THE IMPACT AND REALITY OF FRAUD AUDITING
LOCATING SHELL COMPANIES IN ACCOUNTS PAYABLE

A fraud audit is a proven way to identify fraud. Locating and recognizing shell companies in your accounts payable file is a critical task for today’s fraud auditor. The process starts with effective data mining designed to locate favored vendors, false billing, and pass-through fraud schemes. The fraud audit procedures will focus on proven techniques to determine if the vendor is a shell corporation using the physical existence, legal existence, and the business capacity audit program. The presentation will illustrate the concepts with real-life scenarios.

LEONARD VONA, CFE, CPA
President
Fraud Auditing, Inc.
Valatia, New York

Leonard W. Vona is a financial investigator with more than 30 years of diversified auditing and forensic accounting experience, including a distinguished 18-year private industry career. His firm advises clients in areas of litigation support, financial investigations, and fraud prevention.


Mr. Vona has successfully conducted more than 100 financial investigations for some of the largest high-profile corporations in the United States. He has saved clients millions of dollars through recovery or defense strategies. Financial investigation experience includes embezzlement, economic damage, asset theft, bribery, intellectual property, and disbursement schemes. Mr. Vona’s trial experience is extensive, and he is qualified as an expert witness as a CPA and a CFE.

Mr. Vona lectures nationally and internationally on fraud risk assessments, fraud investigation, fraud prevention and detection, and fraud schemes perpetrated on companies. He has provided more than 1,000 days of fraud training to organizations around the world. In addition, he was on the faculty of the National Association of Fraud Examiners from 1995–2000 and in 2001 for the Lally School of Management at Rensselaer Polytechnic Institute.
Mr. Vona graduated from Siena College with honors, receiving a Bachelor of Business Administration in Accounting. He is a licensed Certified Public Accountant and a Certified Fraud Examiner.

Mr. Vona is a member of the American Institute of Certified Public Accountants, the National Association of Certified Fraud Examiners, and the Institute of Internal Auditors. He was the 1994 President of the NY Capital Chapter of the Association of Government Accountants and the founding President of the Albany Chapter of Certified Fraud Examiners.
### Introduction
Shell companies are often associated with fraud. Although they are legal entities that do have a legitimate function in business operations, shell companies are also used by criminals to facilitate fraudulent activities. Such activities include money laundering, billing schemes, fictitious service schemes, bankruptcy fraud, tax evasion, and market manipulation. Scandals involve anywhere from thousands to millions of dollars. While shell companies are frequently linked to multiple forms of scams, law officials are unable to prosecute all cases because state agencies do not collect enough ownership information on company formation documents. Thus, they leave no paper trail for the government to trace back to a particular individual or individuals.

### Definition
A shell company is a legal entity that has no active business and usually exists only in name as a vehicle for another company’s business operations. In essence, shells are corporations that exist mainly on paper, have no physical presence, employ no one, and produce nothing. Within more sophisticated schemes, the perpetrators might employ the use of an office or employees to provide the illusion of a legitimate business entity. They are frequently used to shield identities and/or to hide money in cases of money laundering, bankruptcy, bribery, and fraudulent conveyances. Within this paper, we will focus on how shell corporations are used to commit internal fraud schemes through the disbursement or revenue cycle. The focal points will be:

- Understanding the inherent fraud scheme approach
- Sophistication of concealment strategies
- Data mining techniques to locate shell corporations
- Fraud audit procedures to identify the shell corporation
Inherent Scheme Structure
All inherent schemes have two aspects: the entity structure and the fraudulent action. The first step is building the fraud scenarios within the audit scope. The second is building the audit response to the identified fraud scenarios. Our fraud audit approach generally starts with the entity structure and then focuses on the action component of the fraud scenario.

Entity Structure
Fraud scenarios involving vendors, customers, and employees tend to use a false entity structure to commit the fraudulent activity. Within each category, there will be permutations that will affect the fraud auditing testing procedures. The most common false entities are:

- The entity was created by the perpetrator, vendors, or customers. Vendors and customers are either legally created or exist in name only. When the entity exists in name only, the entity verification procedures will detect the false entity. For legally created entities, the fraud auditing testing procedure should link the incorporation date to first business date. As a guide, when the entity incorporation date is within 90 days of first business transaction date, that is a red flag of a false entity or a favored entity.

- The perpetrator assumes the identity of a real entity such as a vendor, customer, or employee. Therefore, the address or telephone number within the company master file for the entity should not match the address or telephone number of the entity verification procedures. A caveat exists in the pass-through fraud scheme where one of the perpetrators is employed at the real source of the goods or services, so it is possible to obtain a match of records.
LOCATING SHELL COMPANIES IN ACCOUNTS PAYABLE

**Real Entities**
When the entity is determined to be a real entity, there are generally three possible outcomes:
- Favorite entity status indicates the entity is real, but there might be a real or perceived conflict. If there is a conflict, the fraud scenario would be dependent on the nature of the account, or else there is no fraud scenario occurring.
- The fraud scenario links to a real entity, whereby a decision tree would aid in the determination of the type of scenarios occurring.
- No fraud scenario is occurring. When the entity is established as a real entity, a decision tree can direct the auditor to the inherent scheme structure for the applicable core business system.

**Fraudulent Action**
From a fraud audit perspective, we will focus on shell-company schemes used to commit internal embezzlement.
- False Billing: The payment for goods or services not delivered or provided.
- Pass Through: The payment for goods or services that are provided. In this scheme, a real vendor provides goods or services to a shell company, which in turn provides the goods or services to your organization with a markup on price (the only function the front company provides is a pass through of the goods or services). There are three variations caused by the employment location of the perpetrator. The scheme can be committed solely by an internal employee, an internal employee in collusion with a sales person from the real supplier, or directed by a customer involving cost reimbursable contracts.
Fraud Concealment Impact on Locating Shell Corporations

Fraud concealment involves the strategies used by the perpetrator of the fraud scenario to conceal the true intent of the transaction. Common concealment strategies are: false documents, false representations, false approvals, avoiding or circumventing control levels, internal control inhibitors, blocking the access to information, geographic distance between documents and controls, and both real and perceived pressure. An important aspect of fraud concealment pertains to the level of sophistication used by the perpetrator.

Inherent fraud schemes aren’t thought of in terms of complexity; rather, it is the level of sophistication used to conceal the fraud that is the focus for the fraud auditor. On its most simplistic level, without a concealment strategy, the inherent fraud scheme would be visible. The analogy that comes to mind is that of a baseball pitcher who has one pitch: a fastball with no movement. Everyone in the park knows what he is going to throw, including the batter, who will consequently probably hit it out.

Fraud concealment sophistication should be rated on both the perpetrator’s ability to hide the transaction (our pitcher having several pitches besides that fastball) and the auditor’s ability to detect the transaction (the batter being able to correctly figure out what pitch is coming). To aid in the determination of a level of sophistication applicable to a concealment strategy, a rating scale of low, medium, and high is used.

There is a correlation between fraud detection and the sophistication of the concealment strategy. When the perpetrator’s concealment strategy is more sophisticated than the audit methodology, the fraud goes undetected.
However, in addition to audit methodology, the auditor has the fraud detection tool of awareness. Fraud is revealed when the audit detection is as sophisticated as the concealment strategy, thereby resulting in a directly proportional relationship as shown on the illustration.

**Fraud Audit Plan: Detection of Shell Companies**

The process of detecting shell corporations is a two-step process. The first step is the data mining, which is designed to locate vendors that are consistent with the data profile of a shell corporation or transactions that are indicative of a shell corporation. The second step is performing audit procedures, which are designed to pierce the concealment strategy or reveal the truth. The data mining strategy is a two-fold process. The first step is to understand the impact the sophistication of the concealment strategy has on the data mining process. The second step is building the data profile for the fraud scenario.

**Data Mining Strategy**

There is a direct correlation between the degree of sophistication of the concealment strategy and the number of transactions meeting the data profile requirements. Highly sophisticated concealment strategies tend to have a larger number of transactions required, whereas data mining routines that search for direct matches use a smaller number of transactions. The characteristics of the relationship between the number of fraudulent transactions and the sophistication level of the concealment strategy are listed below:

- Low sophistication of concealment
  - Direct matches of the fraudulent entity structure to another entity structure.
LOCATING SHELL COMPANIES IN ACCOUNTS PAYABLE

- Entity identifying information links to the perpetrator’s known identifying information; for example, a specific street address.
- Fraudulent activity is linked to one or a few entity structures.
- Data mining routine searches key on data matching.
- Overall sample size is determined by the number of transactions that match the data profile; the sample size can range from zero to a large number.

• Medium sophistication of concealment
  - Direct matching routines are less effective. Data interpretation skills are more crucial.
  - Filtering techniques like drill-down analysis are effective in reducing the number of transactions fitting the data profile, thus allowing data interpretation to be more effective.
  - Entity identifying information relates to some aspect of the perpetrator’s known identifying information; for example, a zip code location versus a physical street address.
  - Sample selection relies on data interpretation skills and scenario-specific data mining routines.
  - Sample size tends to be judgmentally determined versus the use of all transactions meeting the matching criteria.

• High sophistication concealment
  - Direct matches seldom occur.
  - Fraudulent activity might be linked to multiple entities or smaller-dollar transactions.
  - Entity identifying information has no relationship with the perpetrator’s known identifying information.
### Locating Shell Companies in Accounts Payable

- Entity identifying information might relate to a mailbox service or an out-of-area address that has a mail-back feature.
- Sample selection relies on data interpretation skills.
- The population for deriving a sample is larger because the selection criterion identifies all transactions in a group versus a specific transaction.
- Sample size tends to be judgmentally determined versus the use of all transactions meeting the matching criteria.

### Building the Data Profile

There are no absolutes; however, there is a lot of hard work. In the previous section, we describe the impact of the concealment sophistication model on the data mining plan. In this section, we will describe the type of considerations we will make in building our fraud data profile.

- **Name:** Shell companies often have non-descriptive names. One search method is to look for names with a limited number of constants. Obviously, this variable will be affected based on where in the world the search is performed. In the United States, we use five constants. We strip out the “Inc.,” spaces, vowels, or special symbols and then count the alpha string.

- **Mailing Address:** There are two approaches: First, search for known mailbox services. Second, strip out all alpha, spaces and special symbols and search for duplicate numeric strings in the vendor database or between payroll and vendor databases. In searching for duplicate numeric strings the zip code field should be linked to street number to minimize false positives.
<table>
<thead>
<tr>
<th>LOCATING SHELL COMPANIES IN ACCOUNTS PAYABLE</th>
</tr>
</thead>
</table>

- **Country, City, State and Postal Code:** One belief is that the shell corporation would be within a radius of the corporation or within the state to avoid crossing state OR country lines. We believe this is more likely with low to medium sophistication perpetrators than high sophistication ones.

- **Telephone Number:** Shell corporations often use mobile lines when no physical office exists. Also, when searching for pass through fraud schemes, a duplicate telephone number search is an effective tool, especially when the pass through is associated with an existing supplier.

- **Create Date:** The ACFE annual study provided statistics regarding the duration that fraud schemes occur without detection. The creation date can be used to filter out vendors less likely to be shell corporations. Second, we search for a correlation between first invoice date and the creation date.

- **Bank Routing Number:** Payments are transferred either by wire or address. The routing number can be used to correlate to prospective individuals. The theory is simple; the perpetrator is smart enough not to use his personal bank account, but would use the same bank for his shell corporation bank account.

- **Bank Account Number:** The search is for duplicate bank account numbers in the master file or between payroll and vendor master file.

- **Vendor Invoice Number:** The invoice number pattern is one the most critical data fields for our data mining plan. The reason is simple: the perpetrator creates the number. The pattern and frequency analysis is critical in the search for false billing schemes. The low sophistication scheme will most likely have a sequential pattern of invoice numbers. For the pass through scheme, the invoice
number pattern will depend on whether the pass through entity has one or a few customers.

- **Vendor Invoice Date:** We search for unusual patterns within the date—i.e., all dates are weekend dates, all dates are the same day of the week, or all days have the same number day.

- **Vendor Invoice Amount:** Correlates to the management position of the perpetrator, the individual’s personal risk tolerance, control levels, and whether the scheme is a false billing scheme or a pass through billing scheme.

**Entity Verification Procedures**

The four entity verification procedures are: physical presence, legal creation, business capacity testing, and reference checking. The first step in entity verification is to determine that the control procedures were adhered to in recording the entity into the business system. Identification of the names associated with establishing an entity structure is needed to be performed for comparison purposes in future fraud audit procedures. The intent is not control testing, but the gathering of information to establish a basis for entity verification.

The order of verification is: testing legal existence, verifying physical existence, testing business capacity, and reference checking. The first three procedures can generally be performed in a covert manner; however, reference checking tends to be overt, and so the procedure is generally performed last.

**Verify Legal Existence**

- All entities have a legal government registration. Employees have birth records and corporations have registration requirements with an applicable
government office. The first step is to establish whether the entity is legally created, and then gather identifying information that can eventually be linked to other pertinent information. Names of registrars; officers’ addresses; and dates related to entity creation, dissolutions, or changes tend to be the critical information gathered.

- Customers and vendors that are not incorporated might have filed a DBA certificate. The lack of a DBA certificate is typically a red flag. Such a certificate can provide the name of a small business owner, although it is not uncommon for small business owners not to file a certificate.
- Small businesses might not be registered in the state matching the address. While small businesses are required to file as a foreign corporation doing business in the state matching the address, not all small business owners are savvy enough about these requirements, especially in regard to their tax descriptive information. Therefore, a national-level search for legal registrations might be required.
- When an entity is a member of a trade association, a business’s membership provides evidence that the entity is a real one. This verification might also be a useful test for incorporated business. One reason small business owners join a trade association is the opportunity to purchase insurance in a group plan. It should be noted that the absence of membership should not be considered as evidence of a false entity.
- Use Internet search companies, such as Lexus Nexus, which gathers public record information that is made accessible to clients. A search of a company on Lexus Nexus can find out if any public records exist on the company and what type of records they are.
**LOCATING SHELL COMPANIES IN ACCOUNTS PAYABLE**

*Verify Physical Existence*
- Telephone Verification: By contacting the entity, you verify physical existence by the mere fact of the call being answered. Then it becomes a question of how the call is answered. How the call is answered is part of the evidence associated with the audit judgment of whether the entity is real or false. By calling, the possible outcomes are: the telephone is disconnected; someone answers in the name of a different entity; or someone answers in the name of the entity in question. Interview skills are the critical skill to ensure the success of the procedure.

Here a few practical tips:
- Use a telephone in the area code of the company you are auditing. Area codes from out of the area might create a suspicion about why you are calling.
- Be prepared to provide an explanation as to why you are calling. Possible explanations are updating records, resolving internal problems, or trying to find original documents that have been misplaced. Try not to raise suspicion at this stage of the audit.
- Have the documents readily available to ask questions or provide answers.
- Avoid calling multiple times; a second telephone call raises suspicions.
- Remember that the entity you are calling might have Caller ID. Therefore, do not indicate that you are someone other than the person associated with the number identified.
- The manner in which a call is answered must be consistent with the anticipated business size. Does their business volume correlate with the audited company usage?
LOCATING SHELL COMPANIES IN ACCOUNTS PAYABLE

- Internet search engines, like Google, can determine what physical structure is located at the known address, and whether the address is consistent with the entity structure. Often, the created entity scheme will use a personal residence address. Remember that many small businesses operate from the owner’s personal residence, so, in this case, reference checking might be preferred in order to reveal that the entity does not conduct business.

- By visiting the site, it can be determined what physical structure is located at the known address, and whether the address is consistent with the entity structure. Private detectives often will perform the procedure for a nominal charge, so the use of one might be useful for verifying entities that are not located in your geographic area.

- Public records can determine whether a government or business recognizes the entity as a real entity and if the address is recognized by other entities. A legal instrument filed by banks securing a loan indicates that the bank believes the entity is real.

- The IRS website can provide federal identification verification, which will determine whether the federal identification number or Social Security number matches the name associated with the ID number. In many parts of the world, corporations will have a VAT number, which can be confirmed with a government ministry.

- The Internet has extensive databases and search engines to gather information. At the simplest level, Google is an excellent starting point. At the advanced level, there are research companies that have made an art of navigating the Internet.
## Locating Shell Companies in Accounts Payable

### Business Capacity Test
- **Proof of Insurance:** Real companies tend to have insurance. For example, companies with employees have workers’ compensation insurance. The fraud testing procedure would consist of a request of the certificate of insurance. Fortunately, such a request is a normal control procedure in many companies, but for fraud audit purposes, the need is to examine the certificate to take note of the date of coverage and types of coverage.
- **Employees:** A company telephone directory provides evidence that the company has employees. By calling the company, you are often referred to the company telephone directory when you do not know an employee’s extension.
- **UCC Filings:** A public record filed by a bank or a financing company can indicate a lien has been filed against the described asset. It also indicates that the bank recognizes the entity as a real one.
- **Shipping documents:** Such as a billing of lading indicates the source of the shipment, therefore providing verification.
- **Websites:** If a company has a website, does such a site provide matching information about the businesses and services offered?

### Reference Checking
- **Professional Associations:** Is the entity recognized by a trade association? Such organizations can also provide useful information on trade practice and trends, which in turn can be used to corroborate representations made by individuals.
- **Competitors:** Contact competitors to establish that the entity conducts business consistent with the goods and services described on the invoice.
LOCATING SHELL COMPANIES IN ACCOUNTS PAYABLE

Competitors may also provide other information regarding ownership and business conflicts.

- Media searches: Information published regarding the entity might provide names, services, and legal actions regarding it. Advertisements by the entity would suggest the existence of the entity and describe the type of services provided by it.

Red Flags Defined

A fraud red flag is an observable event that links to a fraud concealment strategy that is associated with a fraud scenario. Red flags are used by management to build fraud detection controls and by the auditor in the context of conducting an audit as an alert to the possibility of fraudulent activity.

For the red flag to be an effective audit tool, the event must be observable and must be incorporated into the fraud audit program. Red flags by their nature cause an increased sensitivity to the likelihood of a fraud scenario occurring. Not all red flags have the same weight with regard to fraud susceptibility. The weight of a fraud red flag correlates to the predictability of a fraud occurrence. Therefore, the auditor needs to interpret the importance of the red flag to the fraud scenario and be able to arrive at a conclusion regarding the occurrence of the fraud scenario.

There are four categories of red flags: data, documents, internal controls, and behavior. The categories are intended to aid the auditor in identifying the red flags in an orderly fashion, whereb, the auditor should not view the process as a right or wrong exercise, but instead know that certain items can occur in multiple categories. For example, a vendor invoice number can be a data category red flag observed through the use of data mining or a document...
category red flag observed through the application of audit testing procedures.

In addition to the four categories of red flags already mentioned, there are also two other types of red flags: trigger red flags and awareness red flags. With the trigger red flag, the event is sufficient enough to require the auditor to perform fraud audit procedures to determine if credible evidence exists to suggest that the fraud scenario is occurring. As a guideline, there should be no more than five trigger red flags per category, and preferably only three trigger red flags per category. To the contrary, with awareness red flags, the event is not sufficient to require the auditor to perform fraud audit procedures. However, the totality of all the awareness red flags will require an auditor’s judgment on the need to perform fraud audit procedures. While both might lead to the performance of fraud audit procedures, the underlying reasons differ. As a guideline for internal control audits, a red flag that links to a fraud scenario via a key control is denoted as a trigger red flag, whereas, a red flag that links to a fraud scenario via non-key controls is denoted as an awareness red flag. A trigger red flag is similar to the traditional audit use of red flags, whereby when an internal control is not working, it “triggers” a red flag. The use of trigger and awareness red flags will change in fraud audits or specific point analysis, whereas the link is directly associated with concealment strategy and the elements of the fraud scenario.

**Shell Corporation Red Flags**
The fraud auditor should use the entity verification procedures as the basis for building the red flag approach. Within disbursement fraud schemes, the address and the bank account are key fields for building the trigger red flags. Within the transactional testing, focusing on the
vendor invoice number as to patterns or frequency would serve as the trigger red flags.

**Conclusion**

It has been our experience that shell corporations exist in most large corporations. The number of shell corporations and the dollar magnitude is uncertain. We believe that the dollar magnitude of the average false billing scheme is below $500,000, unless committed by a senior executive. The dollar magnitude of a pass through scheme will be in the millions. Fraud auditing is an effective methodology to uncover the shell corporation that is lurking in your databases.