This chapter will discuss the initial investigative steps to be taken when fraud is known or suspected in a bankruptcy case. It is intended to provide a schematic diagram for an attorney or trustee wondering where to start and what to focus on. Readers should be cautioned that this is not meant to be a complete or comprehensive plan of investigation. It should be viewed more as a schematic diagram than as a detailed or authoritative how-to guide.

According to the *Report to the Nation on Occupational Fraud and Abuse* published by the Association of Certified Fraud Examiners, the typical occupational fraud scheme lasted 18 months and the most frequent method for detecting it was a tip from a co-worker, customer, vendor, or anonymous source. The second most frequent method of detection was characterized as "dumb luck". The typical fraudster (93% of them) was a first-time offender – i.e. someone that would not usually be suspected. The threat of punishment was not a serious demotivator because the fraudsters typically began their schemes with very small amounts and with no expectation of getting caught. In their initial stages, the frauds were small and innocent looking enough that they could be explained away as mere mistakes. Over time the frauds grew as their perpetrators gained more confidence that they were not being noticed.

The categories of occupational fraud that usually pertain to bankruptcy are misappropriations of assets and fraudulent financial statements. This is important to keep in mind throughout the following discussion of fraud investigation. Fraudsters tend to be trusted individuals who are good at deception. Their frauds typically start small and are designed to look like mistakes or incompetence, while they probe to determine what they can get away with. They often intended it to be a one-time only event and then got sucked into the addictiveness of free money. As the fraudster gets more confident, the fraud grows in both amount and frequency, and this magnifies the trail that the fraudster leaves behind. As the fraud grows, it becomes more likely to be brought out into the light from a well-structured investigation.

The type of fraud known to or suspected to have occurred determines the scope and type of investigation to be performed. The first steps involve identifying what did or may have happened – the fraud theory upon which you will base the investigation. Narrowing down the theory of the fraud helps in determining which documents and other evidence you should focus on.

Develop a Theory of the Case

The first thing to do when a case with known or suspected fraud comes in is to determine what is known and the extent to which it has already been investigated. Known fraud is usually identified by whistle-blowers, management's internal investigation, a criminal investigation in process, or litigation that has at least been threatened. A case with known or suspected fraud should begin with discussions with as many of the relevant people as possible to determine who knows what. It is common that unless a case has already been exhaustively investigated by law enforcement or competent forensic accountants, there will be many people who each hold a piece of the puzzle but lack an over-all view of the case.

It is important to remember that insolvency can be triggered by many factors. These can be internally generated by poor management, undercapitalization, over-dependence on critical customers or vendors, poor planning or execution, operational deficiencies, and lack of accurate management information. They can also be generated externally by government, industry conditions, the economy, labor problems, obsolescence, competition, shifting consumer preferences, and other factors. Insolvency usually generates anger and feelings of being cheated, which in turn generate accusations and finger pointing. Fraud could be a factor behind the insolvency, but insolvency is not by itself an accurate indication that fraud occurred.

In some cases, insolvency is the motivation for fraud rather than fraud being the cause of the insolvency. Businesses that have suffered economic downturns or have themselves been defrauded may turn to fraud to buy themselves time to recover. In these cases it would be a mistake to focus too much on the cause of the insolvency because the perpetrator of the fraud will already be using that as his or her cloak for the fraud that they've committed. In cases where a debtor has itself been defrauded, that original fraud may be the template that was used to subsequently defraud the debtor's victims.

It is important to understand both the business environment of the debtor and the theory of the fraud case, as there are many different ways in which they can be interrelated.

Whistle-blowers

Whistle-blowers are often anonymous. Their tips can be sent in to management, directors, owners, or outside investigators and can be in the form of phone calls, e-mails, letters, or hotlines. Larger companies may even have websites or blogs created by employees as a place to vent and trade information. Trustees should publicize their appointment as widely as possible in the community that was involved with the debtor so that tipsters know who to come forward to. Anonymous communication should always be considered suspect, but should never be ignored. Determine how seriously to take it based on how plausible it appears, how specific it is, and by how closely the fact pattern described fits with other facts known about the bankrupt company.

Remaining or former employees will often openly come forward with fraud tips in a bankruptcy. It should be kept in mind that in an insolvent company there was not enough money to go around, and the employees coming forward may be doing so out of revenge because they feel cheated or abused by former management. Employee claims should be listened to but handled carefully. In one bankruptcy fraud case that I worked on there were rumors of two senior managers having affairs with employees. In one instance the rumors were never substantiated, but in the second it was found that cash skimmed out of the company had been used for a substantial down payment on an expensive house purchased in the name of the company's shipping clerk, who was having an affair with the other senior manager. Had those rumors not been given credence, the skimmed-off cash would never have been found.

Tips often allege malfeasance, but not necessarily theft or fraud. Identify what the real implications of the tip are and what kind of impact the alleged acts could have had on the debtor. Does the information provided make it plausible that there was fraud, given the state of the controls, systems, and procedures

in place at the company and the ability of the person being accused to over-ride them? If so, further investigation is warranted. Tips involving changes in lifestyle such as new cars or homes, or tips regarding financial stress on an employee such as college, medical or other family needs should always be seriously paid attention to.

Management Investigation

Large companies almost always have internal audit departments. Obtain an understanding whether the focus of the internal audit department was on adherence to policy and procedure or a broader range of review and how likely it is to detect fraud. Deference to management and limitations on the scope of what the auditors were allowed to review can be significant hindrances to internal auditors. Nevertheless, if certain managers obstructed the internal auditors or scaled back their access to certain types of transactions, just knowing this could be a good tip as to an area requiring further investigation. Auditors may also provide valuable information about the corporate culture, the control environment, and other observed patterns in the company that just didn't fit properly in the context they were in.

In rare instances senior management has already begun an investigation into possible fraud at the debtor company. If they know with reasonable certainty who defrauded and bankrupted their company there is a good chance that they have either brought law enforcement into the case or hired a forensic accountant already. This may not always be the case, though – I've been involved in two separate cases where management indicated that their company was a victim of organized crime and they were eager to turn over accounting and other records that would help a third party discover the criminal acts, but were too afraid to go "on the record" with any of their personal knowledge to law enforcement. In this instance the best the investigator can do is get as much information from management as possible and then decide whether that is enough to proceed on.

Management investigations may have been performed to throw the trustee or other investigators off of the correct trail. Large-scale fraud is more likely to have been committed by management than by lower level employees. Beware of managers who are too ready to cast suspicion on a wide net of unspecified employees or outside parties but who only have theories and immaterial or circumstantial facts. Managers who profess too much ignorance typically are not being honest. Managers who truly are ignorant usually do everything they can to hide their ignorance.

Outside Sources

In addition to employees and managers, outside sources are typically a wealth of information about the activities that took place at a company. Vendors and customers know who in the company has lied to them and what aspects of operations those lies covered. Alert vendors often can sense changes in their customer's cash flow patterns sooner than inattentive management can, and observant customers usually detect operational changes within a company by noticing differences in service level, quality, delivery time or method, and other factors. I have been involved with bankruptcy cases where customers reported changes in remittance addresses, changes in the banks used to cash their checks, discounts for cash payment, unusual delivery methods, and other facts that quickly led to the location of diverted funds.

Bankers, tax preparers, outside auditors, legal counsel, insurance agents, payroll processors, travel agents, computer service providers, and outside consultants the debtor used are also good potential sources of information regarding what went on at the company. Great care and discretion should be used in obtaining phone records, but if those can be obtained legally they can be a great source of information that identifies companies, people, or places that someone in the company had significant contact with but for which there is no apparent business purpose. Itemized telephone bills are often maintained in the company's ordinary expense voucher files.

Again, care must be taken not to jump to conclusions when interviewing outside sources. Companies in financial distress often are forced to change delivery methods, payment patterns, sales terms, and general ways of operating. The results of interviews with current and former employees, managers, customers, vendors, bankers, and other parties need to be taken in context. Look for patterns, unusual activity, or connecting facts that can highlight the potential fraud areas to be further focused on.

<u>The control environment of the company</u>

As a part of the information gathering process, examine the operational environment of the company – what do they do, how do they do it, how is the organization structured, how do goods or services flow through the company, how does money flow through the company, what is critical to the success or failure of the company, etc. Where are high dollar items (inventory, machinery, key people, etc.) housed and how are they controlled? How knowledgeable and professional do company personnel appear to be? Assess the apparent trustworthiness of key people - although this is highly subjective, the intuition or "gut feel" of an experienced investigator very often is an extraordinarily reliable indicator of where to begin investigating.

Assess the system of internal controls in place at the company. Internal controls are the policies and procedures that companies use to measure, monitor, control, and react to what is going on in the company. They can be as simple as a lock on a door to as complex as a detailed manufacturing process or specific instructions on the implementation of Generally Accepted Accounting Principles. They can either force specific action to be taken or can monitor and detect what has already occurred. Some controls can be in place without the users ever knowing about them – for example, many accounting software packages have audit trails built into them that track every modification to any accounting entry made in the system, and because this is a standard feature the users may not be unaware that it exists.

Begin the assessment by identifying the processes, control points, significant people, and risks. These vary from company to company – for example, a company that buys and melts gold scrap will require a totally different set of internal controls than a retail convenience store will. In larger companies the controls will be documented. Keep in mind that what is in the procedure manual may not necessarily be reflective of what people actually do – it is not uncommon that controls get documented to satisfy auditors or regulators, but in practice are routinely ignored or circumvented. This can often be determined by observation if the company is still functioning and by discussions with employees about how they perform their tasks on a day to day basis.

While rules and procedures are important, the tone set by management is much more critical. Rules and standards don't prevent fraud—good management, the right culture, and well designed controls that employees will implement and adhere to are what minimize losses. If management is cavalier towards controls and ethics, employees are likely to have that same detrimental attitude. If company managers rely too much on written policies and procedures, they are likely to establish a set of rules far too bulky and complex for the average employee to follow, and the rules will be ignored by even well meaning employees who just can't absorb and comprehend them all. In many companies where employees are not able to follow the controls because they are too cumbersome, management often institutes even more rules and procedures in an attempt to improve operational execution, rather than simplifying what is already too burdensome to be effective. When a company produces a policy and procedure manual that makes the tax code look small and simple by comparison, there is an excellent chance that its internal controls are not being adhered to.

Management tone can be determined in a number of ways. The most common is through discussion with both managers and rank and file employees. Visual observation of workspaces also gives many clues – are workspaces neat or disorganized, self-decorated or company decorated, uniformly clean or up to each employee to clean their own space, etc. Are records well maintained or is paperwork strewn about everywhere? Decorations hung on the sides of computers and cubes give a wealth of information regarding employees' attitudes towards the company, their jobs, and life in general. If possible, notice how employees react when their manager speaks to them or even just enters their work area. How different is the mood in designated break areas as opposed to in work spaces? Do employees carry stress, anguish, boredom, a sense of urgency, dedication, enthusiasm, or other emotions and attitudes in their faces and postures while at work? Do they respect management or snicker behind its back? Do they appear to trust what management tells them? To an experienced eye a preponderance of such observations can often be a more reliable indication of the company's control environment than whatever is written or proclaimed by senior management.

Another indication of management tone that I find particularly useful is to review management expense reports. One fraud case that I investigated makes a particularly good example. Four of the top six executives, including the CFO and Vice President of Sales, had very modest expense reports. The remaining two, the CEO and the Vice President of Operations, spent lavishly – they flew on private jets, stayed in the most expensive suites of the most expensive hotels, and were regulars at one of the city's most expensive steak houses. While their expense reports may not have technically violated company policy, they demonstrated a sense of entitlement and carelessness with company funds that did permeate to other employees of the company. These traits were found most heavily in fellow employees who were identified as guests of these two managers at many of the lavish meals detailed on their expense reports. Some of these employees were subsequently found to have defrauded the company. None of the senior managers who submitted only modest expense reports were themselves implicated in the systematic fraud that was uncovered at the company, even though some of them eventually admitted to being aware of what others in the company were doing.

Information to start with

There are three elements (known as "The Fraud Triangle") that are usually necessary for a person to commit fraud – pressures / incentives, opportunity, and rationalizations / attitudes. Pressures or incentives to commit fraud are usually specific to the individual and difficult to discern from merely studying what went on at the company. The opportunity to commit fraud is directly related to the strength of the company's internal controls. Rationalizations and attitudes very often arise from or are exhibited by the management tone of the company.

As stated above, begin the inquiry with a structured set of questions and observations. It cannot be over-emphasized how important first impressions and intuition are – when something just doesn't feel right or look right while touring a debtor's facility or talking with management, there is a very good chance that it isn't right. Almost all insolvent companies exhibit signs of stress and turmoil at the end of their pre-petition life, but a good eye that has seen many different companies in their terminal phase will be able to differentiate what is normally part of the insolvency struggle and what shouldn't be seen despite everything the company has been through.

The following list of questions is a starting point. The list may appear long, but an experienced investigator can obtain most of this information during the initial walk-through of the debtor company. The questions asked should be tailored to the specific situation and augmented to follow up on any observations or concerns that arise during the information gathering process.

- What specifically has raised the suspicion of fraud?
- Who is aware of the allegations of fraud?
- What time period did the suspected fraud occur in?
- What is believed to have been taken, and who was it taken from? Can it be quantified?
- Which specific transactions or what type of transactions are considered suspect?
- Has there been unusual employee turnover at the company? Can the turnover be satisfactorily explained?
- Have key management people left the company? Are they available to talk with?
- Have any employees in sensitive positions (management, cash handling, accounting, shipping and receiving, etc.) experienced significant lifestyle, attitude, or behavioral changes? Even if the employee proclaims to be unaffected by it, this could include divorce or breakup, family illness or death, financial loss, education needs, helping to realize a child's athletic potential, natural disaster, change in relationship with a member of management, being passed over for promotion or raise, class reunions that could have spurred envy of peers, etc.
- Who are the key people involved? Are they still available to assist with the investigation?
- What computer information, documents and records are available? Are they secured? Where are they? Who has keys or passwords?
- What evidence outside of the company's books and records would be helpful?

Knowledge of the company, its industry, and the environment that it operated in are very important towards helping to put the information gathered into the proper context. Some of the information to gather includes:

- Understand the industry the company operates in – major products and services, key technology, degree of competitiveness, government regulation, the macroeconomics that impact it, the key drivers of sales and costs, the financing and investment environment, and anticipated evolution.
- Understand the company's customers – who are they, how do they make their buying decisions, what are they buying, how do they pay for it, how much does it cost to support them, how easy is it to retain them, how loyal are they, what is their frequency of purchase, what are average transaction sizes, and who are they loyal to (the company, the owner, their salesman, etc.)
- Understand the company's employees – their experience levels, skill levels, contacts, mobility, attitudes, motivations, loyalties, and level of commitment.
- Understand the company's vendors and other creditors – who are they, how much leverage do they have in the relationship vis a vis the debtor, how concentrated is the market.
- Understand the economics of the business – normal or expected gross and operating margins, profit potential and durability, cost structure (fixed, semi-fixed, and variable), breakeven points, cash flow dynamics, etc.
- Understand the company's marketing strategy – pricing, sales tactics, service and warranty policies, advertising and promotion, distribution, who the target market is, etc.
- Understand the company's operations – the operating cycle, the geography, facilities and improvements, budgets and plans, regulatory and legal issues, etc.
- Obtain or generate a flow chart of the organization and identify key personnel, their compensation, their employment and incentive agreements, their roles and responsibilities, key controls that depend on them, and their access to sensitive assets or information.
- For both the company and the industry, obtain historical financial information regarding sales levels, profitability, and key trends and ratios.
- List the major investors and creditors of the company. Who is personally responsible for unpaid liabilities or losses?
- What are the company's major assets? Note that in today's service economy intangibles that are not listed in any company books or records may be the company's most significant assets. These can include customer lists, proprietary processes, trademarks, contractual rights, an assembled workforce, or software. How attractive are these assets, how portable are they, and who has access to them?
- What are the company's major expenses? How are they paid for (payment methods, terms, etc.), who are they paid to, what competitive and financial shape are the vendors in?
- What are the company's major sources of financing? What restrictions are placed on it – covenants, guarantees, security granted, expiration, and other terms.
- Assess the company's accounting and record keeping – are entries booked in a timely manner, are reconciliations performed on a routine basis, who reviews the accounting data, what reports

are generated and who uses them, are physical documents properly stored, is there a reliable audit trail, etc.

Even the very smallest businesses today use some type of accounting software. If possible, obtain an understanding of the system environment of the company, what data will be available, and how reliable it is likely to be:

- What software is being used? Is it off-the-shelf or custom?
- Who has access the data?
- How large are the data files and what format are they in?
- Who initiates transactions? What are they based on? Who approves them?
- Which software modules (sales, production, purchasing, receiving, inventory, etc.) feed entries into the accounting system?
- What entries are system generated? How can they be overridden?
- What source documents exist to support computer entries? How and where are they maintained?
- Understand the accounting workflow. Note that different transaction types – sales, cash receipts, accounts receivable, accounts payable, inventory, etc. can all have different workflows and controls associated with them.
    - What is manual and what is automated?
    - What controls exist and how can they be overridden?
    - At which points in the transaction cycles are entries made?
    - How are entries validated?
    - How much manual calculation, measurement, estimation, etc. is required?
    - Who is responsible for each step in the process? How are they monitored and reviewed?

Obtain and review the company's financial statements for as many time periods back as possible. Was the company's financial deterioration slow and steady or sudden and drastic? Was it unexpected or was it obvious and easy to forecast? What happened to sales, inventory, gross margins, accounts receivable, and cash flow? Are the impacts on all of these items consistent and concerted or are there unexpected divergences? Is the information in the financial statements consistent with what can be observed in walk-throughs of the facilities and conversations with management and key employees, customers, and vendors?

Understand that a single financial statement, by itself, is virtually meaningless for all but the most limited purposes. Financial statements impart meaning only when they are viewed in context of what the numbers represent, the trends and relationships of the numbers to each other and to non-numerical variables, the detail underlying the numbers, and the key factors that drive the numbers that ultimately appear on the financial statements. For example, a single cash flow statement by itself doesn't say much, and a single income statement by itself doesn't say much, but when you have both of them together and they don't correlate, that starts saying a lot more to you. When you have four or five sets

of statements and it is clear that there is not the correlation between cash flow and net income that you would expect, now you have a strong indication that there may have been fraud going on. Some of the first indications of the Madoff fraud (which the SEC ignored) came from this type of analysis, where the number of transactions implied by the financial statements could not possibly have occurred given the size and capability of the company and the markets it operated in.

Financial statements are numbers, and numbers are subject to fabrication or manipulation. Financial statement fraud usually intends to increase the apparent net assets or prosperity of the company. Analysts of financial statements use vertical analysis (analyzing relationships between items within a single statement), horizontal analysis (analyzing changes from one set of statements to another) and ratio analysis (comparing different components of the statements to each other). The more savvy the fraudster, the more he or she will ensure that the analysis does not easily disclose what is really going on. Again, it cannot be stressed enough that analysis of just the financial statements is often not sufficient to find fraud – the message that the financial statements is conveying needs to be checked for consistency with other messages being observed in the company, its market, its peers and competition, and the economy. It is in these inconsistencies that the fraud is often first brought to light.

Every trustee and financial investigator knows to safeguard the accounting records, their supporting documents, and the company's computer system as quickly and thoroughly as possible. What they often overlook is other electronic stores of data – cell phones, flash drives, PDA's, CD's / DVD's, printers, credit card readers, digital cameras, music playing devices such as iPods, and GPS systems. These are all increasingly able to store large amounts of data. When they are analyzed by a competent investigator they can provide clues of people called, places visited, transactions made, undisclosed accounts, or even pictures of crimes being committed. Nothing can be ruled out as a source of data – there have been cases, for example, where stolen goods were found by reviewing places visited on a fraudster's GPS system and where deleted documents were recovered from the memory of a common laser printer. Few people know that most mass-market printers embed a unique code onto each document they print, and this can be used to establish the origin of forged or fraud-related documents.

Be aware that very detailed internal control checklists and questionnaires are commercially available for virtually every area of accounting and business operations. The above set of questions and items is a starting point towards assessing the risk and likelihood of fraud. Once a theory of the fraud has been established, the investigator can narrow down the areas requiring review and focus in much more intently on the parts of the company that have been identified as sensitive. At that point, a more detailed investigation that is beyond the scope of this chapter to describe may be warranted.

Types of Fraud, Symptoms, and Methods of Detection

Fraud has been broken down into different types and categories. The names and categories are generally accepted, but are not absolute – for example, "embezzlement" can cover many of the other types of fraud that are more narrowly defined. Observed symptoms can initially point to multiple types

of fraud – for example, declining gross margins may be indicative of inventory fraud, accounts receivable fraud, disbursement fraud, or skimming.

I've put together a series of charts that show the various types of possible fraud that may have occurred at a debtor, the symptoms that those types of fraud typically exhibit, the usual methods used to detect those types of fraud, and the documents needed to perform those detection methods. Since fraudsters are creative and every situation is somewhat unique, these are not absolute. They do, however, help in determining what information is needed to start a more focused investigation. The first chart shows various types of fraud and the type of scheme they are usually classified as:

	Asset Misappropriation							Management Fraud				
	Skimming	**Embezzlement**	**Accounts Receivable**	**Inventory**	**Fixed Assets**	**Disbursements**	**Payroll**	**Financial Statements**	**Bankruptcy Reporting**	**Bust-outs**	**Fraudulent Transfers**	
Types of Fraud												
Theft of cash	x	x							x			
Theft of sales taxes		x				x						
Theft of payroll taxes		x					x					
Theft of benefit withholdings		x					x					
"Cash back" deposits		x										
False voids, credits, or returns		x										
Unauthorized Credits, discounts, write-offs			x									
Lapping			x									
Unauthorized shipments			x									
Theft of inventory or scrap material				x					x			
Purchasing fraud				x						x		
Selling below company prices				x								
Return fraud				x								
Theft of fixed assets					x							
Unauthorized use of assets					x							
Payments to unauthorized parties						x						
Kickbacks, inflated costs						x						
Duplicate payments						x						
Contract fraud						x						
Ghost employees							x					
False payroll checks							x					
Concealment of assets or transfer of assets for less than equivalent value								x	x	x	x	
Intent to defraud creditors								x	x	x		
Concealed assets or liabilities								x	x			
Personal expenses paid by company								x	x			
Misaplied accounting rules or principles								x				
Fictitious or sham transactions								x				
Overstatement of assets or revenues								x				
Reserve manipulation, earnings management								x				

As expected, different types of fraud exhibit different symptoms. The next chart correlates various symptoms that could be observed in a bankrupt company with the types of fraud that those symptoms usually indicate.

	Asset Misappropriation								Management Fraud			
	Skimming	**Embezzlement**	**Accounts Receivable**	**Inventory**	**Fixed Assets**	**Disbursements**	**Payroll**		**Financial Statements**	**Bankruptcy Reporting**	**Bust-outs**	**Fraudulent Transfers**
Symptoms of Fraud												
Employee Tips	x	x	x	x	x	x	x		x	x	x	
Lifestyle changes in potential perpetrators	x	x	x	x	x	x	x		x	x	x	x
Missing or altered documents or records	x	x	x	x	x	x	x		x	x		x
Gross Profit or inventory anomolies	x	x		x						x		
Management under pressure - financing, tax, divorce, investment, lifestyle, etc.	x	x							x	x	x	x
Irregularities involving customers or transactions for which there is no record	x	x								x		
Changes in cash receipts patterns	x									x		
Lack of normal cash shortages (too much perfection)	x									x		
Ratio of cash to other payment types is low	x									x		
Transactions not consistent with the company or industry's business		x	x	x	x	x	x	x	x	x	x	x
Unusual accounting entries		x	x	x	x	x				x		
Too many bank accounts in relation to business needs		x	x			x			x			x
Write-offs on new accounts, repeat accounts, or balances not yet aged		x	x							x		x
Deterioration in accounts receivable aging		x	x							x		
Excessive credit memos or credit / rebills		x	x							x		
Discrepancies in deposits		x	x							x		
Unusual entries in customer master file		x	x							x		
High number of short-pays		x	x							x		
Increases in reported customer complaints		x	x									
Improper Employee Expense reimbursements		x				x						
Transactions not recorded accurately or timely		x							x	x		x
Large transactions or adjustments at end of accounting period		x							x	x		x
Unusual amount of cash transactions		x							x			x
Check Kiting		x							x			
Bank account does not easily reconcile to books		x								x		
Missing cash		x								x		
Large physical inventory or cycle count adjustments			x	x		x				x		
Decrease in inventory turns				x		x						
Excessive amounts of scrap or obsolete inventory				x		x						
Unusual repairs and maintenance expenses					x	x	x			x		

	Asset Misappropriation							Management Fraud			
	Skimming	**Embezzlement**	**Accounts Receivable**	**Inventory**	**Fixed Assets**	**Disbursements**	**Payroll**	**Financial Statements**	**Bankruptcy Reporting**	**Bust-outs**	**Fraudulent Transfers**
Symptoms of Fraud - continued											
Ficitiious vendors					x	x		x	x		x
Unexplained write-offs of assets					x	x			x		x
Changes in asset usage ratios compared to revenue activity					x	x			x		x
Missing fixed assets					x	x			x		
Changes in capital expenditure activity					x	x					
Improper or unauthorized payments						x	x		x		x
Unusual Payees						x	x		x		x
Higher costs than expected						x	x		x		
Inquiries form taxing authorities						x	x		x		
Duplicate payments						x	x				x
Multiple payees with same address or similar names						x	x				x
Lower quality or unfinished services						x	x				
Unusual expense fluctuations						x	x				
Unusual check endorsements or bank accounts used						x	x				
Altered or missing cancelled checks						x	x				
Payee in records different from payee on check						x	x				
Increased purchases from certain vendors						x			x	x	x
Complaints from vendors not used by the debtor						x			x		
Excess goods						x				x	
Vendor complaints						x					
Handwritten checks in a computerized environment						x					
Unusual fluctuations in payroll costs							x		x		
Out of cycle payroll checks							x		x		
Employee complaints							x		x		
Unusual withholdings on paychecks							x				
Employee turnover higher or lower than expected							x				
Excessive related party transactions								x	x	x	x
Earnings that are too smooth or do not reflect the economy								x	x		
Held checks								x			
Ambiguity in timing of revenue recognition								x			
Misstating investment values								x			
Miscosted inventory								x			
Improper capitalization								x			
Unusual growth or profitability								x			
Financial and operating performance significantly different from industry norms								x			
Use of too many different banks or professionals								x			
Sudden and rapid selling at deep discounts										x	x
New ownership of an established reputation										x	
Sudden increases in asset purchases										x	

The third chart indicates what detection methods would typically be used in looking for each of the indicated types of fraud.

	Asset Misappropriation							Management Fraud			
Detection Methods	**Skimming**	**Embezzlement**	**Accounts Receivable**	**Inventory**	**Fixed Assets**	**Disbursements**	**Payroll**	**Financial Statements**	**Bankruptcy Reporting**	**Bust-outs**	**Fraudulent Transfers**
Time-line chronology	x	x	x	x	x	x	x	x	x	x	x
Talk with employees, former employees.	x	x	x	x	x	x	x	x	x	x	x
Data analysis - filtering, sorting, indexing, aging, statistics, gaps	x	x	x	x		x	x	x	x		
Stastical sampling techniques	x	x	x	x		x	x	x			
Talk with other outside parties - landlords, tenants, bankers, ex-	x	x		x	x	x		x			
Review inventory shrinkage, inventory usage history	x					x		x	x	x	x
Review gross profit trends over time	x					x		x	x	x	
Analytical review of sales and cash history over time	x							x	x	x	
Compare sales recorded to shipment documentation	x							x			x
Compare customer shipments and complaints to sales records	x										
Review organization chart and job functions		x	x	x	x	x	x	x	x		
Scan general ledger postings		x	x	x	x	x	x	x	x		x
Scan files of supporting documents		x	x	x	x	x	x	x	x		x
Link Analysis		x	x	x		x	x		x		
Proof of Cash worksheet		x	x			x	x	x	x	x	
Review transfers between bank accounts		x	x			x		x			
Talk with customers		x	x					x	x	x	
Compare deposits to payment postings		x	x						x		
Analytical review of customer complaint trends		x	x								
Bank account reconciliations		x				x	x	x	x		
Rollforward of accounts receivable balances			x						x		

	Asset Misappropriation							Management Fraud			
	Skimming	Embezzlement	Accounts Receivable	Inventory	Fixed Assets	Disbursements	Payroll	Financial Statements	Bankruptcy Reporting	Bust-outs	Fraudulent Transfers
Detection Methods - continued											
Review credits and write-offs			x						x		x
Match documents for shipments, invoices, credits			x								
Analysis of accounts receivable trends			x								
Compare insurance records to accounting rec ords				x	x			x			x
Inventory usage or turnover analysis				x		x		x	x	x	
Review accounting entries in inventory and COGS accounts				x		x		x	x		x
Sales trend analysis				x				x	x	x	
Physical inventory counts				x				x	x		
Verify fixed asset existance					x	x		x	x		x
Review accounting entries in asset accounts					x	x		x	x		x
Analyze asset usage					x	x					x
Compare cancelled checks to accounting records						x	x		x		x
Review endorsements on cancelled checks						x	x		x		x
Review overall disbursement statistics						x	x		x		x
Review expense trends						x	x		x		x
Review vendor statements						x		x	x	x	
Talk with vendors						x		x	x		x
Review invoices for services, intangibles						x		x	x		x
Review contracts and bids						x				x	x
Review vendor master file						x					
Review payments by amount - under approval limits, round						x					x
Verify existance of employees							x		x		x
Review changes to payroll master file							x				x
Understand general industry conditions								x	x	x	
Compare financial statements to tax returns								x	x		
Understand revenue recognition policies								x			
Review investment documents, confirm key terms and assumptions								x			

The next chart details out the documents needed to investigate each of the various suspected fraud categories.

	Asset Misappropriation							Management Fraud			
	Skimming	**Embezzlement**	**Accounts Receivable**	**Inventory**	**Fixed Assets**	**Disbursements**	**Payroll**	**Financial Statements**	**Bankruptcy Reporting**	**Bust-outs**	**Fraudulent Transfers**
Documents or Files Needed											
Organization chart with duties outlined	x	x	x	x	x	x	x	x	x	x	
Shipping records (fedex, UPS, in-house delivery, etc)	x		x						x		x
Hostorical financial and operating reports of the company	x							x	x	x	
Physical inventory reconciliatons, cycle count adjustments	x							x			
Account reconciliations		x	x	x	x	x	x	x	x		
Documents that support transactios as per company's internal controls		x	x	x	x	x	x	x	x		x
Company general journal or access to journal entries		x	x	x	x	x	x	x	x		x
Original documents - credits, refunds, voids		x	x		x						x
Bank statements		x				x	x	x	x		
Statements of bank accounts previously closed		x						x	x		
Sales invoices, price list (if applicable)		x									x
Accounts receivable transaction detail			x								
Credit and collection files			x								
Customer master file			x								
Insurance policies - property, liability, workers comp, etc.				x	x		x	x	x		x
Shipping logs and documentation				x				x	x		
Physical inventory or cycle count worksheets				x				x			
Original documents - invoices, credits, refunds, voids				x				x			
Fixed asset records					x			x			x
Asset usage logs					x						
Cancelled checks						x	x	x	x		x
Vendor statements						x		x	x	x	x
Original documents - invoices from vendors						x		x	x		x
Contracts and bids						x		x		x	x
Check registers, accounts payable detail						x			x		x
Vendor master file						x					
Payroll system records and reports							x		x		x
Personnel files							x				
Tax returns - income, sales, payroll, property								x	x		
Investment documents								x			

The last chart shows various examples of financial analysis and how the financial statements can be used to detect or at least highlight some of the fraud categories for further investigation.

	Asset Misappropriation						Management Fraud			
	Skimming	**Embezzlement**	**Accounts Receivable**	**Inventory**	**Fixed Assets**	**Disbursements**	**Payroll**	**Financial Statements**	**Bankruptcy Reporting**	**Bust-outs**	**Fraudulent Transfers**
Key Financial Statistics											
Horizontal analysis - trend over time		x	x	x	x	x	x	x	x	x	
Vertical analysis - relationships between different items within a time period		x	x	x	x	x	x	x	x	x	
Ratio analysis		x	x	x	x	x	x	x	x	x	
Comparison to industry norms		x	x	x	x	x	x	x	x	x	
Actual performance vs budget or projections		x	x	x	x	x	x	x	x		
Compare sales to operating expenses		x	x	x				x	x	x	
Accounts Receivable Aging		x	x					x	x		
Average collection periods		x	x					x	x		
Receivables turnover		x	x					x	x		
Days Receivables Outstanding		x	x					x	x		
Inventory Aging		x		x		x		x	x	x	
Gross Margin Trends		x		x		x		x	x	x	
Inventory turnover trends		x		x		x		x	x	x	
Asset Utilization reports		x			x	x		x	x		
Trends in expenses		x				x	x	x	x		

Putting it all together

While the wide range of different types of fraud, different symptoms of fraud, and different detection methods can be daunting, the initial approaches to known or suspected fraud can actually be boiled down quite simply:

1. Quickly secure as many documents, electronic components, and other evidentiary material as possible. Documents from outside parties – bank statements, vendor statements, cancelled checks, contracts, etc. are useful to confirm or dispute what is in the company records. Material that was company generated – accounting records, financial statements, etc. is useful to track company activity and highlight inconsistencies if they exist. Electronic items could still have useful information in memory. If in doubt, don't throw it out.
2. Talk to as many people who are knowledgeable about the company as possible and notice any patterns that emerge in the information you obtain. Information regarding relationships between various parties (both people and business entities), lifestyle issues, and unusual changes is of particular interest.
3. Obtain an understanding of the company's business, its environment, the stresses and pressures it was under, how it operated, what types of controls it had in place, and the management tone. Know enough to be able to evaluate the company's financial statement in the context of what should be expected to be on them.
4. Understand how cash and other assets flow through the company and who has access to them at each of the sensitive points.

5. Perform an initial cursory review of the accounting detail. Become familiar with the general ledger and journal entries. Ascertain what documentary support exists for them. Trace some of this detail from the accounting system directly through to the financial statements to verify that the financial statements do have adequate support behind them (I have seen cases where the financial statements and bankruptcy reports were pure fiction with almost no relationship to the underlying accounting detail that should have supported them).
6. Perform financial analysis as outlined in the chart above to help focus in on potential problem areas.
7. Determine how best to use the company's computer data – check for numerical sequence of recorded transactions; analyze sales by product, location, or employee; review deposit and customer activity; review out of sequence (numerical or date) transactions; review accounting activity; find duplicate or unusual transactions; etc. There are a number of programs available for analytical review and other data-mining functions.
8. There are detailed check lists and work programs available for assessing internal controls and for investigating each of the fraud types discussed above. A good investigator will rely on these as well as on his or her intuition, experience, and background.

How to make "dumb luck" happen

One of the biggest frustrations for beginning students of accounting is the requirement that debits have to equal credits. Another way of expressing "debits equal credits" is Newton's third law of motion; "To every action there is an equal and opposite reaction." The implications of this in a fraud investigation are enormous. Most fraudsters are good at what they do. They are creative and they understand the environment they are operating in better than anyone else does. A significant percentage of cases I've investigated were defrauded for sport, to exercise the fraudster's creativity, and for the challenge of doing it well more than they were for actual financial need. Very often, the fraud will be well concealed. That is where 'debits equal credits" come in.

Unless the fraudster is skimming cash, running a bust-out scheme, or submitting purely fictional statements that bear no relationship to the underlying detail, their activity will need to be disguised with accounting entries. Either a debit or a credit will be made to disguise or conceal what needed to be hidden. The problem that most fraudsters have is this "other side" of the entry, where to hide the offset. Phony disbursements, for example, will manifest themselves in the offsetting areas, usually overstated expenses, inventory shrinkage, or lower gross margins. This is similar to an old fashioned 1970's-vintage water bed – wherever you press down, a part of the structure pops up somewhere else.

Fraudsters are usually more concerned with concealing the evil half of the entry than they are with the other half, and the "plug" half of the entry is usually left dangling out there for the knowledgeable investigator to find. In the beginning of this chapter I noted the ACFE's finding that the second most cited method of fraud detection was "dumb luck". I prefer to think that a lot of that is actually investigator intuition, that after observing and absorbing as much as possible about the subject company, the experienced investigator latches on to a nagging feeling that something doesn't make

sense, something doesn't fit the expected patterns, or something that you would expect to see is missing. Fraudsters with accounting knowledge will often focus too much on the accounting mechanics and end up posting entries that don't make sense in the general business context. Being relentless in identifying and resolving that one piece of the puzzle is very often what brings frauds to light.