly and as thoroughly as possible, usually through empathy and consideration on the part of the forensic accounting investigators. The party or entity engaging the forensic accounting investigators—for example, audit committee, management, or counsel—may be committed to a thorough investigation of all issues and is ultimately responsible for the investigation.

The committee may engage forensic accounting investigators directly and look to them for guidance, or it may ask outside counsel to engage forensic accounting investigators, who usually will work at counsel’s direction in fulfilling counsel’s responsibilities to the audit committee. In some cases, the audit committee may need to work with two forensic accounting teams. One team, deployed by the external audit firm, gets charged with assisting the external auditors to meet their 10A responsibilities and provide advice on the adequacy of the investigation conducted by the company. The other team, engaged by 10A counsel, is responsible for an investigation that assists counsel and the audit committee in determining whether there was an illegal act and, if so, what remedial action is needed.

Many audit committees recognize that simply reauditing the suspect areas is unlikely to resolve the issues. They are also likely to realize that an overzealous witch hunt may alienate management and employees by implying loss of confidence in their competence or integrity. And deadlines—either self-imposed or imposed by a third party—such as a looming earnings release or regulatory filing may place significant pressure on the investigation. Amid all of these pressures, forensic accounting investigators should keep in mind the goals of all constituents yet conduct a dispassionate, objective, balanced investigation that is, to the best of their ability, on time and on target. Internal auditors are enjoying a resurgence of respect in response to recent regulatory requirements and the public outcry for better governance (see

Many companies are strengthening their internal audit functions, which vary in size, scope, focus,

Some internal audit units are powerful, with fully functioning administrations and a key voice at high levels, while others are less so. The practice of internal auditing recently experienced significant change—in light of the

For forensic accounting investigators, cooperating with internal auditors should be planned in a way that reflects the role of internal audit within the organization.
FORENSIC ACCOUNTING INVESTIGATORS’ COOPERATION WITH INTERNAL AUDITORS

Internal auditors bring a great deal to the table when there are concerns about financial fraud. However, most internal audit groups do not have a subgroup of forensic investigators. As such, outside forensic investigators are typically hired to assist internal audit conduct investigations. We have found in the majority of our experiences that teaming with internal audit enhances both the efficiency and effectiveness of the investigation: internal audit knows the company and its personnel and systems better than outside forensic investigators, which causes the investigation to be more targeted.

While it is ideal to work with internal audit in conducting investigations, it is important that a number of factors (explored later) be considered by those assigned the responsibility of conducting an internal investigation—usually the audit committee.

INTERNAL AUDIT’S POSITION AND FUNCTION Note the group’s position in the company’s organizational chart and its actual, day-to-day role—which due to any number of factors may differ from the role implied by the organizational chart. For example, internal audit’s function and reporting relationship may have, by necessity, been diverted in the period following enactment of the Sarbanes-Oxley Act, wherein companies were working to document and assess financial-reporting internal control structures as required by the Act. Begin this assessment with internal audit unit. If possible, consider the way in which the internal auditor is measured by the company with respect to coverage, number of locations visited, types of issues raised, financial savings, and improvements to operating metrics.

Among the considerations are the following:

- Is the internal audit unit focused on controls assurance—typically evidenced by location-based or compliance auditing—or on controls consulting, typically evidenced by forward-looking projects, early involvement in system deployments, and so on?

- Does the internal audit plan comply with IIA standards for a risk-based approach—usually in the form of a risk assessment? A coverage-based metric, such as a site visit to every location every three years, is evidence that risk is not the primary driver.

- Are any internal auditors trained in forensic investigative accounting?

How experienced are they? Do they provide for a separate and distinct group of investigators? When fraud is suspected, do the internal auditors conduct investigations by means of this specialized group of forensic accounting investigators, or do they use auditors already assigned to the particular project?

- Is there consensus about the role of the internal audit unit within the organization?

- Are internal audit’s recommendations implemented, and if not, why not?
All internal audit units must grapple with the issues of independence and conflict of interest. The auditors cannot fulfill their obligations without independence of mind and action, but the types of work they perform call for coordination with operational management. This is a balancing act, and it can often generate tension. How much of the internal audit budget is available to auditors at their own discretion? Are the audit strategic plan and budget developed by the auditors themselves, or are they heavily influenced by the chief financial officer? Has the internal audit unit aided in forensic investigations in the past? Experienced auditors are likely to understand the imperatives and the required mind-set, while inexperienced auditors, however skilled in other elements of internal auditing, may require a strong lead throughout the investigation.

A high degree of correlation usually exists between the level of empowerment granted to the individual and the independence and effectiveness of that individual’s performance. Many internal audit units are oriented toward compliance or operational efficiency and not financial crime investigation. Internal reporting relationships and organizational tone may either enhance or severely limit the effectiveness of the internal audit unit. Most often, the formal report is made to the audit committee, but there may be an administrative reporting relationship with the finance auditor evaluated and by whom? What degree of interaction exists between the internal audit group and the audit committee? Do the two meet frequently and discuss matters in depth, or do they meet only at several formal meetings a year?

RESOURCE MODELS

The internal audit unit’s mission also usually drives operational issues such as the resource model, annual budget, and auditing plan. Among the questions and issues that normally need to be considered in an evaluation of the resource model are the following.

• Whom does the internal audit group principally hire: accounting and controls specialists, certified fraud examiners, certified public accountants (CPAs), MBAs, new or experienced people, internal recruits?

• How are the internal auditors trained? Is their career path restricted to accounting and controls, or does it enter into operational areas of the company?

Do internal auditors rotate through internal auditing and then move such a practice may be counterproductive to building a deep skill set of forensic investigation abilities within the internal audit group.

• Whether the internal audit draws entirely on in-house resources or is sourced is not a significant issue unless the views of the sourcing partner differ on methodology, tools, and approach. These issues should be considered in a determination of what support is available, together with the contractual arrangements with the co-sourcing partner. Sourcing is usually done for one of two reasons: to fill gaps or to build a function. The company may have an internal audit unit but lack specialized information technology resources and look to a source provider. Building a function involves obtaining a capability quickly while providing
knowledge transfer from outside forensic accounting investigators to company employees. On one hand, when the source partner is filling gaps, the mission, direction, and sometimes the supervision of day-to-day work are in most cases controlled predominantly by the company. On the other hand, when the source partner has been hired to build or reengineer the function, the company normally sets the mission and overall direction, but the source provider usually exercises tactical leadership.

WORKING TOGETHER

After gaining a thorough understanding of the factors discussed earlier, consider ways in which the investigative team can best work with the internal auditor and be prepared to make recommendations to the audit committee. Each group brings different skills to the task, and the best solution is usually one that incorporates both working together. The internal auditors usually bring:

• Core skills in auditing. Collecting and corroborating documentation, sampling, interviewing, and testing and analyzing data

• Core skills in project management. Planning, scheduling, document management, creating audit steps (including follow-up), managing issue resolution, and recording and communicating results

• Knowledge of the company and systems. Organizational structure, how transactions take place, how errors are likely to evidence themselves, and the strengths of the company’s people, systems, and processes

3. When staffing an internal audit unit whose mission emphasizes consulting activities, the human resources department of a company may bring MBAs rather than CPAs on board. However, the

MBA skill set may not be as valuable to a forensic accounting investigation as fundamental auditing experience and the ability to understand how financial transactions are recorded.

With these competencies, the internal auditor is very well positioned to obtain background information on people, systems, and processes. Past audits may provide insight. The auditor is also a valuable team member in collecting data or serving as an adviser to the forensic investigators on matters of approach, specific issues that come to light, and potential follow-up actions.

At the same time, all parties should acknowledge that normal auditing protocols do not apply. Sending out announcements of visits and advance requests for documentation may not be consistent with the objectives of a forensic accounting investigation. The internal auditors’ cumulative knowledge of the company can be a powerful frontline force in detection and deterrence. Bear in mind, however, that knowledge of the entity can cut both ways: as an efficient jump start or as a set of assumptions that may hinder objective investigation.
The audit committee or whoever carries ultimate responsibility for the investigation might choose to have it conducted without input from or reliance upon internal resources. The forensic accounting investigator may be asked for input into this decision and should be prepared to respond appropriately. The foregoing discussion of factors to consider may be helpful for all parties involved in conducting investigations.

**FORENSIC ACCOUNTING INVESTIGATORS’ COOPERATION WITH EXTERNAL AUDITORS**

The external auditors of a company are commonly engaged to perform an audit under generally accepted auditing standards, and the primary focus of those external auditors is on auditing the financial statements in compliance with professional standards. How well forensic accounting investigators interact with external auditors typically depends on several factors, including the following.

**CLIENT HISTORY**

The external auditor may be a trusted adviser or may have a strained relationship with the company owing to previous events. Because the forensic accounting investigator is often placed between the company and its external auditor during an investigation, understanding their current relationship is likely to be critical to successful communication during an investigation.

Because external auditors likely know the company better than a newly appointed team of attorneys and forensic accounting investigators, selected in part because of their limited prior experience with the company, they may be very useful sources of information. The audit firm’s knowledge about a company’s areas of risk, business processes, documentation, systems, and personnel can get the investigative team off to a fast start. The forensic accounting team will also be able to use the auditor’s working papers and audit staff to assist in gaining an understanding of the client’s systems, culture, and personnel, as well as other important data. Gaining access to information contained in the working papers of the external auditors may require formal access letters, the terms of which should be carefully considered by counsel. Also, the process of obtaining access letters may often take time away from getting the investigation started promptly.

Forensic Accounting Investigators’ Cooperation with External Auditors

There are situations permitted by law and professional standards wherein an audit committee may retain a forensic accounting team from the external auditor’s firm. Considerations in choosing this option include timing, knowledge of the company’s accounts, systems, personnel, and industry specifics. Relying on a forensic team from the external auditors has an added benefit: the audit firm and hence its forensic accounting team are independent, whereas the other immediately available resources such as the internal audit team or the company’s general counsels’ office is not. A discussion of the rules allowing these services is
found in Chapter 6 (see discussion surrounding our commentary regarding Rule 2-01(c)(4)(x) of Regulation S-X and Exchange Act Rule 10A-2).

Note, however, that the nature of the allegations or certain external events such as the commencement of a lawsuit or a regulatory investigation may require the audit committee to insist on several degrees of separation between the external auditors and the investigative team—especially if the cry “Where were the auditors?” has already been raised.

THE EXTERNAL AUDITOR IN TODAY’S ENVIRONMENT

To meet capital markets’ expectations that financial statements must not be tainted with material fraud and in compliance with the new regulatory requirements of Sarbanes-Oxley, the external auditor will be involved to some extent in most investigations. This is particularly so in situations involving allegations that the financial statements may have been affected by an illegal act. Any investigation to assess this concern will likely be conducted by the audit committee, the process and results of which will be closely monitored by the auditors in accordance with their responsibilities under professional standards and 10A of the Exchange Act. Many external auditors will not complete their audit fieldwork until the investigation is complete and they have access to the findings and the company’s remedial action plan.

Recognizing the responsibilities of the auditor, the investigation team (counsel and forensic accounting investigator) may consider asking for input from the external auditor early on in the investigation. If there is a disagreement with the external auditor on scope, approach, or procedure, the forensic accounting investigator should find that out earlier rather than later and work through the issues raised. The work and findings of the 10A counsel team cannot be kept entirely from review by the external auditors. While 10A counsel and their forensic team may draw certain boundaries around work relating to legal advice and other matters of privilege, it is generally best to include the external auditors in significant aspects of the investigation with periodic reports. Without this level of cooperation, time to complete the financial statement audit once the investigation is completed may be extended while the audit partner digests the findings, establishes the scope of and carries out related audit work, and evaluates the remedial actions, control implications, and financial statement disclosures. Invariably, the question of the attorney work product and attorney–client privileges arises when the question of sharing the findings of the investigation gets discussed.

This is a complex question and the subject of evolving law. Accordingly, audit committees, auditors, and forensic accounting investigators should be prepared to evaluate the specific circumstances of each situation with counsel before reaching a conclusion. It must be recognized, however, that the external auditor has a legitimate need for fully comprehending the scope, findings, and remedial actions taken as a result of the investigation, which may, under certain circumstances, implicate the privileged nature of certain aspects of the investigation.
Auditors are generally well advised to inquire at both the beginning and the end of an investigation as to whether any material either will be or has been withheld from them because of privilege issues. It may be simplest for the auditors to tell the audit committee, with its 10A counsel present, that they need to be informed at any point in the investigation when the privilege is being asserted.

I OBJECTIVES OF ALL INTERESTED PARTIES

The forensic accounting investigator must bring independence and objectivity to the investigation and recognize the objectives of each of the interested parties to the investigation.

FORENSIC ACCOUNTING INVESTIGATORS’ OBJECTIVES

Forensic accounting investigators’ objectives are determined by the scope of work and the desire to meet the goals of whoever retained their services. Regardless of the differing interests of the various constituencies, forensic accounting investigators must typically answer the following questions:

• Who is involved?
• Could there be coconspirators?
• Was the perpetrator instructed by a higher supervisor not currently a target of the investigation?
• How much is at issue or what is the total impact on the financial statements?
• Over what period of time did this occur?
• Have we identified all material schemes?
• How did this happen?
• How was it identified, and could it have been detected earlier?
• What can be done to deter a recurrence?

Forensic accounting investigators should always keep in mind that they are primarily fact finders and not typically engaged to reach or provide conclusions—or, more formally, opinions.4 This differs from the financial auditor’s role, as often

4. The exception is that in civil litigation, a forensic accountant may be asked to opine on the existence of fraud under the civil evidence standards, wherein the existence of a tort is based on a preponderance of the evidence, as opposed to the stricter, criminal evidence standard of “beyond a reasonable doubt.” A forensic accountant who is asked for an opinion takes on elements of the role of auditor and must determine whether the nature, scope, and timing of the procedures were or is sufficient.
Objectives of All Interested Parties

The financial auditor is presented with the books and records to be audited and determines the nature, extent, and timing of audit procedures. On one hand, the financial statements are management’s responsibility, and an auditor confirms they have been prepared in accordance with generally accepted accounting principles after completing these procedures and assessing different set of skills and works at the direction of an employer that may be management.

The selection of audit procedures is judgmental and an integral part of the audit team’s responsibilities. Not surprisingly, when auditors choose to enlist the services of subject matter expect the investigators to offer suggestions on appropriate procedures to be performed as well as related costs, risks, and expected outcomes. The investigators should be careful not to execute such procedures unless specifically asked to do so by the audit team (or whoever is directing the investigators). This approach can lead to frustration on the part of the investigators if, during an investigation, forensic accounting investigators are ordered to stop and in effect put down their pencils. Should that situation occur, it may be entirely appropriate to discuss their concerns with the audit team. But keep in mind that the audit team is generally more knowledgeable about the client’s business as well as other audit procedures that may mitigate the forensic investigator’s concerns. In extreme cases, it may be appropriate to resign in protest, an eventuality discussed in more detail later. But the forensic accounting investigators should take direction from those who engage them, as requested, be they auditors, directors, or counsel.

OBJECTIVES OF OTHER PARTIES TO THE INVESTIGATION

During an investigation, each interested party may view the same facts differently.

For this reason, it is important to understand the likely biases and goals of all stakeholders and to view, in a broad context of expected and quite naturally differing points of view, any conflicts that may emerge.

Management understandably may be eager to bring the investigation to a quick conclusion. The chief financial officer may be defensive over the fact that his or her organization “allowed this to happen.” The CEO may be concerned about the investigation’s impact on share price, company reputation and liability, and employee morale. Perhaps citing cost or scope issues—but likely more concerned about staying as close as possible to events as they unfold in the interest of no surprises—management’s overall reaction may be too tightly manage the investigation.

The board of directors, through the independent members of its audit committee, is likely to focus on conducting a thorough and complete investigation, but its members may lack the experience needed to assess the effort. In addition, they may be concerned about their personal reputations and liability. The board is likely to look to legal counsel and in some cases, to forensic accounting investigators to define the parameters of the project. the U.S.
Department of Justice (DOJ), have enforcement and prosecutorial objectives beyond the scope of the investigative team’s objectives.

Counsel will act in the best legal interests of its client, which could be the management team, the audit committee, or other directors, with the exception of counsel engaged to conduct a 10A investigation. Such 10A counsel must conduct an independent investigation free of the advocacy role required of counsel engaged to prepare a defense of the company in a pending civil litigation, or DOJ or SEC, or other regulatory agency investigation. The role required of forensic accounting investigators by the legal team may vary depending on the team’s needs. As such, the forensic accountants should not expect to participate in all activities typical of financial crime investigations. For example, the legal team may or may not see a need to include the forensic accountants in all interviews, favoring instead to have them attend only those interviews in which the legal team expects accounting issues to surface. In most investigations in which counsel is involved, they are responsible for the conduct of the investigations and will assign and allocate resources accordingly.

The internal auditor may have a variety of objectives, including not alienating management, staying on schedule to complete the annual audit plan, and not opening the internal audit team to criticism. The internal audit team may also feel embarrassed, angry, and defensive that it did not detect the wrongdoing.

The external auditor may have several concerns, including whether the investigation team will conduct an investigation of adequate scope, whether the situation suggests retaining forensic accountants from the auditors’ firm, whether forensic accountants should be added to the audit team, and even whether the investigation will implicate the quality of past audits. Registered independent accounting and auditing firms are good places to look for forensic accounting investigators. However, in light of the requirements of the Sarbanes-Oxley Act, in some circumstances the external auditors may not be engaged and additionally, when they can be engaged, some audit committees are nevertheless averse to engaging forensic professionals from their external auditing firm.

Additionally, there will likely be situations in which auditors may elect to consult with a forensic accounting investigator from their own firm regarding the proposed scope or method of an investigation being conducted at an audit client. For example; the law firm conducting a 10A investigation may decide not to conduct an e-mail review as part of its investigation. This decision may or may not be appropriate. Consultation with a forensic accounting investigator may assist the audit partner and the partner’s team in assessing the scope of

**How Should the Investigation Objectives Be Defined?** Investigation either proposed or performed. As an example of a detailed issue pertaining to scope, in some investigations e-mail is obtained by “copying” the relevant server files. The audit firm’s forensic team might suggest that hard drives found on personal computers, portable mass storage devices like pen
drives, personal digital assistants, and the like be imaged instead of simply copied, so that files not retained on the servers as well as deleted files are captured.

Audit partners may use their firm’s forensic accounting investigators to assist in a variety of ways, including:

• Receiving detailed reports of questions and facts discovered by 10A counsel:

Attending selected interviews with 10A counsel and/or counsel’s forensic accounting advisers may be appropriate in some situations as well. Expanding the audit tests of certain accounts

• Attending updates meetings called by 10A counsel to advice on the progress of an investigation

If the forensic accounting investigators are from the audit firm, the firm may expect to be involved in the procedures and findings at every stage. Some counsel and boards view this as a barrier to hiring the audit firm’s forensic accounting investigator to conduct the investigation; however, no matter who completes the investigation, critical information must still be communicated to the auditors.

Stockholders may become concerned once suggestions of financial impropriety surface. They may file a class-action lawsuit with the objective of extracting the largest possible settlement from the company and other parties, including the external auditors.

The company’s lenders are likely to be concerned about their exposure to losses. The investigation may take place during a period of financing negotiations and may therefore need to address the lenders' objectives.

The public at large may feel some degree of vested interest in the investigation, particularly if the entity is a public, quasi-public, or charitable organization or if it is a significant regional employer. These concerns are often reflected in and fed by media attention, and they create pressure to “get to the bottom quickly.”

HOW SHOULD THE INVESTIGATION OBJECTIVES BE DEFINED?

Forensic accounting investigators should develop a plan that offers the client investigative alternatives. The investigation should obviously focus on the facts that cause concern, with the ultimate objective of determining if an illegal act has been committed. In their quest to achieve the objectives of the investigation, forensic accounting investigators must be mindful that they are governed by the ethical principles and other guidelines of the authoritative professional organization(s) to which they belong—be it the American Institute of Certified Public Accountants, the Association of Certified Fraud Examiners, or both.

The forensic accounting investigator should recognize that auditors may be apprehensive when confronted with issues of fraud—and appropriately so. Sensitivity to auditors’ concerns will go a long way toward easing their natural disquiet when it is determined that the
company has begun an investigation to evaluate allegations of fraud. Keeping auditors informed in an appropriate manner, agreed to by the client, will help ensure the efficiency of the financial statement audit.

In earlier chapters of this book, the issue of financial statement materiality has been raised more than once. In the course of an audit, numerous immaterial variances and adjustments are identified, documented in the working papers, and never adjusted on the books and records of the company. This is appropriate and consistent with auditing standards. Materiality is a filter that allows the auditors to work efficiently and effectively. In the course of a financial investigation, however, a small fact, immaterial under normal circumstances, may have a critical bearing on the overall investigation.

WHO SHOULD DIRECT THE INVESTIGATION AND WHY?

A ship has but one captain and, generally, a company’s audit committee must proactively lead the investigation. Forensic accounting investigators follow the evidence wherever it leads and communicate their findings to the audit committee or to the committee’s designee, such as counsel, whose decisions direct the conduct of the investigation. While the external auditors must be satisfied that the audit committee has directed a proper investigation, they neither direct the investigation nor decide what remedial actions are required by the circumstances.

Financial crime investigations are fraught with uncertainty, and a wrong move can produce harmful results. Audit committees recognize the value of consulting with a competent team of advisers, including counsel and forensic accounting investigators. A forensic accounting investigator working for an audit committee that does not seek advice or that interferes with the investigation would be well advised to resign the assignment.

In the course of an investigation, a time may come when the forensic accounting investigator is alone in advocating a certain course of action or series of procedures.

Suppose the audit committee interprets whistle-blower allegations as implicating the revenue recognition practices of the company but not policies involving the deferral and amortization of related marketing costs, and the forensic accounting investigator disagrees? What is the forensic accounting investigator to do? The evidence should be the driving force in determining the scope and course of the investigation. On one hand, in situations of this kind, be insistent. Historically, materiality has been evaluated primarily by using quantitative measurement standards such as X percent of total assets or net income. In 1999, however, the SEC released Staff Accounting Bulletin 99 (SAB 99), which reemphasized the view that materiality, should be evaluated from a qualitative as well as a quantitative standpoint. View at while following the standards, methodologies, and practices that experience suggests are most appropriate in the circumstances. On the other hand, unlike decisions about the scope of the audit procedures—which rest solely with the auditors—decisions about the adequacy of an investigation’s scope
rest with the audit committee. Typically, the best and most practical use of a forensic accounting investigator is to conduct sufficient procedures to unambiguously resolve the allegations. This is the clearest outcome of an investigation. There is, of course, another outcome: “We conducted our investigative procedures and noted no evidence of fraud.” This may or may not be acceptable, depending upon whether the investigation was robust and thorough. A no-fraud-found result could amount to a comfort level consistent with the objective of the investigation at its outset: that of resolving the allegations. Or, if those who evaluate the outcome of the investigation—such as the auditors or the SEC—conclude that procedures were not robust and thorough, it will be difficult for them to arrive at a satisfactory comfort level with a finding of no fraud. In situations in which a no-fraud finding is the investigative result, the adequacy of the scope is often a key element in justifying the conclusion.

Ideally, the forensic accounting investigator should have significant influence over procedures pertaining to the financial aspects of the investigation.

Counsel should obviously take responsibility for the legal aspects of the matter and support the efforts of the forensic accounting investigator by providing appropriate guidance. The audit committee should rely on these and other professionals, but in the end it is the audit committee’s investigation. The committee must take ownership, albeit with the advice of other parties in the core team that influences the direction of investigation. These may include forensic accounting investigators, legal counsel, internal and external auditors, and possibly others such as a public relations firm. Conferring early and often is routine in these matters and should be strongly encouraged by the forensic accounting investigator.

**READY WHEN NEEDED**

While fraud is not an everyday occurrence at most companies, boards and auditing firms should anticipate the need to conduct a financial fraud investigation at some time in the future. To this end, they may establish protocols that ensure that if fraud exists, there is a high probability that it will be identified completely and dealt with in a timely and correct manner.

Companies and auditors alike may gain benefit from considering (1) whether heightened risk of fraud exists and (2) when there is heightened risk of fraud, what would be an appropriate audit response to the heightened risk. Once indicators of fraud have been identified, a protocol may be put in place for conducting an investigation. If this planning takes place long before the need for an investigation, the procedures can be vetted by all relevant personnel, including the audit committee, management, the legal department, human resources, risk management, and internal auditors.

The external auditing firm may also want to develop a protocol for handling possible red flags and suspicions of fraud. An auditing firm’s basic vision as to how to deploy resources for addressing these concerns would typically address many of the points covered in the sidebar entitled Fraud Response Protocol, which follows.
WHERE TO FIND SKILLED FORENSIC ACCOUNTING INVESTIGATORS

INTERNAL AUDIT

When the need arises for an investigation within a company, management or in-house counsel might naturally first look for a forensic accounting investigator in the company’s internal audit group. Owing to a number of constraints, however, companies and their lawyers often find themselves sooner or later having to look to outside resources. The first and foremost constraint may be a lack of experienced forensic accounting investigators in the internal audit unit. Many companies have the practice of rotating accountants and auditors (as well as other operational disciplines) through their internal audit groups for a variety of reasons.

However, rotation makes it difficult to cultivate the deep skill sets of forensic accounting investigation—for example, interviewing skills.

When an investigation is needed, it is best to deploy the most experienced fraud detection experts available. In actual practice, there is often a strong desire to use the internal auditors: they are already on site or nearby, and it would appear to be most cost-effective to engage this internal resource in the investigation.

This strategy can be most effective if companies develop groups of forensic accounting investigators within internal audit. In the absence of experienced, in-house forensic accounting investigators, our advice is to look outside the company when the need arises.

Internal auditors need access to the same fraud detection and deterrence skills as outside auditors. They may have robust audit programs to deploy on the traditional preventative, cyclic, or rotational basis, absent any specific concerns about possible fraud. Should someone in the organization express specific concerns, even in a general way, consideration should be given to deploying forensic accounting experts. Because audit committees look to internal auditors as the primary group focused on fraud detection and deterrence, a certain number of internal audit professionals should consider attaining the certified fraud examiner (CFE) designation. When testing identifies any situation in which a suspicion of fraud arises, company policy should provide for consultation with professionals from the organization’s risk management and forensic accounting groups.

Building the right investigative team is part of the challenge facing audit committees.

The combination of internal and external resources can greatly enhance the investigative effort if undertaken with eyes wide open, with experience as a guide, and with a deliberate approach.

ENGAGING EXTERNAL FORENSIC ACCOUNTING INVESTIGATORS

If forensic accounting investigators are unavailable within the company, a variety of professional services firms can provide them. Those firms include:
• The external auditing firm
• Registered independent accounting and auditing firms
• Consulting firms (non-auditing and unregistered)

What are the criteria for choosing among these service providers? Care is, of course, needed. Unfortunately, people sometimes identify themselves as forensic experience. No formal requirements in terms of education, specialized training, or experience help the buyer of these services gain some initial sense of the service provider’s real capabilities. The area of forensic accounting investigation has become popular of late, and some firms have added the specialty to their service offerings despite a lack of strongly credentialed, thoroughly experienced professionals. Companies and their lawyers should, therefore, consider quite a

The requisite skills and experience appear in the following, by no means exhaustive, list:

• Technical qualifications, including certifications such as CPA and CFE
• Experience in forensic accounting investigation, with a track record of successfully and unambiguously resolving allegations
• Global resources
• Forensic technology tools and the experience to deploy them
• The ability to understand complex business transactions and their effects on financial statements
• Knowledge of criminology and the workings of the white-collar criminal’s mind and methods
• Testimony experience before regulators such as the SEC and DOJ and at deposition or trial
• Forensic interviewing experience
• Ability to work effectively in an unstructured and dynamic environment
• Patience and listening skills
• The ability to approach situations objectively and without bias
• Persistence and the will to ask tough questions and deal with difficult, high-stress situations
• Integrity
Many forensic accounting investigators would take the position that the typical financial statement auditor may wait too long before calling in the forensic accounting investigator. But no savvy auditor reading these words will fail to notice the possibility of bias in the statement; after all, this book is written by a team of forensic accounting investigators. And so, part of the aim of this chapter is to demonstrate that the decision regarding when to call in the forensic accounting investigator can and must be viewed in an objective light. Before proceeding further, readers might find it helpful to review Chapter 1, where we introduce the concept of using forensic accounting investigators on audits when suspicions arise.

The thoughtful and efficient use of forensic accounting investigators often offers the right balance between conducting routine audits and investigating for possible fraud. A predicate must exist before an investigation is undertaken. A predicate is the totality of circumstances that would lead a reasonable, professionally trained, and prudent individual to believe a fraud has occurred, is occurring, and/or will occur. Predication is the basis for undertaking a fraud investigation. It would be inappropriate—and a violation of the Association of

Some auditors may call in forensic accounting investigators at the slightest suspicion of fraud. Year after year, they may bring in these forensic accounting investigators at the same client; their mind-set is to consult early and often—not only with forensic accounting investigators but also with industry experts and

the risk-and-quality auditors who typically provide, from the center of major accounting firms, an internal consulting service for audit teams in the field.

Auditors who rely on forensic accounting investigators at the first sign of possible fraud usually recognize that the skill set of fraud accountants differs from their own. Just like the actuary called in to evaluate the pension benefit accrual or the tax specialist who reviews the tax accrual, the forensic accounting investigator brings the experience and training required to properly evaluate suspicions of fraud. In our perhaps biased view, at the very first sign of fraud, consideration should be given to bringing in the forensic accounting investigator to evaluate.

At the other extreme are auditors who believe they possess the know-how to conduct forensic investigations but they may not have trained, or trained sufficiently in the field, and certainly lack sufficient experience to meet the circumstances that may arise as an investigation develops. When they grow suspicious of fraud, they often test, they often inquire.
TODAY’S AUDITORS ARE NOT FORENSIC ACCOUNTING INVESTIGATORS

Many outside the profession believe auditors have received extensive training in the skills of forensic accounting investigation. This is not so for most auditors.

Undergraduate accounting programs do not, to the best of our knowledge, require courses in forensic accounting investigation, although some offer elective courses. The authors of this book are not suggesting that auditors be trained as forensic accounting investigators for all the reasons we have addressed, but principally because the discipline of forensic accounting investigation is an art requiring a different set of skills, training, education, and experience. What we expect to evolve in the education of future accountants is a curriculum that increases students’ awareness of detection techniques as well as instruction that enables them to have an appreciation for the capabilities of forensic accounting investigators. In this way these accounting graduates—whether they find their place in the business world in operations, management, or internal audit or as independent auditors—will better know the footprints of fraud and when to call upon the forensic accounting investigators.

AUDITORS ARE NOT AUTHENTICATORS

Auditors are not responsible for detecting counterfeit documents. Any respectable fraudster with access to a color printer or copier can create a false paper trail that would deceive even an experienced auditor. We’ve seen situations, in which entire sets of documents had been created—in some cases, overnight—to deceive who are not routinely trained or necessarily experienced in spotting altered or forged documents. The auditor’s professional standards do not hold auditors responsible for detection if a fraud is concealed by fraudulent documents. However, auditors armed with a healthy dose of skepticism will question the source from which they obtain information, recognizing that that information could be fraudulent.

AUDITORS HAVE LIMITED EXPOSURE TO FRAUD

Nothing short of repeated exposure to fraud can prepare one for effectively investigating frauds. Those who go on to become specialized forensic accounting investigators develop a keen sixth sense that supports the set of skills required for the resolution of complex fraud schemes.

When forensic accounting investigators launch a fraud investigation in an environment in which the perpetrator is unknown, they usually begin with interviews numerous enough to identify possible targets. During that process, they often hear such comments as: “Oh, it can’t be Kathy. Kathy is one of our most loyal, long-term employees. She rarely takes time off, always works late, and helps others with their jobs. She’s friendly, religious . . .” and so on. Such a commentary on Kathy’s work ethic and personality has no impact on the forensic accounting investigator’s attitude, which must remain one of professional skepticism. The great majority of friendly, hardworking employees are honest; they are what they seem. However, most fraudsters also seem to be honest. The word con is a shortened form of the
word confidence. Fraudsters seek to gain one’s confidence, and the best of them are very good at it.

AUDITORS ARE NOT GUARANTORS

For most of the past century, many participants in business—as well as some courts that adjudicated business disputes—believed that the auditor “certified” a company’s financial statements, thereby becoming the guarantor of those statements’ accuracy and reliability. However, in the mid 1980s that understanding of the auditor’s responsibility changed dramatically with the Tread way Commission report. The commission found that responsibility for reliable financial reporting resides “first and foremost at the corporate level.” The commission defined the auditors’ role as “crucial but secondary” and explicitly stated that the outside auditors’ role was not that of “guarantors of the accuracy or the reliability of financial statements.”

Later, in accountant liability litigation, the courts began to reshape their view of the auditor’s role. Notably, in Billy v. Arthur Young & Co.—a decision cited earlier in this book—the judge wrote as follows: An auditor is a watchdog, not a bloodhound. . . . As a matter of commercial reality, audits are performed in a client-controlled environment. The client typically prepares its own financial statements; it has direct control over and assumes primary responsibility for their contents. . . . The client engages the auditor, pays for the audit, and communicates with audit personnel throughout the engagement. Because the auditor cannot, in the time available, become an expert in the client’s business and record-keeping systems, the client necessarily furnishes the information base for the audit. Thus, regardless of the efforts of the auditor, the client retains effective primary control of the financial reporting process.3

No doubt the investing public and others who rely on financial statements have been frustrated over the issue of fraud detection. Who can blame them?

However, those who rely on financial statements cannot get what they want by asking auditors to defy “commercial reality,” as the judge brilliantly explains.

As the public has clearly shown an interest in influencing all of those involved in the corporate reporting chain to improve accountability and performance, there must be greater appreciation for the skills of forensic accounting investigators.

HISTORICALLY, AUDITS MAY HAVE BEEN PREDICTABLE

Many have suggested that the reason auditors did not detect in a timely manner the fraudulent schemes leading to some of the more significant corporate scandals was simply that the auditors’ audit procedures had become predictable.

There is no secret about what well-trained auditors examine in the course of an audit performed in accordance with generally accepted auditing standards (GAAS). Once the audit leader has identified the risk areas in a financial statement prepared by company
management, the focus and scope of the planned audit are defined easily enough. However, the relatively routine, predictable character of audit planning creates opportunities for fraud. When it is easy to determine the scope of an audit, it is often easy to plan a fraud around it. The auditor should incorporate an element of unpredictability in the selection from year to year of auditing procedures to be performed—for example, performing substantive tests of selected account balances and assertions not otherwise tested due to their materiality or risk, adjusting the timing of testing from that otherwise expected, using differing sampling methods, and performing procedures at different locations or at locations on an unannounced basis.

The landscape has changed rapidly for financial statement auditors. Arthur Andersen collapsed in the aftermath of the Enron scandal; a major health care provider has been accused of fabricating documents to deceive its auditors as part of a scheme to increase revenues; and other instances of accounting and audit abuse continue to emerge.

Auditors allegedly have been placed on the front line in the battle against fraud. They face the public and regulatory expectation that they will play a key and continuing role in restoring the integrity of financial reporting. This message is embedded not only in the language of Sarbanes-Oxley, but also in the new

As noted in earlier chapters, American Institute of Certified Public Accountants Statement on Auditing Standards (SAS) No. 99 outlines procedures the auditor must follow in assessing the potential risk of fraud and the impact on financial statements for periods beginning on or after December 15, 2002.

Among its many topics, SAS 99 highlights the need to bring in subject matter experts (SMEs) to assist the audit team or to investigate allegations or indications of fraud. To forensic accounting investigators, the environment newly defined by SAS 99 is just the latest chapter in a lifetime’s work of ferreting out fraud schemes and corporate misconduct via the use of tried-and-true techniques.

Forensic accounting investigators can bring such skills and experience to any stage of the audit, and many firms are considering how best to effectively leverage these skills.

**POTENTIAL TRIGGER POINTS OF FRAUD**

- Anonymous allegations of fraud, whether by letter, e-mail, hotline, or anonymous call. Whistle-blowers should be treated with utmost care.

While seeking to take the allegations seriously, companies may wait too long to respond to whistle-blowers, who then believe they’re not being taken seriously and who make a phone call to a third party such as the U.S. Securities and Exchange Commission (SEC) or the media. Every effort should be taken to respond to whistle-blowers immediately. Whistle-blowers should be encouraged to talk with a forensic accounting investigator who is trained
in working with whistle-blowers. In such an interview, the forensic accounting investigator can form an opinion as to the probable validity of the allegations and can search for the reasons the individual has decided to come forward. The forensic accounting investigator knows there are occasions when people want revenge or attention and use the cover of whistle-blowing to satisfy their own needs. Although all whistle-blowers require immediate and thoughtful attention as required by Sarbanes-Oxley, there should be an attempt to test the allegations for validity—preferably, by face-to-face interview—before the decision is made to launch a full-scale investigation.

• Discovery that a high-ranking official resigned due to known or possible illegal activities. Unless there is evidence indicating an irregularity it is not usual that a forensic accounting investigator will be called in to perform an investigation. Although such an irregularity may emerge as an issue, the primary initial concern is that the executive may have acted improperly in other respects. A forensic accounting investigator may perform procedures—including interview and document examination and, very possibly, e-mail searches—to ascertain the likelihood of the allegations.

If it is proved that the executive did in fact participate knowingly in illegal activities, the forensic accounting investigator usually recommends that the audit team review its audit programs to determine areas in which reliance was placed on the subject executive in the conduct of the audit. Further, the audit committee should be advised that while the investigation is under way, another executive should step in to review relevant prior-year representations so that current-year representations, including

If there is doubt about the integrity of the executive, especially about the CEO or chief financial officer (CFO) who signs the management representation letter, the forensic accounting investigator is likely to search for instances in which such executives worked below their level of and their expected management scope. For example, while interviewing an information technology director, a forensic accounting investigator might learn that the company’s CFO was oddly concerned about programming issues and, in fact, would come into the office on Saturdays and do a little programming. Or the CFO had the habit of bypassing accounting supervisors and going directly to the accounts payable clerk to order the clerk to cut a check to a certain vendor. Facts such as these—should they emerge—coupled with concerns that the executive has doubtful integrity, could have a substantial effect on the audit program. Early consultation with a forensic accounting investigator may avert problems later, when the company’s filing deadline is looming.

• A client identified as the target of an investigation by a law enforcement agency. Were the auditor to wait until the investigation is resolved before considering its implications for the audit, that would be a mistake. The length of time to complete an investigation is usually counted in months rather than weeks. In many instances, the company may not even know that the enforcement agency that launched the investigation has concluded it. Consider bringing in a forensic accounting investigator upon first learning of the investigation to discuss its implications.
• A client who receives a subpoena from a law enforcement or regulatory agency. A subpoena raises similar concerns as in the previous scenario. In this case, the forensic accounting investigator usually requests a copy of everything that is turned over to the agency. It would be a mistake to assume that the auditors have previously reviewed all of the subpoenaed documents, even if the auditors specifically requested and did in fact review what they believed to be the full selection of documents. The company may have withheld critical information. For example, the equipment sales contract the auditors reviewed may not have included a key rider allowing the customer to return the equipment under different terms than originally provided for in the contract, thereby disqualifying the sale for treatment as a sale under Statement of Financial Accounting Standards.

Obtaining another copy at the time of the agency’s subpoena gives the auditor and forensic accounting other documents may show up.

• An auditor who believes that intentionally misleading verbal information has been provided by the client, or that requested documents have been altered, or that documents are being withheld intentionally. Auditors may wish to confront the company personnel who they believe to be involved in the deception. If confronted, an individual may apologize profusely for creating such a misunderstanding and weave an explanation of some kind around the facts. The audit then continues, but the auditors may be left with the uneasy feeling that they have not received an honest response.

Forensic accounting investigators use different techniques. For example, they may make use of indisputable facts about the suspected deception to see whether the individual lies or tells the truth in response to certain strategic questions.

• Discovery that the client has suffered embezzlement—even of a small amount and even if the suspect is no longer on staff. SAS 99, paragraph 76, specifically states: “If the auditor believes that misstatements are or may be the result of fraud, but the effect of the misstatements is not material to the financial statements, the auditor nevertheless should evaluate the implications, especially those dealing with the organizational position of the person(s) involved.”

Forensic accounting investigators, honed by years of experience, know that frauds often occur in the most unlikely situations and often are committed by the most unlikely individuals. Any misstatement that suggests the possibility of fraud should be investigated regardless of materiality.

The cause may be innocent error. On the other hand, an accounting clerk may have perpetrated a small fraud, or the corporate controller may have a hand in it, and the seemingly small fraud may be only the tip of an iceberg.

Suspicions of fraud, regardless of their materiality, require some level of investigation to resolve their implications.
• Indications that a vendor may be fictitious. Fictitious anything should be a concern. One fictitious vendor may not seem all that important—and it may not be; it may represent a small, unintentional error. But it may also be the footprint of a fraud perpetrated by top management and concealed for years. It is advisable to call in forensic accountant investigators when suspicions about possible fictitious vendors arise—for the simple reason that the range of possibility stretches from an innocent recording error to a very large fraud. If an event does indeed indicate that a fraud may have occurred, both GAAS and SEC regulations have specific requirements as to how to proceed when there is evidence of a suspicious act.

• Indications of improper accounting for revenue or expenses such as sales recorded before completed and final, goods shipped before a sale is final, revenue recorded while the customer is still owed future service or goods, or apparently false revenues recorded. While these issues may be investigated by auditors themselves, consultation with forensic accounting investigators may be helpful.

Other indications of fraud that may warrant consultation with a forensic accounting investigator include the following:

- Supplier refunds recorded as revenue
- Unbilled revenues or other accounts receivable being re-aged
- Bill-and-hold issues
- Recording vendor discounts as income
- Revenue recorded from self-dealing or asset exchanges
- Current expenses shifted into later periods
- Expenses improperly capitalized
- Liabilities concealed and not accrued
- Delayed asset write-offs
- Shifting expenses to a later period or advancing revenues

There are a number of other observable events that, while not necessarily indications of fraud, warrant appropriate warnings to the audit staff. The following conditions, either independently or in concert with other conditions, can be red flags of possible fraud. Where all of these conditions are concerned, auditors should proceed with a heightened level of professional skepticism in performing their planned audit procedures. Should indicia of fraud become evident, consultation with a forensic accounting specialist should be considered before proceeding beyond the scope of the audit plan.

Some of the observable events are as follows:

- Transactions that are not recorded in a complete or timely manner or that are recorded improperly as to amount, accounting period, classification, or entity policy
- Managers working below their level of authority
• Unsupported or unauthorized balances or transactions
• Last-minute adjustments that significantly affect financial results
• Evidence of employee access to systems and records inconsistent with the access necessary to perform authorized duties
• Significant reconciled differences between control accounts and subsidiary records or between physical count and the related account balance that were not investigated and corrected on a timely basis
• Unusual transactions, by virtue of their nature, volume, or complexity, especially if such transactions occurred close to year-end
• Transactions not recorded in accordance with management’s general or specific authorization
• Identification of important matters previously undisclosed by management
• Long outstanding accounts receivable balances
• High volumes of sales reimbursements and/or returns after year-end
• Suppliers’ accounts with a high volume of debit and credit entries

✓ Conflicting or missing evidential matter may also be a possible red flag suggesting fraud. These conditions include the following:
• Missing documents
• Unavailability of other than photocopied or electronically transmitted documents when documents in original form are expected to exist
• Significant unexplained items on reconciliations
• Unusual documentary evidence such as handwritten alterations to documentation or handwritten documentation that is ordinarily electronically
• Inconsistent, vague, or implausible responses by management or employees arising from inquiries or analytic procedures
• Unusual discrepancies between the entity’s records and confirmation replies
• Missing inventory or physical assets of significant magnitude
• Unavailable or missing electronic evidence, inconsistent with the entity’s record retention practices or policies
• Inability to produce evidence of key systems development and program change testing and implementation activities for current-year system changes and deployments
• Seriously incomplete or inadequate accounting records
• Contractual arrangements without apparent business purpose
• Unusual transactions with related parties
• Payments for services that appear excessive in relation to the services provided

✓ Problematic or unusual occurrences between the auditor and the client may also be red flags of possible fraud. Such events include the following:
• Denial of access to records, facilities, certain employees, customers, vendors, or others from whom audit evidence may be sought
• Undue time pressures imposed by management to resolve complex or contentious issues
• Complaints by management about the conduct of the audit or management intimidation of audit team members, particularly in connection with auditors’ critical assessment of audit evidence or in the resolution of potential disagreements with management
• Unusual delays by the entity in providing requested information
• Tips or complaints to auditors about alleged fraud
• Unwillingness to facilitate auditor access to key electronic files for testing by means of computer-assisted audit techniques
• Denial of access to key information technology operations staff and facilities, including security, operations, and systems development personnel
• Frequent disputes with the current or predecessor auditors on accounting, auditing, or reporting matters
• Unreasonable demands on auditors, such as unreasonable time constraints regarding completion of the audit or issuance of the auditors’ report—sometimes accompanied by warnings about the audit fee structure and expected duration
• Formal or informal restrictions on auditors that inappropriately limit access to people or information or that curtail the auditors’ ability to communicate effectively with the board of directors or audit committee
• Domineering management behavior in dealing with auditors, especially when there are attempts to influence the scope of auditors’ work or the selection or continuance of personnel assigned to or consulted on the audit engagement
• Client personnel displaying a hostile or unreasonable attitude toward audit personnel
• Client engaging in opinion shopping
• Managers’ laying to auditors or evasion in response to audit inquiries to the point that dishonesty seems a likely diagnosis

The ability of auditors to collaborate with forensic accounting investigators varies widely. Some do so comfortably and well, and some do not. Consider this case: An audit manager at a client happens to say to a forensic accounting investigator:

“We were doing an audit at a plant in Mexico, and while we were down there, they got an anonymous letter about kickbacks and an outside business interest of the general manager. The client was concerned about costs and didn’t want to bring in a forensic accounting investigator, but we were asked to make some inquiries. We didn’t turn up anything, so in the end there was nothing to call you about.”

Even if preliminary inquiries “didn’t turn up anything,” it might have been safer and been better procedure to presume that something was going on at the plant in Mexico. Failing to bring in a forensic accounting investigation professional to dig deeper, the client now might have had a false sense of security because the auditors had made some inquiries. By letting the client influence their response, the auditors may have served it poorly and also put their own firm at risk.
Would calling in a forensic accounting investigator have cost more? Most likely, yes. If an auditor had been replaced with an experienced forensic accounting investigator, the resulting cost might have been $10,000 more. Is that too much to pay? If the preliminary inquiries uncovered further cause for suspicion, additional investigative procedures might have been necessary—at more cost. But weigh that cost against the magnitude of the direct loss to a company and the damage to reputation resulting from a fraud, especially if the fraud goes undetected for a significant period of time.

Consider the contrast between how a questionable situation might be handled—first without and then with a forensic accounting investigator. The two scenarios are hypothetical, but they run close parallels to plausible events: An accounting firm has audited the financial statements of a client company—a publicly held manufacturer and distributor—since 1990. During that time, the company experienced significant revenue growth while many of its competitors stagnated. In auditing the company’s 1999 financial statements, the accounting firm found a large, rounded journal entry that materially increased revenue. The firm determined that the entry had been recorded manually, while most of the revenue entries were posted electronically from the client’s billing system. The manual entry was recorded after the close of the field audit, one day before the company’s earnings release.

The auditors questioned the client’s controller, who said he had no support for this entry and referred them to the CFO. Both officers had previously worked at the auditing firm and were good friends who socialized with the engagement partner and the senior manager on the account. Questioned about the entry, the

CFO said the entry had been made to match revenue with costs in light of entering into a large contract with a new customer after the billing system had been closed. The auditors documented that explanation in their working papers and requested additional support. Later that day, the controller provided a facsimile copy of a customer contract that supported the revenue entry, and he said the original contract had not yet been forwarded from the field to the corporate offices. The auditors documented this in their working papers, along with the facsimile copy of the contract.

Several years later, the SEC received an anonymous letter that accused the company of fabricating revenue. The company’s board of directors reached out to the audit firm to investigate, and the auditors found the following:

- Revenues had been materially overstated each quarter through large, manual, and rounded journal entries entered after the close of the field audit.
- No original supporting documentation for these entries existed.
- The clerk who recorded the entries said the controller had provided on a self-stick note the amounts and accounts to record—with no supporting documentation.

While the auditing firm was looking into these matters, the controller and the
CFO resigned. When the board of directors learned of the findings and the resulting restatements that followed, it asked, “Where were the auditors?” The audit firm was eventually fired and later sued in a shareholder class action for malpractice. During the ensuing litigation, it was alleged that the auditors could have uncovered the fraud in its infancy had they investigated the questionable transaction they identified during the 1999 audit. The suit also asserted that the audit firm’s investigation had been compromised both by the social relationship between its partners and the corporate officers and by the $10-million fee the firm received from the client for consulting services. Ultimately, the audit firm paid a large sum to settle the lawsuit.

How might forensic accounting investigators have acted in this case? Imagine that after hearing the CFO’s explanation of the large, rounded journal entry, the audit firm called in forensic accounting investigators, who suggested that the client’s audit committee be notified of the transaction, the lack of documentation to support it, and the CFO’s explanation. The audit committee then hired the forensic accounting investigators to investigate, including performing a review of general ledger transactions and the electronic files of the controller and the CFO. The investigative team obtained all general ledger activity from 1997 through 1999 and after consulting with the client’s attorney on privacy issues, was able to obtain images of the personal computer files of the controller and CFO.

The forensic accounting investigators found similar large, rounded journal entries recorded late in the closing process for each quarter in 1999, a period when the industry was contracting. Unlike other journal entries made at corporate headquarters, no documentation was maintained in the central files to support these entries. A spreadsheet schedule on the controller’s computer showed that the large, rounded entries matched the difference between system revenues and analysts’ expectations. This document was also found to be attached to several e-mail messages between the two corporate officers.

Presented with these findings, the audit committee authorized additional investigative procedures. The forensic accounting investigators interviewed the two officials. The controller said he had been pressured by the CFO to record these entries and acknowledged that they were inappropriate. The CFO stood by his previous explanation and denied wrongdoing. Both men were placed on temporary leave and escorted from the building.

Subsequent interviews with employees of the accounting and finance departments produced invoices for payments made to certain vendors that had been authorized by the CFO. The forensic accounting investigators examined the company’s vendor master file and found more than 10 vendors with the same post office box number. A review of the canceled checks to these vendors found that all of the checks had been deposited into the same bank account and that they totaled more than $1 million.

The audit committee notified the authorities and its insurer. An investigation led to criminal charges against the two officers. The successful investigation cemented the audit firm’s relationship with the client.
RELIANCE ON OTHERS

When concerns arise that require a company to undertake a 10A investigation, consider the possible advantages of early involvement in working with the company’s audit committee and its 10A counsel to determine the possible financial statement impact. While it is true that it is the company’s responsibility to conduct the investigation, early involvement on the part of the auditor could be advantageous to the company’s goals of resolving the allegations and concerns so that regulatory filings can be timely made and the company can get back to normal operations. Additionally, in order to fulfill their own 10A responsibilities, auditors may consider calling upon forensic accounting investigators to advise on the conduct of the investigation and whether or not its scope and procedures are adequate for the auditor’s needs. This is usually done by shadowing the lawyers and forensic accounting investigators engaged by the audit committee. The practice of shadowing can provide greater comfort that there will be no surprises at the conclusion of the company’s investigation.

In one such investigation, forensic accounting investigators received a call from an auditor, informing them of a recently concluded 10A investigation on one of his audit clients. The 10-K was due to be filed the following week. The auditor disclosed the nature of the investigation to forensic accounting investigators from his own firm. The investigation had been conducted by outside counsel, who had been retained by the audit committee. Outside counsel had chosen to conduct the entire investigation without the use of forensic accounting investigators.

As the auditor recounted the allegations and the procedures performed by the law firm, the forensic accounting investigators on the call knew instantly that there were gaping holes in the investigation. The allegation was that the CFO had instructed divisional controllers to create false entries that inflated revenues.

The CFO had contended in an interview that it was all a misunderstanding and that the error was already corrected. First of all, was an e-mail review performed?

Yes. However, the law firm had accumulated the e-mail data by requesting the company’s information technology department manager to “copy” e-mail folders. Experienced forensic accounting investigators know consideration should be given to collecting e-mail on servers and hard drives through forensic imaging, thereby capturing all deleted files. Merely copying the drives will not capture deleted files. Second, the law firm performed no assessment of the likelihood of involvement in the alleged scheme by anyone in the information technology department. The forensic accounting investigators told the auditor that due to these and other deficiencies in the conduct of the investigation, he should not rely on its results. “Then what am I to do?” asked the auditor. The forensic accounting investigators suggested he contact his risk management group within the firm for further consultation on the various options to consider for possible resolution of the potential issue.
REPORT OF INVESTIGATION

Documenting an investigation is as important as performing it. A poorly documented case file can lead to a disappointing conclusion, can result in a dis-satisfied client, and can even damage the financial accounting investigator’s reputation and that of the investigator’s firm. Various means by which the forensic accounting investigator may report his findings are discussed in greater detail in this chapter. The form of that report—whether oral or written—is a matter to be discussed with the client and with counsel. While it is not the responsibility of the forensic accounting investigator to advise on the legal perils associated with various forms of reporting, there are certain issues of which forensic accounting investigators should be aware as their clients debate the form of reporting that will conclude the investigator’s investigation. This chapter addresses both written and oral reports of investigation.

We suggest that you determine at the outset whether a written report is expected from you and, if so, its form and timing. In the common circumstance that this point cannot be decided at the inception of the engagement, you should conduct the investigation in a manner that will facilitate a comprehensive oral report, including the key documents and any exhibits necessary to illustrate the findings. Many investigations begin small, but there is no way to know with certainty where they will lead and what will be required at the conclusion. Although your client may not have requested a report at the outset of the investigation, some event in the course of the investigation may change the client’s mind, and you should be prepared to respond. For example, you may determine in the course of an investigation that an officer of the company violated a law or regulation, thereby requiring the company to consider self-reporting and possibly bringing a civil action against the officer and other third parties. Alternatively, you may be subpoenaed for your part in an investigation that has captured the attention of regulatory agencies or law enforcement. While you can testify only as to what procedures you recall performing and the attendant findings, your client—and your own reputation—will be better served if you have proper documentation.

TYPES OF REPORTS

The following types of reports are relevant.

• Written reports

  Report of investigation this form of written report is given directly to the client, which may be the company’s management, board, audit committee of the board, in-house counsel or outside counsel. The report should stand on its own; that is, it should identify all of the relevant evidence that was used in concluding on the allegations under investigation. This is important because the client may rely on the report for various purposes such as corporate filings, lawsuits, employment actions, or alterations to procedures and controls.
Expert report filed in a civil court proceeding. We will touch on this topic only as it pertains to civil fraud court proceedings. The American Institute of Certified Public Accountants (AICPA) publishes an excellent practice aid on the full range of expert reports.1

**Affidavits** These are voluntary declarations of facts and are communicated in written form and sworn to by the witness (declarant) before an officer authorized by the court.

**Informal report** These consist of memos to file, summary outlines used in delivery of an oral report, interview notes, spreadsheets listing transactions along with explanatory annotations, and other, less-formal written material prepared by the investigation team.

**Oral reports**

Oral reports are usually given by the forensic accounting investigation engagement leader to those overseeing an investigation, such as a company’s board, or to those who represent the company’s interests, such as outside counsel.

**IMPORTANCE OF ADEQUATE PREPARATION**

“I could have given you a more thorough and accurate report if I had had more time to prepare.” The inexperienced forensic accounting investigator will no doubt say that at least once in a career in response to an irate client who is dissatisfied with a report on the preliminary results of an investigation. In our busy and complex world and in the course of a busy and complex investigation, not everything on the task list has the same priority. Experienced forensic account-

1. American Institute of Certified Public Accountants, Consulting Services Practice Aid 96-3, Communicating in Litigation Services: Reports (New York: American Institute of Certified Public Accountants, 1997). Investigators know that any request for an update on an ongoing investigation is a report in the truest sense of the word report. One should not assume that an update delivered orally can be treated more casually than a written update.

All reports deserve adequate preparation time and presentation in accordance with professional standards of practice.

Reporting is a critical responsibility of the forensic accounting investigator, and adequate preparation is necessary to present the status of the investigation in a manner that enables the decision makers to assess how to proceed. No report, oral or written, should be considered “unofficial.” Regardless of what you say or write to qualify your comments, once a document leaves your hands or words leave your lips, you cannot control the further distribution of the information you have communicated. Take the time to get it right.
STANDARDS OF REPORTING

Depending on your professional affiliations, you will be required to follow the reporting standards of your profession. If you are a certified fraud examiner (CFE), the applicable standards can be found in the Fraud Examiners Manual, 2 published for its members by the Association of Certified Fraud Examiners. If you are a certified public accountant (CPA), you should follow the reporting standards required for consulting engagements and found in the AICPA’s Statement on Standards for Consulting Services. If you are both a CFE and a CPA, you will be required to follow the standards of both associations. Because the AICPA standards are quite broad, while the standards of the Association of Certified Fraud

ACFE STANDARDS

The ACFE Reporting Standards are included in the Fraud Examiners Manual, a comprehensive guide designed specifically for use by members of the ACFE. (The Fraud Examiners Manual is also available to nonmembers.) Unlike the

AICPA’s rather general rules, ACFE reporting standards document a basis for reporting the results of a financial crimes investigation in a practical manner that can aid the forensic accounting investigator in preparing reports. The standards, both broad and detailed, give the forensic accounting investigator an overview of conceptual objectives as well as enough detail to guide both the novice and the experienced professional in reporting matters. The following points reflect

ACFE reporting standards

Preparation

Do not expect to generate a well-written report from a poorly performed and/or poorly documented investigation. If the investigation has been performed and documented properly, then the reporting of procedures and findings should flow as a natural extension of the investigation. Preparation is critical to the reporting process and serves as the foundation for the other reporting standards. Preparation requires organizing each stage of the investigation from the initial engagement letter and data gathering to analysis and corroboration. Deficiencies in performing the investigation are likely to be very evident in the Report of Investigation.

Accuracy

It goes without saying that all reporting should be accurate. Accuracy applies not only to the information conveyed in the report, no matter how incidental, but also to the mechanics of communication: grammar, spelling, and the like. Mistakes in your report, however trivial,
could cast doubt on the credibility of information that you know to be decisive. Accuracy in reporting basic data, dates, events, and names is critical.

Clarity

Use clear and simple language to eliminate to the greatest degree possible any doubt about your intended communication. Written communications should be crafted in such a way that an average group of citizens selected for jury duty could understand the facts and their interpretation. Because forensic accounting investigators are fact finders, the fact pattern described in the report should make the evidence clear, thus enabling the trier of fact—the individual (judge) or group (jury) rendering a decision—to reach the proper conclusion. You are there to assist them.

Impartiality

Bias destroys credibility. The AICPA SSCS rules on integrity and objectivity, discussed earlier (see CS 100.07), parallel the impartiality requirement of the ACFE Reporting Standards. As a fact finder, the forensic accounting investigator contributes a crucially important set of findings to the trier of fact. Any perception of bias detected in reports may destroy the credibility of reported facts and thereby render the forensic accounting investigator’s work less useful. Opinions as to culpability in criminal matters should not be stated. Subjective opinions and impressions often express unstated (or stated) bias and have no place in reporting, oral or written. The facts must speak for themselves.

Relevance

Every investigation uncovers information that is irrelevant to the issues at hand.

The report should include only facts relevant to resolving the allegations being investigated. Not only is irrelevant information distracting to recipients, but also the forensic accounting investigator’s credibility may be at risk by implying flawed judgment as to what really matters.

Timeliness

The report, as well as information gathered in support of it, should be submitted in a timely manner. This point is especially true of interviews that, if not documented and reported upon without delay, may cause decision makers to be less influenced by their contents.

THE WRITTEN REPORT OF INVESTIGATION

Needless to say, reports documenting an investigation differ considerably from audit opinions issued under generally accepted auditing standards (GAAS). The investigative report writer is not constrained by the required language of a governing standard, and investigative reports differ from one another in organization and content depending on the client’s stated needs. In contrast, audit reports adhere to set formula prescribed by GAAS. The uses of written reports also differ.
The client could do any of the following things with an investigative report, among others.

- Distribute the report to a select group of individuals associated with the company in various capacities.
- Voluntarily give the report to a prosecutor as a referral for prosecution.
- Enter the report as evidence in a civil fraud proceeding.
- Give the report to outside counsel for use in preparing regulatory findings, entering negotiations, or providing other legal services on behalf of the company.

Whatever the ultimate fate of the written report, its basic elements will be much like the following elements.

**BASIC ELEMENTS TO CONSIDER FOR INCLUSION IN A REPORT OF INVESTIGATION**

- Identify your client:

  [Firm] was engaged by Cutting Edge Technology Corporation (the “Company”).

- In the case of a lawsuit, identify the parties: I, [forensic accounting investigator’s name], have been retained by [name of law firm] (“Counsel”) to investigate certain of the claims and allegations made by Philip Hart (“Hart”), John Harrington (“Harrington”), and Robert Geller (“Geller”) against Peter Langley (“Langley”).

- State in broad terms what you were asked to do—for example, “to provide expert testimony or investigate certain allegations”:

  . . . to provide forensic accounting investigation services in order to assist in pursuing your concerns related to certain allegations made against Jane

- Describe your scope, including the time period examined:

  I was engaged to perform investigative procedures related to review of the Company’s purchasing and receiving policies and practices in effect over fiscal years 2001–03. We have performed background checks of certain employees at the direction of [name of outside counsel], reviewed and analyzed certain of the Company’s accounting records and other documents, performed various data mining and data interrogation of the Company’s electronic files, and conducted interviews of current and former Company employees.

- Include mention of any restriction as to distribution and use of the report:

  This report was prepared in connection with the aforementioned matter and is intended solely for your information. It may be used only for the purposes of this engagement and may not be used for any other purpose without our written consent.

- Identify the professional standards under which the work was conducted:
We performed our work in accordance with the American Institute of Certified Public Accountants’ (“AICPA”) Statement on Standards for Consulting

• Identify exclusions in the reliance on your report:

Our work does not constitute either an audit performed in accordance with the AICPA’s generally accepted auditing standards or an attestation service.

We make no representation as to the adequacy of our procedures for your purposes.

• State that your work should not be relied on to detect fraud:

Fraud and irregularities by their very nature are most often hidden, and no absolute assurance can be given that all such matters will be detected. Our engagement cannot be relied on to disclose all irregularities or illegal acts, including fraud that may exist. During the course of this engagement, we will inform you of any such matters that come to our attention unless they are clearly inconsequential.

• Include the procedures you performed, technical pronouncements relied upon, and findings:

12. You might consider indicating that if you are presented with a subpoena, you will inform the client that you intend to comply unless the client makes court filings in an attempt to quash the subpoena.

13. If appropriate, also perhaps include the implications of your observations and findings.

SUMMARIZING YOUR FINDINGS

A summary can be helpful to the reader but may be perilous for the report writer in terms of keeping critical information and perspectives intact. Caution is advised when preparing two types of summary sections: executive summary and conclusion. We do not recommend writing a summary conclusion. If for any reason you nonetheless do so, be careful not to offer an opinion on the factual findings unless specifically requested to do so. The facts should speak for themselves. It may be appropriate to position in a concluding section of the Report of Investigation certain recommendations for additional investigative procedures or a description of control breakdowns you have observed.

Again, while we do not recommend summary conclusions, a carefully written executive summary at the beginning of the report can be extremely helpful to the reader, especially when it precedes a long and complex report. The executive summary should offer in simple, straightforward language an accurate statement of significant findings. Each summarized finding should include a reference to the full description of findings included in the complete Report of Investigation.
WRITTEN REPORT OF EXPERT WITNESS OPINING

FOR THE PLAINTIFF ON A CIVIL FRAUD CLAIM

A report written for submission at trial or like proceedings, such as arbitrations, is beyond the scope of this text. Forensic accounting investigators required to author such a report should take direction from client counsel in preparing a

EXECUTIVE SUMMARY

As a result of our work, we have noted the following preliminary findings as summarized below. It is important to note that the evidence we have identified in this Report of Investigation suggests but in no way incriminates any individual or entity. This Executive Summary is not meant to substitute for our following Report of Investigation. A summary of the evidence we have reviewed suggests that:

• Clark and Kent skimmed at a minimum $2,500,000 in cash from the Atlanta Division from February 1999 through their termination on July 5, 2001.

• Clark directed at least $1,280,000, in aggregate from the Atlanta Division, to his brother’s company, Built-Right Construction, and his father’s company, B&B Construction, from 1999–2001. Invoice review and interviews with personnel indicate that the services provided by these two companies may not have been performed. (See Sections B-3 & B-4.)

• Approximately $8,500,000 was paid from the Atlanta Division to twenty-six construction companies during 1999–2001 (see Section B-2); $415,000 was attributable to companies in which “cut and paste” invoices were discovered in Kent’s desk. (See Section A-4.)

• Clark, Kent, and Clark’s brother also benefited financially through transactions involving petty cash and theft of store merchandise. (See Sections A-9 & D.)

Our analysis has utilized Company-provided documentation and files beginning when the Company acquired a 100% interest in the Atlanta Division in 1999. Due to the schemes noted, the size of the dollars at risk, and general manager Clark’s tenure of 26 years, we recommend that the Company inform the seller and expand the scope of this investigation to include the years where only a 50% interest was held.

Additionally, we recommend that further investigative procedures be conducted to resolve the allegations we present in our findings below.

Written Report of Expert Witness Opining for the Plaintiff on a Civil Fraud Claim 459 report that meets all of the requirements of Rule 26(b) of the Federal Rules of Civil Procedure or such other rules as may be applicable to their appearance.

In most forensic accounting investigations there is no need to provide expert witness testimony. The forensic accounting investigator may, however, be asked to testify as a fact
witness. As indicated earlier, the forensic accounting investigator is principally a fact finder and reports facts in a straightforward manner so that others—judge; jury, audit committee, board of creditors, or other interested party—can interpret those facts and make determinations as to their implications, including compliance with laws and regulations. There are, however, instances in which the forensic accounting investigator may be asked to prepare a formal expert report to a court in advance of a planned court appearance, at which time the investigator is expected to testify as to findings and to offer an opinion on a civil fraud claim. An example of a civil fraud claim opinion follows.

In the example, the expert witness is a forensic accounting investigator with both CPA and CFE credentials. He conducted an investigation at the request of counsel representing the buyer of a manufacturing business. In the course of the investigation, he learned that most sales under the previous owner had been affected through the payment of kickbacks and bribes. When the new owner took possession, he was unaware of the pattern of kickbacks and bribes, and he refused to pay when he was approached by customers or their agents. Not surprisingly, sales dropped off significantly. Through his lawyer he filed a civil lawsuit, including among his claims that the defendant seller had known of the kickbacks and bribes, had failed to disclose them, and had thereby materially damaged the buyer. The forensic accounting investigator was asked to opine on the civil fraud charge. Following is that section of his report.

**OPINION**

Based upon my review, it was evident to me that there were numerous disbursement transactions between BUILDIT Manufacturing (BUILDIT) and a number of its vendors prior to buyer’s involvement, which misrepresented the proper business purpose of the transactions. That is, invoices were presented to BUILDIT for goods and services that had not been furnished. However, given the level of kickbacks and bribery within BUILDIT, the testimony of individuals, and other evidence, I believe that the preponderance of the evidence indicates that a fraud was perpetrated upon the buyer of BUILDIT. I base my conclusion on the following definition of fraud. Fraud in the inducement

Fraud occurring when a misrepresentation leads another to enter into a transaction with a false impression of the risks, duties, or obligations involved; an intentional misrepresentation of a material risk or duty reasonably relied on, Misrepresentation

I believe that the seller made numerous misrepresentations to the buyer, which includes:

- Failure to disclose that at least $2,469,910 was paid to shell companies, thereby providing cash for bribes to be paid to the owners of the companies

(“Shell Companies”) listed on page 3 of this report. No goods and services were provided in exchange for cash paid to these entities.

- Failure to disclose that these payments were made to companies owned by individuals that were employed by significant customers of BUILDIT
• Incorrectly classifying the payments to the Shell Companies as “direct labor” and “materials” expense

• Providing the buyer with financial statements that included misclassifications of both revenue and expense

In my opinion, transactions were created in such a way as to conceal the true nature of the expense. There may have been other misrepresentations made by the seller to the buyer. However, these examples, I believe, satisfy the above definition.

Reliance

The misclassification and recording of the payments to the Shell Companies concealed material risks that were not known by the buyer. In my opinion, had the buyer known about the existence of kickbacks and bribes, he would not have gone forward with the purchase. The fact that the buyer did go forward with the purchase demonstrates reliance.

AFFIDAVITS

An affidavit is a written statement submitted in a legal proceeding. Affidavits should receive the same level of care as that given to more extensive written reports. Typically not as long as reports of investigation, they attempt to summarize salient facts or they are submitted as sworn testimony previously submitted in the form of the forensic accounting investigator’s report of investigation. The forensic accounting investigator should carefully edit the affidavit so it accurately conveys his own thoughts. The investigator should use words and phrases that are terms of art to the accounting profession, not the legal profession. A poorly drafted affidavit signed by a forensic accounting investigator can diminish that investigator’s credibility. Like the report of investigation, the affidavit is the work product of the forensic accounting investigator.

INFORMAL REPORTS

There are certain informal types of reports, the most common of which are memos to file and presentations. Because any communication, written or oral, may be discoverable, professional care should be taken to ensure that all communications are accurate and comply with the relevant reporting standards.

A memo to file is a standard approach to the documentation of important events and understandings at points in time. The purpose of such memos is to document certain events and investigator. At times, clients may ask for copies of such memos as substitutes for formal reports. While some clients may insist on receiving the memos prepared during the course of the investigation as opposed to a written report, they should be reminded that a memo is prepared at a point in time and is not a substitute for a written report. Presentations are an informal manner of reporting the results of an investigation. Presentations have the attributes of both written and oral reports—and can be dangerous if prepared carelessly. A written report allows for the possibility of thoroughly explaining a finding and its impact. The very
nature of a presentation is brevity—in the expectation that the presenter will flesh out the information summarized in the slides. When using the presentation format in lieu of a detailed written report, the financial accounting investigator should consider whether a page with a boilerplate “Statement of Responsibility” could serve to remind the audience of certain limitations (see similar material at the beginning of the earlier discussion on the written Report of Investigation). Also, consider including a statement at the bottom of each page reading, “The accompanying Statement of Responsibility is an integral part of this presentation.”

While oral reports may require less effort and therefore generate less expense for the client, preparation for an oral report should be no less comprehensive than for a written report. Planning an oral report also requires both designation of a member of the team to deliver it and a decision regarding other team members who should be present. It may be wise to have staff members present or at least nearby who are most familiar with the details of certain interviews and events so the staff members can be called on in the event that the client wishes more detail.

An advantage of oral presentations is that there is ample opportunity for the forensic accounting investigator to clarify points, and those receiving the report can seek clarification by asking questions and can convey their particular concerns then and there. The interactive aspect of oral reports is probably their greatest benefit.

In the context of financial investigations, reports can take many different forms. Due to the dynamic nature of financial investigations, stakeholders involved in the oversight of investigations or relying on the results may want interim reports, which, while preliminary, represent an important responsibility of the forensic accounting investigator. Interim reports or updates are more useful if they include both a summary of the procedures performed, with related findings, and an overview of recommended procedures and expected outcomes.

Additionally, an interim report should record what, if any, obstacles have hindered the forensic accounting investigators in the performance of their work.

Investigations are something like a black box for those who must evaluate the results. The more factual information investigators report, the better it is for their audience, who are the decision makers.

An illustration may help here. Let us say that forensic accounting investigators have been investigating allegations that a drug company paid kickbacks to physicians for favoring the company’s products. About two weeks into the investigation, the audit committee calls a hastily planned meeting with the forensic accounting investigators and asks for an update. The partner investigator indicates that his team of three professionals has been in the field for two weeks and has incurred $100,000 in fees and expenses. The partner reports that to date, the team has found hear this report. However, this bare-bones summary report, while correct, hardly gives either a correct impression or the comprehensive status of the investigation.
Preferably, the partner leading the forensic investigation advises the audit committee that a day of preparation to assimilate information from the team covering planned procedures performed to date, obstacles encountered, findings to date, and recommended further procedures will be beneficial. During this fact gathering stage, the partner may reevaluate previously planned procedures and identify others he intends to suggest to the audit committee. Now he is adequately prepared. He presents orally to the audit committee and includes the same information as before regarding fees and expenses, but he is also in a position to add the following: “We learned yesterday that the electronic general ledger file is missing some journal entries made during a critical period. We have our information technology forensic team working to rectify the problem and get us complete electronic files. Additionally, we learned from several doctors whom we called randomly that they do recall being solicited by a company representative in a manner they felt was inappropriate. While we have yet to find conclusive evidence of the alleged improprieties, the preliminary evidence does suggest an expansion of the scope of our investigation to include telephone interviews of most of the doctors likely to have been called and follow-up with face to- face interviews of those reporting that they received such calls.” The partner could continue the update by citing other issues and possibly including change of- scope recommendations.

The example here focuses on oral reports because the oral report is a form of reporting that is often treated too informally—that is, not with the same diligence of preparation and review that a written report generally receives.

GIVING A DEPOSITION

The forensic accounting investigator may be called on to give a deposition which is testimony in the presence of a court reporter and sometimes a videographer.

Giving a deposition is an important activity and should not be taken lightly. Your professional reputation is at stake. Everything you have done in the course of an investigation is likely to come under close scrutiny. Your analysis, findings, and conclusions—even procedures you determined not to perform—all may be questioned. Expect that opposing counsel has met with another forensic accounting expert and received coaching on questions to ask you. Opposing counsel is likely to use techniques that attempt to impeach your credibility. That is opposing counsel’s job, and experienced attorneys generally are very good at it. Do not underestimate their ability to dissect responses and catch the unwary forensic accounting investigator in a contradiction. Be sure to spend adequate time with counsel who will be defending your deposition, and consider all of counsel’s recommendations. If you take issue with any of them, work it out before the deposition. Surprises at the deposition are unwise. While we recommend that you dedicate time to training materials such as the videotape preparing for a Deposition in a Business Case.

BE PREPARED

A mistake on the part of inexperienced forensic accounting investigators is to prepare inadequately. They may believe that because they have performed the investigation, merely
telling someone about it will be a simple matter. Caution is the preferable attitude: take depositions seriously, and take the time to prepare well. Scrutinize each working paper just prior to the deposition, even if you have previously performed a detailed review. Question yourself on findings and procedures as a final step in preparing for a deposition.

**IT’S YOUR DEPOSITION**

The most important thing to remember is that it’s your deposition. You are in control from the standpoint that no else knows the material of your report better than you do. Also, you can have a substantial impact on the tone and the pace of the deposition. For example, counsel may try to rush you through questions, but you are entitled to take the time required to formulate the best response to each question.

It is important to take the necessary time to prepare for your deposition.

Remember that your reputation and your firm’s reputation are at risk if you are ill prepared. Tell counsel approximately how much time you need to prepare, and do not waiver from this point. It is your deposition, and you should treat it according to your own and your firm’s high standards. During the deposition, if you do not understand a certain question or if opposing counsel asks compound questions that are confusing, either ask for the question to be rephrased or simply say that you do not understand. Counsel may try to make you uncomfortable by commenting that you should be capable of understanding and answering a question. Such a comment may seem intimidating.

Do not be intimidated; respond with professional courtesy and politeness—especially in more heated situations. If the opposing attorney fails to rephrase the question suitably, you can always say, “I apologize, and I want to be as complete in my response as I can, but I don’t understand your question and cannot properly answer until I do.”

**OBJECTIVES OF A DEPOSITION IN CIVIL LITIGATION**

A deposition is a form of discovery. The other side is permitted to “discover” what you did, what you learned your opinions, if any, and their basis. You are required to be responsive to all questions, but you need not volunteer any information that has not been requested. You will not convert the opposing lawyer to your perspective, no matter how hard you may wish to try. You are not there to educate opposing counsel even if it is evident from the line of questioning that opposing counsel is confused. No points are scored for being witty, and witty responses may backfire.

Stay true to your objective, which is to listen to the questions very carefully and to answer only those questions as honestly and succinctly as possible. Listen closely to the question and answer only the question asked.

**YOU ARE BEING MEASURED**

The deposition is probably the first opportunity for the other side to meet you.
While you are in their presence, you are being measured. They are picturing you in front of the judge or jury, evaluating what kind of witness you will make at trial. They will notice your appearance, your demeanor, and your level of overall confidence. Introduce yourself to the other side as well as to the court reporter.

Present your business card to them. As with any business meeting there is often causal discussion of various topics at the beginning: the weather, travel plans, and the like. Joining these discussions should be approached cautiously because one of them may turn into a discussion of the case and your role in it—“This must be your biggest case”—which is not an appropriate subject to discuss off the record. This advice also holds for casual encounters with opposing counsel in the elevator or hallway. Project confidence, and watch what you say at all times.

Without question you are required to be honest and not withhold information; however, it is perfectly acceptable to say, “I don’t know” if in fact you don’t.

Granted, we have heard tales of witnesses who, when they are trying to hide some incriminating facts, say they don’t recall or they don’t know. This is not what we mean to suggest here. It seems that one of the toughest things for some professional advisers to say is “I don’t know” to a question put to them in an area they did not investigate or should not be realistically expected to comment on.

They believe that an admission of ignorance will make them look weak, so they make the mistake of speculating, which in most cases is not a good idea. Unless you are specifically asked to speculate, you should not. Opposing counsel is free to ask questions and probe—sometimes in an effort to get you to speculate—or to ask for an opinion. You may hear the following, for example, from opposing counsel: “Well, wouldn’t you expect the CFO [chief financial officer] to be informed about such matters?” This question calls for your opinion, not a report of your factual findings. As with all questions, you must respond truthfully. If you had such an expectation, you must say so. If, however, you have not formed opinions about what should have happened—as opposed to reporting your discoveries of what did happen—you should say so. Counsel may try to make you feel you should know by following up with a comment along these lines: “You told us just a moment ago that you have been a CPA for 20 years and have done hundreds of audits. Shouldn’t you know the answer to this question?” Do not be intimidated; you have no obligation to know what others were hoping you would know or were hoping would be within the scope of your work. Often, the worst thing you can do is to assume or speculate in response to a question when you really do not know the answer. You are not expected to have a photographic memory. In this regard, you may wish to consult with counsel about preparing a binder containing the most relevant materials from the investigation, precisely because you are unlikely to remember every detail of a complex case.
REVIEWING YOUR DEPOSITION TRANSCRIPT

Generally, each person deposed may review the deposition transcript for any errors made by the court reporter and then sign the deposition after noting any corrections necessary. Counsel establishes different protocols in different cases, and accordingly, you may be asked to waive signature at the conclusion of your deposition. This means that the deposition will stand as transcribed—without your review. Counsel can advise you in advance of the practice in the particular case, and if you are unsure whether or not it is acceptable to you, discuss it with counsel. First, you want to ensure that what you said was transcribed correctly. Second, you may notice an inaccurate response unknown to you at the time but now evident as you review your comments.

Third, opposing counsel’s questions and your testimony may identify a weakness in your investigation for which you will want to be prepared at trial.

And if you gave a response that was factually inaccurate, you will want to advise counsel of the error. Even if you believe the deposition went well, take time to read it thoroughly.

OTHER CONSIDERATIONS

One of the best ways to ensure a successful deposition is to spend adequate time with the attorney who will be defending your deposition. No two depositions are alike, so even if you have given a number of them, you must still become acquainted with your counsel’s strategy for the deposition. Also make sure counsel defending your deposition knows the limitations of your knowledge and expertise. Again, the deposition is not the place for surprises. Based on the experience of the authors, the following are additional considerations.

• Think before you speak. The deposition transcript bears no indication of the time it takes you to respond to a question. Once said, words cannot be deleted from the deposition transcript.

• Be cautious in responding to questions that contain absolutes such as never or always.

• Avoid clever sound bites that may be used against you at trial.

• Speak in complete sentences, using proper grammar in a lucid manner at an ordinary speed. That will enable the court reporter to record your words accurately.

• Pause before each answer, no matter how confident you are of your answer. That allows you to repeat the question silently to yourself and gives counsel defending your deposition time to enter an objection if counsel cares to do so.

• When asked to comment on an exhibit, if time to read it isn’t offered, ask permission to read it before responding. Make sure you are familiar with it, and if you are not, state that for the record. You have the right to read every document presented before responding to questions about it.
Opposing counsel may seem annoyed at your request to read a document, but despite that discontent it is generally advisable to make sure you know what a document says before answering questions about it.

• Be specific in your answers, and do not exaggerate. For example, if you are asked, “Have you ever audited a financial institution before?” and your answer is, “Sure, a great many,” do not be surprised if opposing counsel pulls out a sheet of blank paper, gets ready to start writing a list, and says, “Please tell me the name of the first financial institution you audited, your responsibilities in that engagement, and when that occurred.” If it is true that you have audited “a great many,” opposing counsel would expect to write down a very long list. If your experience includes eight financial institutions, you may think eight is a great many, but others may think of eight as only a few. The better reply to the initial question may be, “Yes, I have.”

If you are properly prepared, giving a deposition is somewhat similar to an oral report, although often not organized in the manner you would select.

Remembering that your comments will become a written transcript and that your spoken words, once transcribed, can never be taken back, should instill in you the importance of adequate preparation.

MISTAKES TO AVOID IN REPORTING

The following brief discussions highlight and review issues raised earlier in this chapter.

Mistakes to Avoid in Reporting

AVOID OVERSTATEMENT

In the memorable TV series Dragnet, Sgt. Joe Friday used to say, “Just the facts, ma’am.” The same holds true when it comes to reports of investigation. The closer one sticks to the facts, all the facts, and just the facts, without embellishment, the better the report. The facts should speak for themselves. This is not to say that all facts are created equal: some facts are smoking-gun discoveries—for example, memos demonstrating both knowledge and intent. However, even in respect of obviously important facts, be careful not to overstate them.

AVOID OPINION

Other than the engagement to serve as an expert witness in a civil matter, the forensic accounting investigator should not offer opinions about the matter at hand. Also, opinions as to the intent or culpability (in criminal matters) of certain persons or as to whether an act was in fact a fraud should be avoided. These are matters to be decided by the trier of fact based on the factual material gathered and presented by the forensic accounting investigator. The forensic accounting investigator should not endeavor to influence the outcome beyond presenting the findings of the investigation in a clear and logical order.
IDENTIFY CONTROL ISSUES SEPARATELY FROM INVESTIGATIVE FINDINGS OF FACT

Often your client may ask you to identify control issues spotted during the course of your investigation. While appropriate to include in your report, we suggest including them in a separate section so as to focus on your primary task, which is that of a fact finder. The discovery of facts, leading to the resolution of potential criminal issues, is the forensic accounting investigator’s professional calling.

Identifying control breakdowns is a natural by-product of a fraud investigation, but such breakdowns should be addressed in a separate section of the report.

What does it mean in practice to give precedence to the pertinent facts? An example: A number of laptops are missing, and several of them can be traced directly to your target. If you actually wanted to give precedence to the control issue, you would write, “The control over laptop assignments is weak, and it was therefore impossible to account for all laptops acquired by the accounting department.” But if you put your focus where it belongs, you would write something of the following kind: “Over the past year, 11 laptops were purchased by accounting and assigned to 10 individuals, including two to the controller. When questioned, the controller showed us one of the laptops and could not account for the other.”

USE SIMPLE, STRAIGHTFORWARD LANGUAGE FOCUSED ON THE FACTS

The task of the forensic accounting investigator is to take a complex situation, properly investigate it to determine the relevant facts, and then report those facts in a simple, straightforward manner so that the reader or person hearing the report understands the facts and how they should be interpreted for resolution of the events occur? Why did the company not catch the problem earlier? In reporting the answers to these questions, there is no room for speculation.

Again, let us reduce these observations to an example. We would not recommend writing as follows: “The CFO admitted to recording false revenue but said he didn’t mean to hurt anyone. He wanted to keep the numbers up so that the division would not be closed.” Text similar to the following may be preferable:

“The CFO admitted to generating false revenue in an effort to achieve budgeted sales figures. He admitted to making the monthly entries with full knowledge of the fact that he was deceiving corporate officials and that his actions were improper under GAAP and company policy. His stated reason for his action was his fear that corporate headquarters would close the division and lay off a large number of employees in his division.”

AVOID SUBJECTIVE COMMENTS

As a fact finder, the forensic accounting investigator must restrict comments to presentation of the facts in such a way as to resolve the allegations that occasioned the original
engagement. The investigator may give opinions about standard and customary business practices that relate to the observed behavior but not directly attempt to characterize the facts as discovered. The investigator should simply report them. If the finding is, for example, that the executive director of a charity has taken a number of trips, reportedly for business purposes, accompanied by family members, the investigator should not characterize such trips as “excessive” or “without business purpose” but should report only the facts. Those reading or hearing the facts can evaluate them in light of organizational policies and applicable laws and regulations.

In the written or oral report, how should the forensic accounting investigator convey an understanding of the facts? We would not recommend the following:

“We noted that the executive director took excessive trips to New York with his family, which were inappropriate and unrelated to the business of the organization, although he expensed the trips as business related.” The foregoing is replete with errors.

• Excessive. The word excessive is judgmental and appears to reflect the personal standard of the forensic accounting investigator. Synonymous words—such as abusive, unacceptable, and extravagant—are also judgmental characterizations and may not have a valid place in your report.

• Inappropriate. This term characterizes the observed action and should be avoided. It conveys a conclusion, not a fact. In the strictly factual realm, the report could note that such travel took place, that it required approval by the individual’s supervisor, and whether or not the required approval was sought or given. The report could also reference a specific provision of the organizational-policy handbook to document the requirement. Each of these facts would enable readers of the report to characterize the subject’s actions—and those readers are then more than likely to deem the actions inappropriate. But that is their role, not the forensic accounting investigator’s role.

• Unrelated to the business of the organization. Such statements are usually made on the basis of assumptions. More likely than not, the trips were indeed unrelated to the organization’s business, but it would be wrong to characterize them as such. The investigator should report either that no business purpose was discovered or that the individual admitted in interview that he knew the trips were strictly personal. Either of these statements may be a better manner of reporting. They report facts, not characterizations.

WORKING PAPERS

Given the familiarity that most auditors have with working-paper-documentation techniques, many of which are applicable to forensic investigation, those techniques are not discussed at length here. However, certain techniques are especially pertinent to investigation, as the following pages demonstrate.

A forensic accounting investigator, once engaged, needs to take certain internal steps to document procedures, findings, and in some cases, recommendations.
These elements of the investigation process are documented in a collection of evidence termed working papers, which divide into two broad categories: internal/administrative and substantive work product.

Forensic accounting investigators naturally want legitimate protections over their work, such as liability limitations and work product privilege, when applicable.

Here are a few important tips for achieving those goals. Judgment, as always, is needed here—these tips are not applicable in all cases—but generally speaking, we advise the following measures.

**SIGNED ENGAGEMENT LETTER**

It is always best to begin the engagement only after you have a signed engagement letter in hand. While there are exceptions to this rule, they should be rare.

Even if the client states you will receive it on the first day of fieldwork, insist on having it faxed to you before traveling to the client site. Often, the client is not focused on engagement administration when there is a need to get the investigation going, but from your standpoint that is exactly the time to get the paperwork done. A client that knows you will not begin the investigation until the engagement letter is signed will be motivated to complete this aspect of engagement administration to set the investigation in motion. Given the sensitivity of the issues covered in the engagement letter, you may now agree more fully than at the beginning of this discussion that it is best to have a signed engagement letter before setting to work.

**RELATIONSHIP REVIEW**

Most firms that provide forensic accounting services have their own procedures for performing a relationship review, or conflicts check, that is, identifying relationships that the firm may have had or now has with any of the parties involved.

The points reviewed and documented may well include the following:

- The date on which the relationship review was cleared
- The individual who cleared it
- Notations of pertinent discussions in clearing current and prior relationships
- The date on which the assignment was accepted

In order for forensic accounting investigators to become familiar with a specific company or situation, they may perform some background research such as checking the Internet, performing a public records search, obtaining a Dun.

However, no investigative work of substance should begin before the relationship check has cleared. Identifying a conflicting relationship that may preclude a firm from accepting the assignment after work has begun reflects negatively on the practitioner, the firm, and even the
client, especially if court-imposed deadlines—such as deadlines for naming experts—have passed.

**SUBSTANTIVE WORKING PAPERS**

Depending on the assignment, substantive working papers in either hard copy or electronic form may include many different items. If the work is being performed under privilege, all working papers should be clearly marked to that effect.

The practitioner should endeavor to prepare working papers as though a third party or regulatory authority may seek to review them. It is not the task of the forensic accounting investigator to assert the privilege or contest subpoenas; the forensic accounting investigator’s task is to maintain its viability of privilege should counsel decide to assert it and likewise to advise counsel if subpoenas are received so counsel can decide whether to contest them. Exhibit 23.2 is an example of a working paper clearly marked with the designation “Privileged, Attorney Work Product” to help identify it as a privileged communication.

**EACH WORKING PAPER SHOULD STAND ON ITS OWN**

Any working papers created by the engagement team should be clearly marked to indicate the name of the creator, the date, the source of information, the information’s classification, and the issue addressed. Such working papers should also be secured so as to ensure that only members of the immediate engagement team have access to them. Certain matters will require the forensic accounting investigators to prove that they have used reasonable means to secure from others the working papers and other evidence. In such matters, custody can be sheet for all who have access to the room.

If a working paper was prepared by the client, it should be so designated, usually by the initials PBC (for prepared by client). If the purpose of a working paper is not evident upon inspection, a simple note of explanation should suffice.

The purpose of a complete set of working papers, as noted earlier in the chapter, is to document the forensic accounting investigator’s work, which should be planned and performed in the expectation that a report will be issued at the conclusion of the engagement even if not specifically requested at the outset.

Numerical amounts or other relevant data should be cross-referenced using the to/from format. The cross-reference on the left should indicate where the number is coming from—for example, an invoice—and the right cross-reference should indicate where it is going to—for example, another schedule or the Report of Investigation. Working papers using this format will tend to have an even flow, such that an independent reviewer will have little difficulty in understanding the nature of support for the conclusions ultimately reached.

Many of the preceding observations have made clear that working papers should be prepared in such a way that they are understandable to an independent reviewer. It is important from
an efficiency perspective to consider that the purpose of the working paper is to document procedures performed and conclusions reached. Neatness, while desirable, is not an end in itself; if it is understandable, then it is acceptable. The most efficient method to make corrections should be used. In many instances that method will entail simply writing on it. Redoing the entire working paper may be unnecessary. Working papers need not be typed or formal. They are intended to document your work. That is all. If the document you create is clear, accurate, and readable, it qualifies as a working paper.
OTHER DIMENSIONS OF FORENSIC ACCOUNTING

Some believe that all forensic accountants perform financial crime investigations. This view is explained largely by the fact that in the post-Enron, post-WorldCom era, forensic accounting has for many become associated solely with fraud detection and investigation. In reality, forensic accountants offer a much wider range of services. Although this book is focused predominantly on the deterrence, detection, investigation, and resolution of corporate fraud, it makes sense to offer here a chapter-length overview of the other dimensions of forensic accounting.

In their day-to-day practice, some forensic accountants focus on commercial disputes in specific industries or practice areas. In commercial disputes, forensic accountants typically play three roles: expert witness, consultant on technical accounting or financial issues, and arbiter of facts. As an arbiter or trier of facts, sometimes referred to as special master, forensic accountants are appointed by the court to act as judge and jury. In their consulting role, forensic accountants may provide discovery assistance, prove business facts, compute damages, and assist counsel in the development of strategy. One should not assume that a forensic accountant involved in commercial dispute projects is qualified to perform financial crime investigations. Close attention should be given to the individual’s qualifications—including certifications and especially experience—before deciding on the right forensic accountant for the task at hand. Assuming that all forensic accountants are interchangeably capable of executing all forensic accounting investigation engagements would be analogous to assuming that all certified public accountants are qualified to prepare tax returns.

While fraud can be sensational and garner headlines, commercial disputes as well as, say, marital disputes among high-net-worth individuals occur often, may entail billions of dollars, and may involve complex issues requiring expert analysis.

The majority of forensic accounting work actually occurs outside of investigations in a wide range of specific practice areas. A glimpse of these areas, suggesting why forensic accounting expertise may be helpful, follows.

CONSTRUCTION

“How does a capital project with a $100-million budget end up costing us $1 billion?”

This question is heard all too often from municipal authorities as well as chief executives and board members of corporations, universities, and hospitals.
Unfortunately, when the creation, development, and execution of a capital project are not the core activities of an organization, cost overruns, scheduling delays, and quality issues sometimes occur.

Good counsel during the planning stages and an active approach taken toward risk management of capital projects may head off many problems before they even start. Ultimately, however, disputes and litigation are reasonable probabilities because capital projects often are fraught with change, and many changes may have various implications for the cost, scheduling, and quality of the project. In many disputes, the contractor brings a construction claim against others involved in the project who are responsible for the added costs. The list of those against whom claims may be made often includes owners as well as other contractors involved in the project. These added costs may take several forms: additional work, forced delays, acceleration of time frames, disruption of work flow, unabsorbed overhead, and marginal cost of capital are some of the possibilities.

Proving the sequence of events, facts, and circumstances that lead to these additional costs may require specialized forensic accounting that blends construction with accounting expertise.

Suppose that in the scope of a project during construction, changes arise that affect the contractor, the construction manager, and several subcontractors.

Further assume that each must now revise estimates regarding time, cost, and materials. Owing to the complexity of the work and the interdependency of relationships, the costs associated with unplanned changes may have multifaceted consequences or cumulative effects that may wipe out all of the contractor’s anticipated profits for the project. Unfortunately, a simple ticking and

Environmental Issues tying of invoices may not help the contractor prove its case. Forensic analysis is often helpful in proving a logical connection between changes in the project and the resulting damages. Moreover, those damages should be calculated to the standard of reasonable certainty, which has been well established by legal precedent.

Given the complexity of the accounts and sequence of events, forensic accountants are often found on both sides of such cases. While one set of forensic accountants may calculate damages and provide expert testimony in court or at arbitration on behalf of the plaintiff, others may work for the defendants by analyzing plaintiff’s expert’s findings and possibly additional issues not considered by plaintiff’s expert, ultimately providing expert testimony intended to rebut damage claims with due force and persuasiveness. Defendant’s expert may also be asked to support a counterclaim with financial analysis and expert testimony.

ENVIRONMENTAL ISSUES

The shock felt across the United States when the Cuyahoga River caught fire in 1969 or when the entire community alongside Love Canal was evacuated in
1977 because of hazardous chemicals buried there has been converted into reasonably tough federal and state environmental legislation. The Comprehensive Environmental Response, Compensation and Recovery Act (Superfund Act); the Resource Conservation and Recovery Act (Hazardous Waste Act); and to a lesser extent the Clean Air and Clean Water Acts sometimes generate complex disputes in which forensic accounting expertise may be helpful.

Specifically, the cradle-to-grave provisions of the Hazardous Waste Act and the shared responsibility of successive owners in the Superfund Act mean that environmental costs and damages can occur quite suddenly and under the leadership of a management team that was not in place at the time of the event. As a result, companies seeking to limit, reduce, or eliminate the costs of cleanup may engage forensic accountants to help reconstruct and present the operations of the company during the period in question.

Suppose that the successive owner of a property that is now a Superfund site is sued for the cleanup of a certain chemical remaining there. By conducting a forensic investigation that demonstrates that it never bought, sold, made, or took possession of the chemical in question, the defendant in the litigation may be able to eliminate or significantly reduce its liability.

In the environmental arena, forensic accountants may be useful in helping to reduce fines levied by the U.S. Environmental Protection Agency under the so called economic benefit model. While the government looks at the economic benefits that have accrued to a company for being out of compliance, forensic accountants look at and present historical expenditures that were made to achieve compliance. Such expenditures may be used to offset portions of penalties ultimately payable.

INTELLECTUAL PROPERTY

In 1982 the value of intellectual assets constituted approximately 38 percent of the aggregate market capitalization of the Standard & Poor’s 500 Index. By 1992 the figure had grown to 62 percent, and in 2002 the figure climbed to over 80 percent. Those figures demonstrate that intellectual property—consisting of patents, trademarks, copyrights, and trade secrets—represents a significant portion of corporate value. As intellectual property grew in importance, so too did the patent and copyright activity designed to protect such assets. For many industries, patents and copyrights represent an important barrier to entry. Yet even as many companies move to protect their intellectual property, they increasingly engage in technology-sharing agreements as well.

While all of these trends contributed materially to the quality of life and productivity gains, they sometimes create fertile ground for disputes, including litigation.

Because intellectual property has unique characteristics, determination of damages may require complex analysis. For instance, in an intellectual property infringement case, there
may be claims of lost sales and profits. But infringement tends to have an impact on prices, competition, and quantities in the marketplace.

Therefore, forensic accountants may often go beyond lost sales and find the additional losses associated with the effects of price erosion, reduced economies of scale, and the presence of competition, among other factors that might not have otherwise existed. In some disputes, forensic accountants may calculate what a reasonable royalty would have amounted to had such a royalty arrangement been in place. This calculation often considers the large number of terms and conditions that typically appear in complex royalty agreements—for example, exclusive versus nonexclusive—and their economic implications.

Many disputes arise out of licensing agreements. Licensors of intellectual property, disputing the ways in which licensees utilize their rights, may claim damages as well as lost profits. Forensic accountants may be consulted to help establish the damages sustained by the licensor, as well as the lost profits resulting from actions taken by the licensee.

In the area of patents, owners of intellectual property may seek protection not just for specific technologies but also for fundamental processes and algorithms.

For example, in 1991 Kodak paid $873 million to Polaroid in a patent rights dispute involving instant cameras and films. The figure that forensic accountants had to establish in this case was the amount of profit that Polaroid had lost.

1. These percentages were derived by a PricewaterhouseCoopers team from S&P 500 market capitalization amounts rather than actual valuations of assets represented on public company financial statements, which do not recognize the market value of most types of intellectual property unless and until there is a transaction such as a sale of the company. Needless to say, investors do factor in off-balance-sheet values, such as market capitalization, when making investment decisions.

GOVERNMENT CONTRACTING

The federal government is the largest customer in the world and has unparalleled creditworthiness. Given the size of contract awards—frequently in the hundreds of millions and billions of dollars—disputes and litigation often arise in the course of government contracting that require complex financial analysis.

In some instances, the government litigates to recoup its costs. For instance, in one landmark case the termination of a contract for a U.S. Navy attack plane, the A-12, provoked a $2-billion demand from the government for the return of progress payments, which in turn resulted in several countersuits for wrongful termination. In disputes brought by the federal government, forensic accountants typically support counsel for the defense, since the government is supported by expertise from other governmental agencies such as the Defense Contract Audit Agency or Office of the Inspector General. The government will also retain external forensic accountants or experts to assist with litigation.
The vast majority of suits, however, are actions brought against the government by contractors or disputes between parties that are government contractors. Claims in these suits often revolve around two primary issues: costs and performance.

Cost disputes frequently center on allocation between direct and indirect costs and their allow ability. When the government disallows costs, plaintiffs may obtain a forensic analysis to help determine the compliance of a cost with a contract or the connection of a cost to work requested.

Performance-based disputes take several forms. For instance, if a government contractor is being terminated, questions may arise as to whether the termination is based on performance or simply for the convenience of the government.

Forensic accountants sometimes conduct a financial analysis of costs incurred against established, time-phased budgets to help demonstrate whether performance is adequate or not. Finally, disputes related to the costs of performance often occur when the government makes so-called constructive changes to a contract.

Forensic accountants assist plaintiffs by analyzing and quantifying the amounts involved.

Corporate forensic investigations can intersect with government contracting when a corporation detects fraudulent activity in the work it is doing for the government.

Forensic accountants also provide investigation support for qui tam

3. The forensic accountant’s testimony is not intended to provide insight on how the contract should be interpreted. Forensic accountants do not offer legal opinions. The financial accounting expert provides a financial analysis based on a specific contract interpretation communicated by counsel, who has engaged the expert. Cases brought against a company by a relator and the government, when fraudulent activity is alleged. In such cases, in addition to conducting an investigation to detect the possible existence and extent of the fraud, forensic accounting investigators may assess the financial impact of the fraud so that adequate reparations can be made to the government in an effort to ward off litigation with attendant possible criminal sanctions.

INSURANCE AND BUSINESS INTERRUPTION

Many insurance policies now include a professional fees endorsement. Many believe that the existence of these endorsements represents recognition on the part of insurers that the preparation of a claim in the event of a catastrophe and the resulting interruption of business involve a complex matter that generates a risk for the policyholder. Companies often retain forensic accountants to help them prepare claims, establish damages and losses, and, in some circumstances, rebut the arguments of the insurance company’s forensic accountants.

One of the primary challenges often facing the insured is to put accounting information into a format that reflects how insurance policies are written. Specifically, while corporate
accounting calculates profit and loss within a production framework, losses from business interruption claims are structured quite differently. In the context of a business interruption claim, loss represents the difference between what happened to a company following a loss versus what would have happened had the loss not occurred. In other words, but for the loss, how would the company have performed? Calculating loss in this fashion is often a multifaceted challenge that, while utilizing accounting, also requires an understanding of factors such as the industry and company personnel. Forensic accountants are often able to reconstruct and estimate how a business might have performed had the insured event not occurred. This is usually compared with post event performance, recognizing the changes in revenues and expenses that occur as a result of the disaster. Changes in the revenue and expense components can be complex because the operations of the business—from what it sells, to where and how products and services are produced—can be fundamentally changed by the disaster that befell the company.

Forensic accountants may establish and calculate the company’s sustained loss and also provide expert-witness services to defend their findings. The challenge is compounded by the activities of similar expertise on the other side of the dispute. Given that reality, forensic accountants acting on behalf of the plaintiff may adopt the pragmatic goal of fighting for the best possible result rather than an overwhelming victory.

MARITAL DISSOLUTION

The incidence of divorce between spouses with substantial wealth often creates several challenges in setting entitlement awards as well as the valuation and division of marital property. For example, when there is a prenuptial agreement, Shareholder Litigation such contracts often specify entitlements based on the living expenses of each spouse. Thus, in a marital dispute, the calculation of the entitlement may rely on estimating these expenses. A complication: the spending patterns established during the marriage often reflect joint expenditures. Forensic accountants may help analyze and separate historical spending to provide a basis for and defense of a proposed entitlement.

Apportionment of marital assets may present a number of challenges, compounded by whether or not the divorce is occurring in a community property state or an equitable distribution state. Questions may arise as to the value of assets that were initially brought into the marriage (premarital assets), their current value, and the portion of the marital estate they now represent. The task of apportionment of assets may lead to the work of tracing assets to determine who account during the apportionment process. The location of assets not disclosed by a spouse may materially weaken a proposed apportionment or give rise to dispute over a proposed settlement. Forensic accountants may be helpful in bringing important facts to light.

Forensic accountants may also address the value of professional goodwill in cases of marital dissolution in community property states. There is a wide range of valuation techniques for
professional goodwill. Establishing a value for this asset—or determining whether it even exists—may have a material impact on the apportionment of marital assets.

SHAREHOLDER LITIGATION

Three federal securities acts create the framework in which interstate securities transactions are regulated. These are the Securities Act of 1933, the Securities Exchange Act of 1934, and the Private Securities Litigation Reform Act of 1995.

Together these laws attempt to ensure that the investing public has sufficient information to enter knowledgeably into securities transactions. Although each law defines a different standard of recovery for investors, the three share a common goal: to make the plaintiff whole via reversal of inappropriate transactions or through monetary compensation of losses stemming from the violation or infraction of the law.

In general, the remedy of monetary compensation requires forensic analysis in order to estimate damages. There are several widely accepted techniques for estimating damages. One of the most widely employed is the so-called out-of-pocket measure, which is the difference between the price paid for a security and the actual value at the date of the sale. While this approach is easily understood, its application is often complex. Forensic accountants can estimate the value of the security in question, absent the alleged fraud or misrepresentation that provoked the action to begin with. The process often requires analyses that take into account macroeconomic information as well as industry and company-specific information. A more numerical, statistical approach to valuing securities uses linear regression analysis.

Shareholders sometimes file lawsuits against corporate officers and directors for violation of securities laws in addition to a wide range of other alleged offenses, including breach of fiduciary duty, personal appropriation of corporate opportunities, discrimination, self-dealing, oppression of minority shareholders, and violation of environmental laws. The majority of suits are brought against directors for the first alleged infraction in the preceding list: breach of fiduciary duty. In such suits, forensic accountants may be engaged to evaluate the causes of a business decline and assess the relationship of that decline to a board’s decisions and performance.

BUSINESS VALUATION

The concepts and principles of business valuation for litigation purposes are the same as those for business valuations pursuing other purposes such as a buyout, creation of an employee stock option plan, or an equity investment. Business valuation in litigation frequently may occur as a result of marital dissolutions, dissident shareholder disputes, corporate dissolution, or a taxable transaction that is subsequently challenged by the Internal Revenue Service or other taxing authorities.

Forensic accountants engaged to clarify such situations often perform intensive data gathering in terms of the financial, contractual, legal, operational, and historical dimensions
of the business under review. That information may be used to develop valuations under a number of generally accepted techniques, including market comparisons, discounted cash flow, net assets, comparable transactions, and comparable sales. Because disputes can arise with shareholders of different classes, the analysis often goes beyond the aggregate determination of value. In many instances, forensic accountants take into account the rights, privileges, and restrictions on various equity securities and assign values to each class.

Forensic accountants sometimes value preferred shares as well as pure equity securities. In such instances, the focus of analysis usually shifts toward a risk based examination, in which forensic accountants evaluate a company’s ability to make preferred-share payouts based on the presence of other fixed-payment obligations and other short- and long-term debt.

**BUSINESS COMBINATIONS**

Some business combinations provoke disputes related to antitrust laws, while others may generate disputes because of clauses in merger and acquisition contracts and the effects they have on purchase prices. In the former arena, plaintiffs establish harm from the anticompetitive effects of the defendant’s antitrust violations.

Forensic accountants may be engaged to help plaintiffs prove, and defendants rebut, alleged damages stemming from restraint of trade. Restraint of trade can take numerous forms, including monopolization, exclusive dealing, price discrimination, and mergers that substantially lessen competition, among others. In many cases, success may rest on testimony and analyses by forensic

**Cybercrime accountants**, who may be able to demonstrate lost profits based on a competitive impact analysis, market definition analyses by product and geography, and price elasticity in the marketplace.

Of course, not all business combinations provoke antitrust claims, but merger or acquisition contracts may generate disputes between buyers and the sellers— for example, disputes that arise from irregularities discovered after closing, the application of offsets, notices of objection immediately following closing, interpretations of materiality, and earn outs. Those are just a few of the possible grounds for dispute. Forensic accountants may assist one or both parties in formulating the dispute, discovery, analysis, and calculation of damages. In litigation connected to merger and acquisition activity, there can be a high degree of subjectivity because of the personal involvement by the principals in the transaction.

Forensic accountants may be helpful in such situations: they have no emotional involvement in the transaction. By providing objective, unbiased analysis, they may help move disputes toward resolution.

**CYBERCRIME**

In the current environment, a security breach may more likely refer to the attack and penetration of a computer network than to a masked intruder on the premises after hours.
When an electronic breach occurs, security specialists may be retained to determine the point of weakness in a corporation’s information systems and to implement remedies that will prevent a comparable breach from occurring in the future. Forensic technologists may be called on to help determine what information or records were compromised and perhaps to look for telltale signs that could aid in identifying the attackers.

Often, however, an attack has consequences that go beyond the immediate need to repair a security breach. In such instances, forensic accountants may be called on to help quantify losses that may include costs to remedy, lost productivity, price erosion, reduction in barriers to entry, and still other factors. Quantifying these losses may also be required in support of criminal or civil litigation.

During the course of litigation, forensic accountants may serve as expert witnesses to establish facts and fact patterns associated with a cybercrime. Forensic accountants may also assist in the filing of an insurance claim associated with losses from cybercrime.

When a cybercrime has occurred, forensic accountants may be asked to help support the settlement of claims between a company and its vendors. The existence of outsourced technology services often means that an attack and penetration result in liability for one or more companies providing technology services.

Forensic accountants may be able to assist counsel in formulating claims specified by their technology outsourcing agreements. The formulation of such claims is often complicated by the interdependent relationships among technology vendors.

As a result, counsel may desire detailed analysis to support claims it is making on vendors.

LOOKING FORWARD: THE FUTURE
The preceding chapters have looked at forensic accounting investigation from a multitude of different perspectives, but one further perspective remains to be explored: the future of the discipline. Compared with the well-defined professions of accounting and auditing, forensic accounting investigation is in its infancy. The largest and most recognized certifying organization in the field, the Association of Certified Fraud Examiners, was founded in Austin, Texas, only in 1988. There could be no clearer sign that the future of the forensic accounting investigation specialty, emerging out of financial auditing and criminology and developing its own repertoire of goals and methods, will be much longer than its past. What can be understood on the basis of conditions and trends today about the further development of this very young branch of accounting?

We propose to approach the intriguing topic of “where-do-we-go-from-here?” in terms of five concerns:

1. The evolution of the discipline itself, including the boundary between financial statement auditing and forensic accounting investigation
2. Education and training for a new generation of forensic accounting investigators
3. The changing regulatory and legislative environments
4. The changing corporate environment, in which the decision to investigate and the process and results of investigation encounter real-world benefits and costs
5. Changes in corporate reporting, especially with respect to nonfinancial operating data (NFOD) that may be subject to some form of assurance or formal review and may be subject to fraudulent manipulation

**Evolving Discipline**

We believe that the boundary between financial statement auditing and forensic accounting investigation will become more clearly drawn as major practitioners, from the Big Four accounting firms to forensic accounting investigation consultancies, gain more experience. At the time this book went to press, that boundary appeared to be still somewhat fluid in firms that offer both audit services and forensic accounting. Statement on Auditing Standards (SAS) No. 99, Consideration of Fraud in a Financial Statement Audit, of the American Institute of Certified Public Accountants.
Public Accountants (AICPA) has sharpened the focus on professional skepticism by instructing auditors to design and conduct tests for detecting material fraud and to hold periodic team discussions that cover the potential for material fraud. Many of the larger audit firms have instituted increased levels of training in fraud awareness. All of these developments are needed and important, yet throughout this book we have underscored the critical importance of bringing in qualified, specialized forensic accounting investigators when the red flags of possible fraud become evident. In our view, the complexity and breadth of forensic accounting investigation—and the need for experience—make this the appropriate decision. The more thoroughly forensic accounting investigation is understood, the more quickly and prudently policy is likely to be developed in multiservice firms—and in the minds of corporate management, directors, and counsel—as to when it makes sense to engage forensic accounting investigators.

Paradoxically, a clearer boundary between financial statement auditing and forensic accounting is likely to be accompanied by greater contact between the two functions—more “touch points,” as some people put it. This will not arise in the normal course of auditing but, rather, only when suspicions of fraud arise on the audit.

An interesting parallel to the discipline of forensic accounting investigation can be found in the medical profession. There was a time when the general medical practitioner was the first and last doctor to see a patient. However, as medical science progressed, specialists emerged to diagnose and treat complex ailments that were becoming increasingly well understood. We believe the discipline of forensic accounting investigation will evolve in much the same way—and very rapidly. Just in the past decade—and certainly since Enron and World-

Com—there has been greater appreciation of the discipline of forensic accounting investigation. Management and the board better understand the discipline’s effectiveness in investigating and resolving allegations of fraud, and independent audit firms have built forensic accounting investigation teams within their organizations to be deployed when the need arises.

Like the movement from the general medical practitioner to the medical specialist, we believe that the next step, over the coming 5 to 10 years, will be forensic accounting investigation subspecialties within the broader discipline.

Just as forensic accounting investigation emerged as an independent specialty from two disciplines—financial accounting and criminology—we expect subspecialties to emerge soon within the field itself. They are likely to be industry focused, offering expertise in the business practices that investigators will encounter in such industries as telecommunications and financial services (examples chosen because they are global and complex). However, before this change can occur, the numbers of those specializing in forensic accounting investigation will need to increase drastically from current levels. While there are more than 336,000 certified public accountants (CPAs) in the United States, only about 5 percent carry CFE (certified fraud examiner) certification from the Association of Certified Fraud
Examiners. On a global basis, the percentage is even lower when compared with accounting certifications that are comparable to the CPA. With the increasing levels of complexity and integration in the global economy, demand for the specialized insight of forensic accounting investigators will increase, especially if regulatory regimes continue to add requirements.

A third trend is toward greater use of digital tools in aid of forensic accounting investigation. Two factors appear to be driving that trend: (1) increasingly clear technology preferences and strategies among businesses and among regulators that require business data and (2) improvement in the digital tools available to forensic accounting investigators. U.S. regulatory authorities are beginning to standardize around certain systems and to have preferred software. On their side, many companies are becoming increasingly skilled at using their digital networks to reduce costs. They use networks to limit their paper, store records, operate systems of approval, and to do much else. In many enterprise-wide accounting systems, the approval recorded in the system awaits the matching of documents, after which the transaction is automatically approved and moves through the system.

The still-growing role of digital networks has implications for the future of forensic accounting investigation. One of the subspecialties that may well appear may evolve into a commodity-like, standardized service. We believe it is important that the two functions remain combined for the simple reason that data analysis may fall far short of its objective if data is not gathered in a forensic manner.

Data gathering is too important a task to outsource to those unfamiliar with forensic accounting investigation. It would be comparable to having the police outsource evidence gathering and opt only to analyze whatever the service provider gathered and dropped off at the police station. Most of us would not think this a good idea. Data gathering is no different.

At present, collecting and interpreting data are closely linked services performed by unified teams of professionals who really understand accounting systems.

They typically know where to look, how to find the critical data points in a fraud investigation, and how to interpret what comes to light. Will the increasing capabilities of digital systems drive a wedge between doing and thinking, between data collection and interpretation? We don’t think so. Experience indicates that the two capabilities are complementary and equally necessary in corporate investigations. However, the challenge for the provider of these services is to manage a business based on intellectual capital while at the same time offering commodity-like services based on standardization.

NEW TOOLS

There can be no doubt that the electronic tools available to forensic accounting investigators will continue to ramify and improve. As in many other fields, the Internet has created communities of interest at Web sites where participants can share information about new tools and the use of existing tools.
One of the most interesting trends is toward improving on existing software applications by developing proprietary applications of far greater capability than those offered commercially. For example, while powerful data-mining software is commercially available, it may not always be capable of extremely high volume, data-mining exercises. Forensic accounting investigators involved in such projects may need to ask their technology coworkers to adapt existing programs to meet the demands of such large-scale projects. For projects of average scope, however, commercially available software is virtually certain to keep improving and to be up to the challenge.

EDUCATION AND TRAINING: TO BETTER SUPPORT THE NEW DISCIPLINE

We see signs of a positive trend: in the future, an increasing number of undergraduate and graduate programs are likely to offer courses in forensic accounting investigation. For courses to be more than conceptual overviews, they should be taught by those who have performed hands-on work in actual investigations.

This need suggests the value of crossover teaching arrangements that have, in fact, already been piloted with success at a handful of U.S. institutions. Working forensic accounting investigators often prove to be enthusiastically willing to teach and team teaching with resident academics may be the most effective formula.

Even guest appearances by experienced forensic accounting investigators would be gains in the context of ongoing courses on audit methods. Seasoned forensic accounting investigators should find a place in universities.

Firms with forensic accounting investigation capabilities may be persuaded to fund tours of duty for academics to join their forensic accounting investigation teams, so that those individuals can experience the attitudes and methods and the uncertainties and problem solving of the real world of forensic accounting. As well, we would expect—and we certainly hope for—a trend toward investment in education on the part of major firms with forensic accounting investigation capabilities either by their funding of college programs or by their funding of chairs in forensic accounting investigation.

Fraud detection is a continuing concern of regulators and auditors. The cooperation of auditors with forensic accounting investigators is an important element in restoring investor confidence. Education and training need to catch up with the new realism initiated by SAS 99 and the Sarbanes-Oxley Act. We believe this will occur in the next 5 to 10 years.

REGULATION AND ENFORCEMENT

Today’s environment in corporate reporting is one of increased transparency.

Major U.S. corporate scandals and the 2002 enactment of the Sarbanes-Oxley Act signal what we take to be a prolonged swing toward heightened regulation and enforcement. The 302 and 404 requirements of Sarbanes-Oxley, the definition and
enforcement of services prohibited to professional services firms, the reactions of audit committees to those new rules, highly publicized criminal charges against formerly influential executives, investigations and enforcement actions against entire sectors of the financial services industry and world-class financial institutions—all of this and more signal a strong swing of the pendulum toward a risk-averse operating environment for U.S. businesses and for foreign businesses operating in the United States.

Will the trend last forever? Has it become an enduring feature of the U.S. business and economic climate? Even while it has been gaining strength, there have been dissenting voices, not without reasonable points of view. It is all costing too much to no purpose, some say. It is anticompetitive. It is making our capital markets less and less attractive to foreign companies and investors. Material financial statement fraud is estimated to occur in just 2 percent of all U.S. public companies, and in any year typically less than 1 percent of all registrants are accused of making false filings. In light of these statistics, aren’t the American public, legislators, and regulators overreacting by treating all companies as if they were about to enter that 2 percent category?

From our perspective, these are all reasonable points, although they too should not be taken too far. While the percentage of wrongdoing is small, the devastating effects of the catastrophic business failures of the past few years should not be minimized. One could argue, for example, that the Federal Aviation Administration imposes excessive scrutiny on the airline industry out of concern for safety. But would any of us be happier with less oversight and a markedly higher crash rate? That is highly unlikely. While it may not be fair to compare loss of wealth to loss of life, both safe aviation and the integrity of public companies are significant matters of public concern, on which the lives and welfare of many millions of people depend. We believe the trend toward risk averse regulation and aggressive enforcement will continue for at least another five years.

By the fall of 2004, the U.S. Securities and Exchange Commission (SEC) had nearly completed building a much-enlarged staff. The SEC was deliberately hiring very experienced individuals—including partners and directors from major accounting firms. The Public Company Accounting Oversight Board, created by Sarbanes-Oxley and still very new as this book went to press, had not yet fully demonstrated how it would approach its mandate, including enforcement. But overall there could be little doubt that federal agencies charged with safeguarding the integrity of public markets and overseeing independent public accounting services would be more far-reaching and active than at any time past.

Pressure exists on the accounting profession—external auditors, internal auditors, and forensic accounting investigators—to scrutinize accounting policies and practices, and to respond quickly and thoroughly to government inquiries. Regulators have widened their focus on alleged acts of individual wrongdoing. How can or should the regulatory and
enforcement environments affect the forensic accounting investigator? From a technical perspective, they have their impact: new regulation is likely to create additional zones of corporate activity in which fraud allegations show up and require investigation. The forensic accounting investigator’s advisory role is likely to increase as clients decide on how to respond to new regulation imposed on corporations and on the accounting profession and how to create safeguards and systems to comply with the requirements as economically as possible. The forensic accounting investigator’s role is unlikely to decrease. There is a constant need for such expertise and practical capability, and the integrity of public markets relies in part on the readiness of forensic accounting investigators working in concert with auditors, directors, and management to resolve allegations thoroughly and efficiently.

**CHANGING CORPORATE ENVIRONMENT**

In many cases, managements and boards of directors are becoming much more aware of their obligations, new and long-standing, to deter and combat fraud within their organizations. Many audit committees are listening; they are meeting more frequently and more probingly with auditors, and they are requesting additional investigation of alleged frauds when that seems to be the prudent course.

Some audit committees are adopting the loose-thread approach to evidence of possible fraud, which we have recommended in this book: where there are small indicia of fraud—small threads out of place—those audit committees are interested in looking more closely to discover whether something more important and pervasive may be underlying. The professional standards governing the work of those committees now require further inquiry when evidence of possible fraudulent behavior surfaces, even if the amounts is likely to be quantitatively immaterial.

1 The CEO and chief financial officer (CFO) are specifically charged with certifying the financial statements, and they must report to the external auditors and the audit committee any incidence of fraudulent behavior committed by those involved in the internal controls over financial reporting.2

Many companies are recognizing the need for codes of conduct and ethics statements that suit their particular industry and circumstances. When there are ethical benchmarks of this kind in place—and training programs to support those—companies can hold their executives and staff to certain standards: “What do you mean, you didn’t know that you shouldn’t do that? You signed off on the

**Changing Corporate Environment code** of conduct and the code is crystal clear in this area.” Companies can leverage well-constructed codes of conduct to ensure accountability from the top to the bottom of the organization.

In the coming years, more companies will be clarifying their organizational approach to fraud investigation. Often enough, still today, a business unit in a distant location may prefer to conduct its own investigation of alleged fraud rather than refer the issue to headquarters for
advice and counsel. Unfortunately, when distant business units act in this way, they may prevent corporate management and the board from gaining an accurate picture of the problems of geographically remote operations. In the end, putting up a screen around local fraud investigations, so as to avoid criticism or questioning from higher-ups, can work against the larger purposes of the company. The local business unit may assert that it was only trying to do the right thing, but headquarters may have the perception that the unit has something to hide. That is hardly a productive situation for either party. There are signs that companies are becoming aware of this type of problem and addressing it.

Similarly, we see a positive tendency on the part of companies to prepare better in advance through policies and procedures that will address allegations of fraud without delay, should they arise. Companies are learning not to wait until fraud is detected to develop an operating plan. Management and/or the audit committee is more frequently asking itself such questions as, What will we do if we’re subject to an investigation by SEC enforcement? What will we do if the president of a foreign subsidiary is accused of cooking the books? Management and the board need not adhere in every detail to the crisis management plan thus formulated, if and when a serious fraud allegation crops up, but at least they have a blueprint for response. Companies wholly unprepared for these types of events may become, at least temporarily, ineffective and slapdash in their decisions, with negative consequences both internally and in the public arena.

Thorough planning in advance of an event is becoming more common today, driven by the requirements of Sarbanes-Oxley, by SEC rules, and by evolving professional guidelines for financial statement auditors.

INTERNAL AUDIT

Are there signs of change in the fraud detection capabilities of the internal audit function in U.S. public companies? Some companies’ internal audit functions are becoming more capable of fraud detection through training. It is fair to say that internal audit teams in public companies are under pressure to make a solid contribution to procedures that comply with Sarbanes-Oxley Section 404, which requires public companies “to publish information in their annual reports concerning the scope and adequacy of the internal control structure and procedures for financial reporting. This statement shall also assess the effectiveness of such internal controls and procedures.” While internal audit units are quickly becoming more skilled at doing process reviews and 404-related work, few of them may be ready at this time to undertake, for example, an investigation of alleged fraud in a workers’ compensation fund or suspicious accounting in an overseas subsidiary, to name two types of investigations that can be complex in scope and depth, but the trend is toward increased awareness and clearer recognition of circumstances in which it makes sense to call in forensic accounting investigators.

There are many, fully justified; barriers that prevent internal audit shops from growing their own fraud investigators—for example, staff rotation and the desire to dispel the perception
that internal auditors are corporate police. This does not mean that management and the audit committee should not direct internal audit to prepare for the possibility that investigations may be needed. To touch again on the theme of advance preparation, many perspicacious managers and directors are also prearranging with outside accounting firms or other forensic service providers for the timely engagement of forensic accounting investigators.

Thoughtful planning will enable a company to properly interview prospective firms and agree on terms and hourly rates ahead of time so that when the need arises, forensic accounting investigators can be deployed immediately. Having these arrangements in place can go a long way toward meeting the challenges of investigation in a timely and effective manner, and time is often of the essence.

CORPORATE JUDGMENT CALLS

We want to call attention to an issue that is more than likely to evolve as companies gain experience under the new fraud-related rules and obligations applicable to management, boards, and auditors. Management and the board face decisions when allegations of fraud are investigated and there appears to be evidence of questionable conduct or outright wrongdoing. In times past, some management have found themselves weighing their regulatory obligations and personal ethics against their mandate to enhance shareholder value and protect their company’s reputation. These companies in the past may have struggled with a decision whether to disclose the conduct that today is made much more easily. Today’s environment demands greater transparency and full disclosure.

We believe that the new reality argues toward fuller disclosure and greater transparency despite the potential risks of public disclosure that corporations may fear. Sarbanes-Oxley and other regulation have put a firmer legal framework around greater transparency, and companies are learning—at least from the experience of other companies that get into trouble on issues of fraud—that it can serve long-term shareholder interests to investigate and report.

FORENSIC ACCOUNTING INVESTIGATORS SERVING INDIVIDUAL CORPORATE CLIENTS

Individual corporate leaders are likely to continue to be the targets of investigations by the U.S. Department of Justice (DOJ) and the SEC. The result may be a new deployment of forensic accounting investigation expertise directly in defense of individual executives. As this book went to press, forensic accounting investigators continued to be deployed primarily to investigate allegations within the corporation and alleged irregularities in financial statements. But it seemed clear enough that senior executives and directors under fire might find it

The formal accounting definition of error, in APB 20, reads that you can err in making an estimate if you overlook, misuse, or misinterpret facts available to you at the time. An estimate is basically a decision. Forensic accounting investigators have long looked at estimates, as have auditors, and considered whether the decisions in question were reasonable
in light of the portfolio of information available at the time. This long-established element of both forensic accounting investigation and financial statement auditing may become a core defense over the next 5 to 10 years for senior executives who are alleged by the DOJ or SEC to have broken the law.

Because actions against individuals often occur after actions against companies, attorneys defending those individuals and calling in forensic accounting investigators to help them assemble and analyze the facts will often be able to draw on records already established, such as the trial record, discovery record, deposition record, and/or SEC hearing record. It may serve these individuals well to be able to demonstrate that they did not know certain things at the time they reached certain decisions or that someone with the intent to do what they are accused of doing would have had to know certain things, entirely unknown at the time, in order to accomplish the alleged wrongdoing. The forensic accountant’s command of investigation and analysis may become a central asset on both sides of these cases.

NONFINANCIAL OPERATING DATA

For the most part, this book addresses the risks to financial statements and their attendant disclosures, but an even greater challenge waits. Beyond the financial statement numbers lies an entire universe of numbers and assertions disseminated by corporate management that influences investors and lenders alike as they decide how and where to deploy their capital resources. Financial statement numbers are not the only numbers that generate interest in companies. For example, an impressive, publicly stated number of cable subscribers or the dazzling, publicly stated market prospects of a new drug may well attract an investor’s gaze more quickly than any balance sheet, income statement, or earnings forecast.

While regulators and legislators are quickly implementing rules designed to restore investor confidence over financial reporting, another issue has arisen.

Nonfinancial operating data (NFOD) is quickly gaining importance in the investment community, and although many investors and market analysts may not yet realize it, very little if any of this data is audited. True, management bears the responsibility, imposed by regulators, to report NFOD accurately, and the external auditor must read such data, but the external auditor provides no assurance on the accuracy, completeness, and validity of such data. Hence, the concluding topic of this book: NFOD in relation to the work of the forensic accounting investigator. Real challenges lie ahead.

To ensure success, businesses today must carefully manage a complex web of what we call value drivers, many of which can be measured and reported. And, a noted earlier, investors are increasingly looking at indicators other than historical earnings to assess the financial health of a corporation. Value drivers vary from company to company and from industry to industry, but they typically include the ability and commitment of their people to deliver on strategy, the degree to which customers trust their products and services, the competitiveness and reliability of their business models, and their capacity to share knowledge, to learn, and to adapt to changing circumstances. None of these is a financial measure, yet all are
increasingly important not only as pieces of internal management information but also as measurable, reportable data. Other nonfinancial performance indicators of and format that information, we believe that there will be a need for skilled forensic accounting investigators to address concerns over possibly fraudulent