Principles of Fraud Examination, Ch. 4

**Billing Schemes**

**Learning Objectives**

After studying this chapter, you should be able to:

List the five major categories of fraudulent disbursements

Define billing schemes

List the three categories of billing schemes

Understand what a shell company is, and how it is formed

List and understand the four ways false invoices are approved for payment

Understand why most shell company schemes involve the purchase of services rather than goods

Understand how a pass-through scheme differs from the usual shell company schemes

Be familiar with the methods identified in this chapter for preventing and detecting shell company schemes

Understand how pay-and-return schemes work

Understand how non-accomplice vendor schemes work

Be familiar with the methods identified in this chapter for preventing and detecting non-accomplice vendor schemes

Understand how personal purchases schemes work

Be familiar with the methods identified in this chapter for preventing and detecting personal purchases schemes

Be familiar with proactive audit tests that can be used to detect billing schemes

Exhibit 4-1



**Case Study:** **Medical School Treats Fraud and Abuse 1**

1Several names and details have been changed to preserve anonymity.

Fraud seemed to plague a certain Southeastern medical college, with one bad case erupting after another. One supervisor’s minor transgression opened a Pandora’s box of fraud perpetrated by his assistant. It all began when Bruce Livingstone, a married supervisor at the college’s three-person business office, took his girlfriend on a business trip using school funds drawn from a suspense account (a temporary account in which entries of credits or charges are made until their proper disposition can be determined). Livingstone did not submit an expense report to offset the charges that month, a violation of a policy governing the college’s extensive travel budget.

Once officials realized that employees had grown lax about submitting timely expense reports, they attempted to reconcile the suspense account by requiring employees to settle their own accounts before receiving their paychecks. Not wanting his indiscretion revealed, Livingstone had to disguise the additional expense of taking his girlfriend on a business trip. He submitted a phony expense report in which he unwisely named a female senior auditor at the college as his traveling partner. He forged the auditor’s signature on a letter that stated she had participated.

As luck would have it, the unsuspecting auditor herself reviewed the bogus report. She was quite surprised to find she’d taken a trip with Livingstone. She immediately informed Harold Dore, the director of internal audit for the institution, of the forgery. Dore alerted others.

Following a short interview with college officials, Livingstone admitted his wrongdoing and was promptly terminated. The executive vice president authorized Dore to conduct a full fraud examination. As they were soon to find out, they had not seen the worst of it yet. Livingstone’s amorous business trip was just the tip of the iceberg.

“Whenever there’s fraud found here,” said Dore, “I automatically conduct what I call a ‘magnitude investigation.’” He has learned that perpetrators rarely limit themselves to the fraud initially uncovered: “Chances are, they did something else.”

As part of the information-gathering portion of his investigation, Dore decided to interview Cheryl Brown, the 30-year-old administrative assistant who had worked under Livingstone for three years. The interview was to be conducted with the dean of the dental school president, so Dore headed across campus toward the business office.

But Brown left before Dore arrived. She told coworkers that her uncle had been shot and that she had to depart for California immediately. In her haste to get away, she even left her paycheck behind.

Taking that as a sign, Dore immediately sealed the empty office Brown and Livingstone shared and began searching its contents. The search uncovered bags of expensive dental tools and prostheses, which it turned out he had been illegally selling to dental students for years.

Knowing vendor kickbacks are common—and since one of the main functions of the business office was to process invoices submitted by vendors—Dore started by reviewing the master file. The list had never been purged and contained tens of thousands of names—all the vendors who had ever supplied goods and services as part of the college’s annual budget of $55 million. He selected 50 vendors, deliberately choosing those without a phone number or street address.

Then Dore took his list to the next stop in the payment process, the accounts payable department. After methodically pulling all corresponding documentation, he quickly focused on one vendor: Armstrong Supply Company. It regularly billed two or three times a month for strange items named but unknown by Dore, and always for amounts under $4,500, thus eliminating the necessity of two authorized signatures. All of the request-for-funds forms attached to the invoices either bore the signature of Livingstone or the dean of the dental school. Furthermore, Dore could find no vendor application on file for Armstrong Supply. He also failed to find any competitive bidding process in place.

“Once I looked at the actual invoices, that really got me going,” said the fraud examiner. Some carried invoice numbers; others did not, but they did carry a four-digit post office box number. (Subsequent research revealed that postal authorities had switched to five-digit and six-digit PO boxes years earlier.) Billed items included such things as “3 dozen TPM pins” (the identity of which baffled even the long-time stockroom manager).

“The invoices just smelled fake,” said Dore, who packs more than 20 years of auditing experience. What’s more, he later found blank invoices for Armstrong Supply in one of Brown’s desk drawers. He even noticed one completed invoice that had been readied for submission. (Apparently, Brown left in too much of a hurry to dispose of the smoking gun.)

Based on those questionable invoices, the accounts payable department would issue a check for the stated amount. On the request-for-funds forms attached, Brown always indicated that she would personally present the check to Armstrong Supply. (Due to lax controls, vendors and employees were allowed to pick up checks.) Canceled checks revealed that a man named Claude Armstrong III cashed them at various check-cashing services, which sometimes called Cheryl Brown for additional verification, as noted on the backs of the checks.

Further research showed yet another scam, according to Dore. The office mail contained a department store gift card with a note from a vendor to Brown, thanking her for her recent business. The California vendor had billed the college for roughly $42,000 worth of copy machine cartridges—running $4,500 apiece—and Brown had processed the invoices. After a fruitless search for this valuable cache in the school’s storerooms and copy centers, Dore called local dealers and discovered that their most expensive cartridge cost only $483. Under his direction, private investigators located the vendor’s “corporate headquarters” in a rental unit at a retail postal center, but the college abandoned their long-distance pursuit of recovery when it proved too costly.

Although Dore tried to keep his three-month-long investigation quiet, the campus buzzed with news of his activities. Brown’s many friends, including two in the accounts payable department, kept her abreast of his movements.

Next he pulled in Livingstone for a chat about the new evidence supporting vendor fraud and kickbacks, as well as his backroom sale of orthodontic supplies. According to Dore, it became apparent during the interview that the philanderer knew nothing about the vendor schemes. Brown had perpetrated the $63,000 vendor fraud without Livingstone’s help. He seemed quite taken aback that it had occurred under his nose by someone he trusted so much. In some cases, Brown had forged the signatures of her supervisor and the dean of the dental school. In others, the unwitting bosses actually signed the bogus forms.

At the same time the Livingstone interview was being conducted, the school’s general counsel received a call from Brown’s lawyer. “He asked if we had ever given leniency to an errant employee in the past, if he were to admit to everything,” said Dore. Once the general counsel deemed it a possibility, they scheduled a meeting for September. It was to be attended by both attorneys, Dore, the executive vice president of the college, and Brown, who had never returned to work since her hasty departure. Her lawyer also relayed her request to bring along a friend as a character witness, a nurse for whom she had once worked and who could attest to the good nature of this unmarried mother supporting three small children.

Brown was quiet and cooperative at the meeting. Dore took her through his voluminous file folder on Armstrong Supply, the sham company she had created. She willingly identified each and every document that detailed her duplicity, which had begun five months after her hire. Dire cash emergencies prompted the first few deceptions, she said. As Brown realized how easy it was in light of the weak controls, her confidence grew and she stepped up her thefts with no signs of stopping. “It became addictive, in her words,” recalled Dore.

To illustrate her need, she explained that her husband had developed a drug and alcohol problem and that she had been dragged into drug abuse as well. She claimed that after she had become addicted, her husband abandoned her and the small children. She then broke down and cried, the first of many times during the interview. Brown went on to point out that she was seeing a doctor for her addictive behavior. When Dore asked how long she had been seeing her doctor, “She said her first visit was going to be next week.” (Months later, a casual conversation between Dore and a coworker who had once dated Brown raised doubts about her excuses. “He swore she never touched drugs or alcohol,” said Dore.)

She said her accomplice, Claude Armstrong III, was a friend with a history of drug abuse. (Background checks showed an arrest and conviction on drug charges for Armstrong; Brown had no prior arrests or convictions, and her references proved favorable.) She also admitted that her cover story about the uncle in California was fabricated.

After Brown expressed remorse over the fake invoices, Dore asked her about her relationship with the phony cartridge supply firm. She totally disavowed any knowledge of that scam. She insisted that the invoices were legitimate and the cartridges were stacked in a storeroom. (Note: No one has found the cartridges to date.)

Even without owning up to the recent $42,000 cartridge scam, Brown seemed surprised to learn that her Armstrong Supply fraud had netted $63,000 over two years.

Given the small percentage of the annual budget that was pilfered, college officials were not surprised that the fraud went undetected by the Big Four firm that served as their external auditor. Their contract stated that “audit tests are not all-inclusive and not designed to find fraud,” a disclaimer that auditors rely on to absolve them from possible culpability. “If they were that detailed, nobody could afford an external audit,” said Dore, also a certified internal auditor.

Looking back, he saw that some good stemmed from the frauds. Since then, the college has instituted much stronger controls and makes sure to enforce them. Dore said tales of his dogged investigation enhanced respect for the audit function, “[a]nd probably instilled a bit of fear among the 4,500 employees, because the college officials did pursue a criminal prosecution against Brown.”

During the course of her trial, the district attorney informed Dore that his testimony was not needed, even though it would have shown hell-bent intent on the part of the defendant. With her lawyer acting on her behalf, Brown struck a deal with the prosecutor. She was placed on probation and ordered to pay partial restitution. (Brown was found three-fourths culpable and Armstrong one-fourth. Because half of the stolen funds came from federal grants, $30,000 was charged off to the federal granting authority.)

As part of the deal, Brown was also sentenced to six months’ house arrest—with exceptions granted for her to attend work and church.

**Overview**

In Chapter 2, we saw that the vast majority of asset misappropriations target cash, as opposed to noncash assets. We also saw that cash misappropriations are subdivided into three categories in the fraud tree: *skimming, cash larceny*, and *fraudulent disbursements*. Skimming and cash larceny have already been covered, so we will now turn our attention in the next five chapters to fraudulent disbursement schemes. There are five major categories of fraudulent disbursement in the fraud tree:

* Billing schemes
* Check tampering
* Payroll schemes
* Expense reimbursement schemes
* Register disbursement schemes

The first category of fraudulent disbursements to be covered is billing schemes. These may be loosely defined as schemes in which a fraudster causes the victim organization to issue a fraudulent payment by submitting invoices for fictitious goods or services, inflated invoices, or invoices for personal purchases. As the data from ACFE research shows, billing schemes are among the most costly, and the most common, forms of occupational fraud.

**Billing Scheme Data from the ACFE *2009 Global Fraud Survey***

Among the fraudulent disbursement categories, billing schemes were most commonly reported in the *2009 Global Fraud Survey* (see Exhibit 4-2). Of 921 reported fraudulent disbursement cases, 52 percent involved billing fraud. Billing schemes were also the second most costly form of fraudulent disbursement, with a reported median loss of $128,000 (see Exhibit 4-3).

Exhibit 4-2 *2009 Global Fraud Survey*: Frequency of Fraudulent Disbursements a



aThe sum of these percentages exceeds 100 percent because some cases involved multiple fraud schemes that fell into more than one category

Exhibit 4-3 *2009 Global Fraud Survey*: Median Loss of Fraudulent Disbursements



**Billing Schemes**

In a billing scheme, the perpetrator uses false documentation—such as an invoice, purchase order, credit card or purchasing card bill, and so on—to cause his employer to issue a payment for some fraudulent purpose. The actual disbursement of funds is performed by the organization in the same manner as would be a legitimate disbursement. The crux of the fraud is not that a bogus payment is issued; instead, the key to these schemes is that the fraudster is able to deceive his employer so that the organization willingly and unwittingly issues the bogus payment.

Billing schemes generally fall into one of three categories:

* Shell company schemes
* Non-accomplice vendor schemes
* Personal purchases schemes

***Shell Company* Schemes**

Shell companies, for the purposes of our discussion, are fictitious entities created for the sole purpose of committing fraud. As we saw in the case study at the beginning of this chapter, they may be nothing more than a fabricated name and a post office box that an employee uses to collect disbursements from false billings. However, since the payments received will be payable to the shell company, the perpetrator will normally also set up a bank account in his new company’s name, listing himself as an authorized signer on the account (see Exhibit 4-4).

Exhibit 4-4 False Billings from Shell Companies



**Forming a Shell Company**

In order to open a bank account for a shell company, a fraudster will probably have to present the bank with a certificate of incorporation or an assumed-name certificate. These are documents that a company must obtain through a state or local government. These documents can be forged, but it is more likely that the perpetrator will simply file the requisite paperwork and obtain legitimate documents from his state or county. This can usually be accomplished for a small fee, the cost of which can be more than offset by a successful fraud scheme.

If it is discovered that a company is being falsely billed by a vendor, fraud examiners for the victim company may try to trace the ownership of the vendor. The documents used to start a bank account in a shell company’s name can sometimes assist examiners in determining who is behind the fraudulent billings. If the corrupt employee formed his shell company under his own name, a search of public records at the local court house may reveal the person as the fraudster.

For this reason, the corrupt employee will sometimes form his shell company in the name of someone other than himself. For example, in Case 4737, an employee stole approximately $4 million from his company via false billings submitted from a shell company set up in his wife’s name. Using a spouse’s name adds a buffer of security to an employee’s fraud scheme. When a male employee sets up a shell company, he sometimes does so in his wife’s maiden name to further distance himself from the fictitious company.

A more effective way for a fraudster to hide his connection to a false company is to form the company under a fictitious name. In Case 4455 an employee used a coworker’s identification to form a shell vendor. The fraudster then proceeded to bill his employer for approximately $20,000 in false services. The resulting checks were deposited in the account of the shell company, and currency was withdrawn from the account through an ATM.

The other issue involved in forming a shell company is the entity’s address—the place where fraudulent checks will be collected. Often, an employee rents a post office box and lists it as the mailing address of his shell company. Some employees list their home address instead. In Case 4434, a department head set up a dummy company using his residence as the mailing address. Over a two-year period, this man submitted over $250,000 worth of false invoices. Eventually, the scheme was detected by a newly hired clerk. The clerk was processing an invoice when she noticed that the address of the vendor was the same as her boss’s address. (By a lucky coincidence, the clerk had typed a personal letter for her boss earlier that day and remembered his address.) Had the department head used a post office box instead of his home address on the invoices, his scheme might have continued indefinitely.

One reason employees might be hesitant to use post office boxes in shell company schemes is that some businesses are especially wary of sending checks to vendors that do not have street addresses. Such an address, as we have already discussed, can signal fraud. For this reason, fraudsters may use the address of a relative, friend, or accomplice as a collection point for fraudulent checks.

**Submitting False Invoices**

Once a shell company is formed and a bank account has been opened, the corrupt employee is in a position to begin billing his employer. Invoices can be manufactured by various means such as a professional printer or a personal computer. As we saw in the case study at the beginning of this chapter, false invoices do not always have to be of professional quality to generate fraudulent disbursements. The phony invoices Cheryl Brown used to bill from Armstrong Supply Company “just smelled fake,” according to Harold Dore, yet they were sufficient to generate checks.

**Self-Approval of Fraudulent Invoices**

The difficulty in a shell-company scheme is not usually in producing the invoices, but in getting the victim company to pay them. Authorization for the fictitious purchase (and therefore payment of the bill) is the key. In a large percentage of the shell company cases in the ACFE studies, the fraudster was in a position to approve payment on the very invoices he was fraudulently submitting. In Case 446, for example, a manager authorized payment of $6 million worth of phony invoices from a dummy company he had formed. Similarly, an employee in Case 982 set up a bogus freight company and personally approved $50,000 worth of bogus invoices from it. It is only logical that those with authority to approve purchases would be among the most likely to engage in billing schemes, since they have fewer hurdles to overcome than other employees.

A slight twist to this method was used in Case 4542. The victim organization in this case properly required vouchers to be prepared and approved by different persons. The fraudster in this case had approval authority, but was not allowed to prepare the vouchers that he approved. Therefore, this person created false vouchers and forged a coworker’s initials as the preparer. Then the perpetrator approved the voucher for payment under his own authority. It therefore appeared that two employees had signed off on the voucher, as mandated by the organization’s controls.

Not all companies require the completion of payment vouchers before they will issue payments. In some enterprises, payments are issued based on less formal procedures. In Case 4436, for example, the CEO of a nonprofit company simply submitted “check requests” to the accounting department. As the CEO, his “requests” obviously carried great weight in the organization. The company issued checks to whatever company was listed on the request in whatever amount was specified. The CEO used these forms to obtain over $35,000 in payments for fictitious services rendered by a shell company he had formed. In this case, invoices were not even required to authorize the payments. The check request forms simply listed the payee, the amount, and a brief narrative regarding the reason for the check. This made it so easy for the CEO to generate fraudulent disbursements that he eventually had three separate companies billing the victim company at the same time. It is obvious that, as CEO, the fraudster in this case had a wide degree of latitude within the company and was unlikely to be obstructed by one of his subordinates. Nevertheless, this case should illustrate how the failure to require proper support for payments can lead to fraud.

**“Rubber Stamp” Supervisors**

If an employee cannot authorize payments himself, the next best thing is if the person who has that authority is inattentive or overly trusting. “Rubber stamp” supervisors like this are destined to be targeted by unethical employees. In Case 4759, for example, an employee set up a fake computer supply company with an accomplice and “sold” parts and services to his employer. The perpetrator’s supervisor did not know much about computers and therefore could not accurately gauge whether the invoices from the dummy company were excessive—or even necessary. The supervisor was therefore forced to rely on the perpetrator of the scheme to verify the authenticity of the purchases. Consequently, the victim company suffered approximately $20,000 in losses.

**Reliance on False Documents**

When an employee does not have approval authority for purchases and does not have the benefit of a rubber stamp supervisor, he must run vouchers through the normal accounts payable process. The success of this kind of scheme will depend on the apparent authenticity of the false voucher he creates. If the fraudster can generate purchase orders and receiving reports that corroborate the information on the fraudulent invoice from his shell company, he can fool accounts payable into issuing a payment.

***Collusion***

Collusion among several employees is sometimes used to overcome well-designed internal controls of a victim company. For example, in a company with proper separation of duties, the functions of purchasing goods or services, authorizing the purchase, receiving the goods or services, and making the payment to the vendor should be separated. Obviously, if this process is strictly adhered to, it will be extremely difficult for any single employee to commit a false-billing scheme. As a result, the ACFE studies included several schemes in which employees conspired to defeat the fraud prevention measures of their employer. In Case 444, for example, a warehouse foreman and a parts-ordering clerk conspired to purchase approximately $300,000 of nonexistent supplies. The parts-ordering clerk initiated the false transactions by obtaining approval to place orders for parts he claimed were needed. The orders were then sent to a vendor who, acting in conjunction with the two employee fraudsters, prepared false invoices that were sent to the victim company. Meanwhile, the warehouse foreman verified receipt of the fictitious shipments of incoming supplies. The perpetrators were therefore able to compile complete vouchers for the fraudulent purchases without overstepping their normal duties. Similarly, in Case 4099, three employees set up a shell company to bill their employer for services and supplies. The first employee, a clerk, was in charge of ordering parts and services. The second employee, a purchasing agent, helped authorize these orders by falsifying purchasing reports regarding comparison pricing, and so on. The clerk was also responsible for receiving the parts and services; a third conspirator, a manager in the victim company’s accounts payable department, ensured that payments were issued on the fraudulent invoices.

The cases above illustrate how collusion among several employees with separate duties in the purchasing process can be very difficult to detect. Even if all controls are followed, at some point a company must rely on its employees to be honest. One of the purposes of separating duties is to prevent any one person from having too much control over a particular business function; it provides a built-in monitoring mechanism whereby every person’s actions are in some way verified by another person. But if everyone is corrupt, even proper controls can be overcome.

**Purchases of Services Rather Than Goods**

Most of the shell company schemes in our survey involved the purchase of services rather than goods. Why is this so? The primary reason is that services are not tangible. If an employee sets up a shell company to make fictitious sales of goods to his employer, these goods will obviously never arrive. By comparing its purchases to its inventory levels, the victim company might detect the fraud. It is much more difficult, however, for the victim company to verify that the services were never rendered. For this reason, many employees involved in shell company schemes bill their employers for things like “consulting services.”

***Pass-through Schemes***

In the schemes discussed so far, the victim companies were billed for completely fictitious goods or services. This is the most common formula for a shell company fraud, but there is a subcategory of shell company schemes in which actual goods or services are sold to the victim company. These are known as pass-through schemes.

Pass-through schemes are usually undertaken by employees in charge of purchasing on behalf of the victim company. Instead of buying merchandise directly from a vendor, the employee sets up a shell company and purchases the merchandise through that fictitious entity. He then resells the merchandise to his employer from the shell company at an inflated price, thereby making an unauthorized profit on the transaction.

One of the best examples of a pass-through scheme in the ACFE studies came from Case 4763, in which a department director was in charge of purchasing computer equipment. Because of his expertise on the subject and his high standing within the company, he was unsupervised in this task. The director set up a shell company in another state and bought used computers through the shell company, then turned around and sold them to his employer at a greatly exaggerated price. The money from the victim company’s first installment on the computers was used to pay the shell company’s debts to the real vendors. Subsequent payments were profits for the bogus company. The scheme cost the victim company over $4 million.

**Preventing and Detecting Shell Company Schemes**

Because shell company schemes are among the most costly of all forms of occupational fraud, it is imperative that organizations have controls in place to prevent these frauds. As is the case with all forms of billing fraud, it is critical that duties in the purchasing process be separated. Most billing schemes succeed when an individual has control over one or more aspects of purchasing, authorizing purchases, receiving and storing goods, and issuing payments. If these duties are strictly segregated, it will be very difficult for an employee to commit most forms of billing fraud, including shell company schemes.

Because shell company schemes, by definition, involve invoicing from fictitious vendors, one of the best ways to counter this type of fraud is to maintain and regularly update an approved vendor list. The legitimacy of all vendors on the list should be verified by someone independent of the purchasing function, and whenever an invoice is received from a vendor not on the list, independent verification of that company should be required before the invoice is paid.

**Identifying Shell Company Invoices**

In addition to controls aimed at generally preventing billing fraud, auditors, accounting personnel, and other employees should be trained to identify fraudulent invoices. One common red flag is a lack of detail on the fraudulent invoice. For example, the invoice might lack a phone number, fax number, invoice number, or tax identification number, or other information that usually appears on legitimate invoices. Another common sign of fraud is an invoice that lacks detailed descriptions of the items for which the victim organization is being billed. Finally, the mailing address on an invoice can indicate that it is fraudulent. In most shell company schemes, the mailing address for payments is a mail drop or a residential address. Any invoice that calls for a payment to one of these locations should be scrutinized, and the existence of the vendor should be verified before a check is mailed.

In some cases, a fraudster will print or create several invoices and then submit them to his employer one at a time over an extended period so that the amount he is stealing will be spread out, making it less noticeable. These schemes can sometimes be detected because the invoices used by the perpetrator will be consecutively numbered. In other words, the invoice numbers might be 4002, 4003, 4004, and so forth. This is clearly a sign of a shell company, because it indicates that the vendor in question is only sending invoices to the victim. Suppose, for example, that an organization receives invoice #4002 from a vendor on September 1, and receives invoice #4003 on October 1. This would indicate that the vendor issued only a single invoice in September—the invoice received by the company in question. Obviously, a legitimate company could not operate this way and survive.

Organizations can detect this sort of anomaly by regularly reviewing the payables account and sorting payments by vendor and invoice number. Also, in many shell company schemes the perpetrator will repeatedly bill for identical or similar amounts. If the perpetrator has purchase authority, these amounts will tend to be just below the perpetrator’s approval limit. So if Employee X is committing a shell company scheme and is authorized to approve purchases up to $10,000, his shell company invoices might tend to fall in the $9,000 to $9,999 range. This can be detected by sorting payments by vendor and amount.

**Testing for Shell Company Schemes**

As discussed above, sorting payments by vendor, amount, and invoice number is one way to search out red flags that might indicate a shell company scheme. There are a number of other trends and red flags that are frequently associated with these frauds, and organizations should regularly test for them as part of a proactive fraud detection program.

Billing schemes will typically cause an organization’s expenses to exceed budget projections, so organizations should be alert to large budget overruns, and to departments that regularly exceed their budgets. Billing schemes will also tend to cause an increase in expenses from previous years. In a small company a billing scheme could significantly affect the financial statements and could be detected through horizontal analysis (comparison of financials on a year-to-year basis). In a very large company, a billing scheme might not have a significant impact on the overall financials, but it could still be detected by analyzing expense trends on a departmental or project basis. Obviously, by fraudulently increasing purchasing expenses, billing schemes will also tend to cause an increase in cost of goods sold relative to sales, and therefore will tend to negatively impact profits.

Because billing schemes generally involve the purchase of fictitious goods or services, a review of purchase levels can help detect this form of fraud. As we have stated, most shell company schemes involve purchases of fictitious services, since these “soft account” items cannot be traced to inventory, leaving no physical evidence that the transaction was fraudulent. However, these schemes will cause an increase in service-related expenses. So, for instance, a large, unexplained rise in consulting or training expenses could indicate a shell company scheme. When this red flag shows up, the underlying purchases should be reviewed, and both the performance of the service and the legitimacy of the provider should be confirmed. By tracking approval authority for all purchases, organizations can also run comparison reports looking for employees or managers who approve an unusually high level of services based on their job function.

In cases where a shell company bills for goods, these goods either will be nonexistent or will be overpriced as part of a pass-through scheme. In either case, this will cause expenses and cost of goods sold to rise, as discussed above. Furthermore, if an individual causes his organization to buy nonexistent goods, that means the quantity of items purchased will increase by the number of fictitious items bought from the shell company. Unexplained increases in the quantity of goods purchased should be investigated, particularly when the increase does not translate to increased sales. Purchases of nonexistent goods will also cause inventory shortages, because the purchased items will be added to the organization’s perpetual inventory system but will never enter the physical inventory. Purchases that cannot be traced to inventory are a clear red flag of shell company schemes.

Alternatively, if the shell company sells existing goods as part of a pass-through scheme, then the price for these items will be substantially marked up. Organizations should monitor trends in average unit price of goods purchased. Significant increases could signal not only pass-through schemes, but also kickback schemes and other types of billing fraud. If prices on a particular transaction or set of transactions seem out of line, other vendors should be contacted to determine the industry norm. Assuming the pricing is way out of line, the organization should review the transaction to determine how the vendor was approved, and what employees were involved in the transaction. In addition, steps should be taken to confirm that the vendor is legitimate, as discussed below.

In addition to reviewing *quantities* purchased, organizations should also pay attention to *types* of goods and services that are purchased. In many shell company schemes and other forms of billing fraud, the nature of the purchases is patently unreasonable, but the invoices in question are nevertheless rubber-stamped. For instance, when a law firm buys a truckload of gravel, red flags should immediately go up. This kind of test is really an issue of common sense, and it requires that auditors, managers, and accounting personnel have a good understanding of how their organizations function.

Because employees sometimes run shell company schemes using their home address to collect payments, organizations should periodically run comparison reports for vendor addresses and employee addresses. If a match occurs, the employee in question is probably engaging in a shell company scheme.

Fraudulent vouchers are also generally run through the payables system more quickly than legitimate ones. The employees who commit these schemes try to get their bogus invoices paid as quickly as possible, both because they want their money immediately and because once the invoice gets paid the likelihood of the scheme being detected drops considerably. A report showing the average turnaround time on invoices sorted by vendor might show that a particular company tends to have its invoices paid much more quickly than other vendors. If so, steps should be taken to confirm that the company exists, and that the purchases were appropriate.

**Verifying Whether a Shell Company Exists**

It is usually fairly simple to determine whether a particular vendor is legitimate. A good first step is to simply look up the vendor in the phone book. The absence of a phone number for a vendor is generally an indication that the company is a shell. It is also a good idea to contact others in your industry to determine whether they are familiar with the vendor. If the vendor only appears to have billed your company, or if no one else in your community seems to have heard of it, the company may not actually exist. Finally, if questions persist about whether the vendor is a shell, someone from the victim organization should verify the vendor’s address through a personal visit or using satellite imaging software.

**Identifying the Employee behind a Shell Company**

Even when a company has been identified as a shell, there is still the matter of determining who is behind the scheme. In most cases, the perpetrator will have been involved in selecting the vendor or approving the purchase. However it may be necessary to gather independent verification to prove the identity of the fraudster. This can make it easier to obtain a confession during an investigative interview, and it will also serve as useful evidence if the matter eventually goes to trial—a possibility that exists in any fraud investigation. There are a number of ways to verify the identity of the person or persons operating a shell company.

In many cases the person who creates a shell company will register the company with the appropriate government authority, because such registration is necessary to open a bank account in the shell’s name. These documents require the name, address, and signature of the person who is forming the company. Therefore, a search of the company’s registration, which is a matter of public record, may indicate who committed the fraud. Articles of incorporation are maintained by the secretary of state (or the state corporation bureau or corporate registry office) in every state. DBA (Doing Business As) information can usually be obtained at the county level. These public records can be obtained without a subpoena.

When conducting a records search, it is important to remember that fraudsters might set up a company under a false name to avoid being identified with the shell. One common technique is to establish the shell in the name of a relative or accomplice who does not work for the victim organization. If the perpetrator is male and is married, he might also form the shell under his wife’s maiden name. When checking public records, investigators should be alert for related names, as well as addresses, phone numbers, Social Security numbers, or other identifiers that may match an employee’s personnel information.

Rather than conduct a records search, it may be possible to confirm the identity of the fraudster based on other factors. For instance, a company could compare checks that have been converted by the shell company with information from the suspect’s payroll checks or direct deposits. Matching account numbers or signatures would indicate that the payments were deposited into the same bank account. Similarly, handwriting samples on business filings or communications from the suspected vendor can be matched against the handwriting of suspected employees.

Another way to identify the perpetrator behind a shell company scheme is to conduct surveillance of the mail drop to determine who collects checks on behalf of the shell company. Finally, if a suspect or suspects have been identified, a search of their office or workspace might also reveal trash. Many shell company schemes are detected when a vendor’s invoices or letterhead are discovered in an employee’s work area. However, any workplace search must be done carefully, ensuring that the employee’s privacy rights are not violated. Workplace searches should be conducted only after consulting with an attorney.

**Billing Schemes Involving Non-Accomplice Vendors**

***Pay-and-Return Schemes***

Rather than use shell companies as vessels for overbilling schemes, some employees generate fraudulent disbursements by using the invoices of non-accomplice vendors. In pay-and-return schemes, these employees do not prepare and submit the vendor’s invoices; rather, they intentionally mishandle payments that are owed to the legitimate vendors (see Exhibit 4-5). One way to do this is to purposely double-pay an invoice. In Case 4020, for instance, a secretary was responsible for opening mail, processing claims, and authorizing payments. She intentionally paid some bills twice, then requested the recipients to return one of the checks. She would intercept these returned checks and deposit them into her own bank account.

Exhibit 4-5 Pay-and-Return Schemes



Another way to accomplish a pay-and-return scheme is to intentionally pay the wrong vendor. In Case 756, an accounts payable clerk deliberately put vendor checks in the wrong envelopes. After they had been mailed, she called the vendors to explain the “mistake,” and requested that they return the checks to her. She deposited these checks in her personal bank account and ran the vouchers through the accounts payable system a second time to pay the appropriate vendors.

Finally, an employee might pay the proper vendor, but intentionally overpay him. In Case 2649, an employee intentionally caused a check to be issued to a vendor for more than the invoice amount, then requested that the vendor return the excess. This money was taken by the fraudster and deposited into her own account. Similarly, an employee might intentionally purchase excess merchandise, return the excess, and pocket the refund.

**Overbilling with a Non-Accomplice Vendor’s Invoices**

In some cases employees use invoices in the name of existing vendors to generate fraudulent payments. This occurs in kickback schemes when the vendor is an accomplice in the fraud, but it can also occur when the vendor is unaware of the crime. The perpetrator either manufactures a fake invoice for a vendor who regularly deals with the victim organization or reruns an invoice that has already been paid. The perpetrator submits the fraudulent invoice and intercepts the resulting payment. Since the bill is fictitious, the existing vendor is not out any money. The only victim is the employer’s organization, which pays for goods or services that it does not receive. In the following case study, Albert Miano took a copy of a contractor’s invoice, replicated it, and used the phony invoices to bill his employer for over a million dollars’ worth of false work. CFE Terence McGrane put a stop to Miano’s scheme.

**Case Study:** **Cover Story: Internal Fraud 2**

2Several names and details have been changed to preserve anonymity.

Sometimes fraud is discovered by chance instead of deliberate effort. In the $4 million embezzlement fraud by an employee of a magazine publisher, more than one coincidence brought down the perpetrator.

A popular magazine and large direct-mail publishing house decided to outsource much of its direct-mail operations to specialized mail vendors. The company began converting its plant in Pleasantville, New York, from a direct-mail-order factory to an office complex. Part of the office complex construction involved building an auditorium that was to be identical to another auditorium in historic Williamsburg, Virginia. Terrence McGrane had just begun his third day on the job as chief internal auditor. In an effort to get to know his new company, he had scheduled a series of interviews with all the vice presidents. His first interview was with the vice president of administrative services, Harold J. Scott, who was in charge of many construction projects and maintenance services. Because of the massive renovation project, it was not unusual for hundreds of invoices to be forwarded to Scott.

Coincidence one: McGrane stopped by the accounts payable department and retrieved a series of recently submitted invoices for various trade expenses related to the auditorium construction project. “One of the things I wanted to accomplish was to understand how the accounting codes worked—what was capitalized; what was expensed; how it was recorded, etc.” So he grabbed a stack of processed invoices with accounting codes and went up to the construction site to meet with the vice president for an hour-long interview.

As the two walked around the grounds, McGrane asked the vice president if he could explain the accounting codes to him: “He stared at the [top] invoice for approximately 30 seconds and said: ‘That is not my signature on the invoice!’

As he looked through the stack, he found what appeared to be about three or four other forgeries. He was completely baffled.”

The initial investigation revealed that all of the forgeries were in the painting division, budgeted at approximately $500,000 a year. The company employed only one person to oversee the painting operations in its facilities department: Albert Miano.

Miano, a 35-year-old from New Fairfield, Connecticut, earned about $30,000 a year. It was his job to coordinate time-and-materials contracts with the scores of painters, carpenters, electricians, and plumbers who toiled daily on the renovation, repair, and construction of the building complex. As facilities supervisor, Miano regularly forwarded invoices to the vice president of administration services for approval.

Miano launched his scheme by crafting false invoices for the jobs done by the painters. He took a copy of a trade invoice from an existing painting contractor and, using his home computer, created a replica into which he would record slightly different hours for the trade contractors’ work.

McGrane related a probable scenario of how Miano executed his scheme. “Let’s say he knew that during the month of February, as an example,” McGrane said, “there were twenty-seven painters on the grounds during the course of one week.” Miano also knew the total number of hours and the volume of materials used in that time. “He would create invoices that were similar in nature, but record only eleven painters on the grounds,” McGrane said. Miano would not reinvoice exactly the same work done during a week, but he would make it look so similar that no one’s suspicions were ever aroused. Effectively, there were no work orders on the “phantom work” he created on these invoices. Miano always listed fewer painters on the false invoice than the actual number who had worked that week, and he registered less time for their services than they had actually worked.

As part of his job, he regularly brought the trade invoices into the administrative VP’s office for signature approval. After delivering a stack of these invoices, he would return to collect them within the next day or two and deliver the approved invoices to the accounts payable department. “It was this opportunity,” McGrane said, “that this individual was allowed to go and collect the approved invoices and insert his own replicated fraudulent invoices as approved. This was the first piece of an ‘electronic circuit’ that allowed him to commit the fraud.” The second piece of the circuit for the fraud to ignite, McGrane said, was allowing this same employee to transport the invoices to the accounts payable department, and ultimately to collect the check.

After seeing how easy it was to slip in his own false invoices in the stack of approved ones, Miano became bolder in his scheme. He began calling accounts payable, claiming that a carpenter or painter had arrived on the grounds and needed his check “immediately.” To keep the project flowing, the employees in the accounts payable department accommodated him. Many employees knew and liked Miano, who had worked for the company for nearly 15 years.

Eventually, this routine became so familiar to employees in accounts payable that Miano did not even need to make up an excuse to pick up checks. Each time he would collect them, he stashed the check for the false invoice in his pocket. When he returned home to New Fairfield, Connecticut, he took the check to his bank, forged the contractor’s name on the back, then endorsed it with his own name and deposited the check.

McGrane explains that Miano was able to pull off the scam due to failure of internal controls and employees not following standard accounting procedures. “For any business transaction, the invoices should be dispatched independently to the approving authority. Once signed, the approved invoices should be sent independently to accounts payable. When the check is prepared by accounts payable, they should mail it directly to the third party. Under a strong internal control system, the employees and/or contractors should not be allowed to come in and collect checks directly. Direct contacts with accounts payable personnel make it too tempting for someone to try to misappropriate funds.”

Accounts payable also failed to combine the invoices into a single check—they wrote a check for each invoice. “Had they combined it,” McGrane said, “his false invoice would have been added into the legitimate painter’s monthly invoice summary, and the money would be mailed to the legitimate contractor,” McGrane said. Accounts payable neglected to study the invoice signatures for forgeries, and the accounting department dropped the ball by not perusing processed checks for dual endorsements, another red flag for potentially misappropriated funds.

Miano’s first transaction totaled $1,200. His second transaction jumped to $6,000—his third, $12,000. His largest single transaction came to over $66,000. Miano refined his strategy by pacing, on a parallel basis, a certain amount below the total due the painter. “If the painter submitted an invoice for $20,000 a month,” McGrane said, “Miano would submit an invoice for, say, $14,000. If the painter submitted a $6,000 invoice, he’d submit one for $3,000.” The individual invoice amounts, because of the continuing construction, would not have alarmed even an auditor.

Miano’s behavior at the office was the same as ever. He dressed the same way, drove the same car to work, and shared little of his private life with other workers. He had not taken a vacation in over four years, and his boss thought he should be promoted (a move Miano resisted, for reasons now obvious). After hours, however, Miano was a different person.

Coincidence two: McGrane’s secretary was not only on Miano’s bowling team, she was also his neighbor. They saw each other regularly at the local bowling alley. She took notice when Miano’s behavior became somewhat extravagant. At first he took to buying the team drinks, a habit most appreciated by his teammates. However, the secretary began wondering where all the money was coming from when he showed up in his new Mercedes (one of five cars he bought) and talked about a new $18,000 boat. He also invested in real estate and purchased a second home costing $416,000.

McGrane’s secretary approached Miano one night after he had spent some $800 on drinks for the team. “Did you win the lottery, or what?” she asked. He explained that his father-in-law had recently died and left a substantial inheritance to his wife and him. Miano’s father-in-law was actually quite alive, but no one ever bothered to check out the claim. No one suspected Miano of doing anything sinister or criminal. All of his associates considered him “too dumb” to carry out such a scheme. One person described him as “dumb as a box of rocks.”

Coincidence three: After four years without a vacation, Miano took what he considered a well-deserved trip to Atlantic City. But he wasn’t there long before he was called back to Pleasantville. One can imagine his chagrin at having to leave the casinos and boardwalks and head back to the office. Little did he know that things were about to get a lot worse.

Upon his return, Miano found himself confronted by the auditor, the vice president, and two attorneys from the district attorney’s office. He readily admitted guilt. “He said he had expected to get caught,” McGrane said. “He did it strictly based on greed. Miano claimed there was no one else involved, and the sum total of his fraud was about $400,000.” But the internal audit found that Miano had forged endorsements on more than fifty checks in those four years, totaling $1,057,000. Ironically, the auditors could only identify about $380,000 spent on tangible items (boats, cars, down payment on a home, etc.). The investigators could not account for the other $700,000, although they knew Miano had withdrawn at least that much from the bank.

Miano served only two years of an eight-year sentence in a state penitentiary. At the time of his indictment, his wife filed for divorce, claiming she knew nothing of her husband’s crimes. Miano told a reporter in jail that the loss of his family and the public humiliation had taught him his lesson.

“For a nickel or for $5 million, it doesn’t pay,” Miano said. “You enjoy the money for a while, but you lose your pride and your self-respect. It ends up hurting your family, and no money can ever change that.”

**Preventing and Detecting Fraudulent Invoices from a Non-Accomplice Vendor**

Prevention of non-accomplice vendor invoicing schemes is largely dependent on the purchasing function controls already discussed in this chapter. Efforts at detecting these schemes should focus on several red flags that are common to non-accomplice vendor invoicing. For example, if an employee produces invoices designed to mimic those of a known vendor, the mailing address or electronic payment information might differ from that of the real vendor. This variation is necessary so that the perpetrator can collect the payment. As discussed previously, organizations should maintain up-to-date approved vendor lists that include contact, mailing, and electronic payment information for approved vendors. Deviations from this information, such as a change in mailing address or electronic payment information, should be flagged, and the changes verified as legitimate before a disbursement is issued. In addition, a fraudulent invoice prepared by an employee to mimic that of a legitimate vendor might have an invoice number that is significantly out of sequence. A sort of disbursements by vendor, date, and invoice number could reveal this type of anomaly.

Instead of producing fraudulent vendor invoices, some employees simply rerun invoices from existing vendors and divert the payments that result from the second run. This type of fraud should be easily detectable if an organization has an effective duplicate checking system to ensure that the same invoice cannot be run through the payables system twice. In manual systems, every paid voucher should be clearly marked “paid” to prevent reprocessing. In an electronic system, duplicate invoice numbers should be automatically flagged. In order to dodge a duplicate checking system, some fraudsters will slightly alter the invoice number. For instance, invoice #44004 might be changed to #44004a, or a zero in the number might be changed to the letter *O* so that the number will look the same to the naked eye but will not show up as a duplicate in the accounting system. However, a sort of invoice numbers from a particular vendor in ascending or descending order will reveal these as out of sequence.

Pay-and-return schemes can be mostly prevented if the duties of purchasing, authorizing, and distributing payments are separated and if all invoices are matched to purchase orders before payments are issued. Incoming mail should also never be delivered directly to an employee. All incoming mail should be opened by mailroom personnel to ensure that every incoming check is recorded. In addition, each incoming check should be photocopied, with the copy attached to the remittance advice. This will help prevent a dishonest employee from being able to recover an amount that was intentionally double-paid.

When the targeted vendor in a pay-and-return scheme returns an overpayment to the fraudster, it is often as a check payable to the victim organization. To make it more difficult to convert such a check, organizations should instruct their banks not to cash checks payable to the organization.

Finally, if a pay-and-return scheme is suspected, organizations should spot-check past accounts payable files for overpayments. Identify all persons involved in processing any overpayment, and review their transactions for similar “mistakes.”

***Personal Purchases* With Company Funds**

Instead of undertaking billing schemes to generate cash, many fraudsters simply purchase personal items with their company’s money. Company accounts are used to buy items for fraudsters, their businesses, their families, and so on. In Case 649, for instance, a supervisor started a company for his son and directed work to the son’s company. In addition to this unethical behavior, the supervisor saw to it that his employer purchased all the materials and supplies necessary for the son’s business. In addition, the supervisor purchased materials through his employer that were used to add a room to his own house. All in all, the perpetrator bought nearly $50,000 worth of supplies and materials for himself using company money.

Conceptually, one might wonder why a purchases fraud is not classified as a theft of inventory or other assets rather than a billing scheme. After all, in purchase schemes the fraudster buys something with company money, then takes the purchased item for himself. In Case 649 discussed in the preceding paragraph, for example, the supervisor took building materials and supplies. How does this differ from those frauds that will be discussed in Chapter 9, whereby employees steal inventory, supplies, and other materials? At first glance, the schemes appear very similar. In fact, the perpetrator of a purchases fraud is stealing inventory just as he would in any other inventory theft scheme. Nevertheless, the heart of the scheme is not the *taking* of the inventory but the *purchasing* of the inventory. In other words, when an employee steals merchandise from a warehouse, he is stealing an asset that the company needs, an asset that it has on hand for a particular reason. The harm to the victim company is not only the cost of the asset, but also the loss of the asset itself. In a purchasing scheme, on the other hand, the asset that is taken is superfluous. The perpetrator causes the victim company to order and pay for an asset that it does not really need, so the only damage to the victim company is the money lost in purchasing the particular item. This is why purchasing schemes are categorized as billing frauds.

**Personal Purchases through False Invoicing**

Most of the employees in our studies who undertook purchases schemes did so by running unsanctioned invoices through the accounts payable system. The fraudster in this type of fraud buys an item and submits the bill to his employer as if it represented a purchase on behalf of the company (see Exhibit 4-6). The goal is to have the company pay the invoice. Obviously, the invoice that the employee submits to his company is not legitimate. The main hurdle for a fraudster to overcome, therefore, is to avoid scrutiny of the invalid invoice and obtain authorization for the bill to be paid.

Exhibit 4-6 Invoice Purchasing Schemes



**The Fraudster as Authorizer of Invoices**

As was the case in the shell company schemes we reviewed, the person who engages in a purchases scheme is often the very person in the company whose duties include *authorizing* purchases. Obviously, proper controls should preclude anyone from approving his own purchases. Such poorly separated functions leave little other than his conscience to dissuade an employee from fraud.

Nevertheless, we saw several examples of organizations in which this lapse in controls existed. As we continue to point out, fraud arises in part because of a perceived opportunity. An employee who sees that no one is reviewing his actions is more likely to turn to fraud than one who knows that his company diligently works to detect employee theft.

An example of how poor controls can lead to fraud was found in Case 888, where a manager of a remote location of a large, publicly traded company was authorized to both order supplies and approve vendor invoices for payment. For over a year, the manager routinely added personal items and supplies for his own business to orders made on behalf of his employer. The orders often included a strange mix of items; technical supplies and home furnishings might, for instance, be purchased in the same order. Because the manager was in a position to approve his own purchases, he could get away with such blatantly obvious frauds. In addition to ordering personal items, the perpetrator changed the delivery address for certain supplies so that they would be delivered directly to his home or side business. This scheme cost the victim company approximately $300,000 in unnecessary purchases. In a similar case, 770, an employee with complete control of purchasing and storing supplies for his department bought approximately $100,000 worth of unnecessary supplies using company funds. The employee authorized both the orders and the payments. The excess supplies were taken to the perpetrator’s home, where he used them to manufacture a product for his own business. It should be obvious from the examples cited above that not only do poor controls pave the way for fraud, a lack of oversight regarding the purchasing function can allow an employee to take huge chunks out of his company’s bottom line.

In some situations, the perpetrator is authorized to approve purchases, but controls prevent him from also initiating purchase requests. This procedure is meant to prevent the kinds of schemes discussed above. Unfortunately, those with authority to approve purchases are often high-level employees with a good deal of control over their subordinates. These persons can use their influence to force subordinates to assist in purchases scheme. In Case 95, for example, purchases under $1,000 at a certain utility company could be made with limited-value purchase orders (LPOs), which required two signatures—the originator of a purchase request and the approver of the request. An LPO attached to an invoice for less than $1,000 would be paid by the accounts payable department. In this case, a manager bought goods and services on company accounts, and prepared LPOs for the purchases. (In some cases, the LPO would falsely describe the item to conceal the nature of the purchase.) Once the LPO was prepared, the manager forced a clerk in his department to sign the document as the originator of the transaction. The clerk, intimidated by her boss, did not question the authenticity of the LPOs. With two signatures affixed, the LPO appeared to be legitimate and the bills were paid. The scheme cost the victim company at least $25,000.

**Falsifying Documents to Obtain Authorization**

Not all fraudsters are free to approve their own purchases; those who cannot must rely on other methods to get their personal bills paid by the company. The chief control document in many vouchers is the purchase order. When an employee wants to buy goods or services, he submits a purchase requisition to a superior. If the purchase requisition is approved, a purchase order is sent to a vendor. A copy of this purchase order, retained in the voucher, tells accounts payable that the transaction has been approved. Later, when an invoice and receiving report corresponding to this purchase order are assembled, accounts payable will issue a check.

So in order to make their purchases appear authentic, some fraudsters generate false purchase orders. In Case 634, for example, an employee forged the signature of a division controller on purchase orders; thus, the purchase orders appeared to be authentic and the employee was able to buy approximately $3,000 worth of goods at his company’s expense. In another instance, Case 434, a part-time employee at an educational institution obtained unused purchase order numbers and used them to order computer equipment under a fictitious name. The employee then intercepted the equipment as it arrived at the school and loaded the items into his car. Eventually, the employee began using fictitious purchase order numbers instead of real ones. The scheme came to light when the perpetrator inadvertently selected the name of a real vendor. After scrutinizing the documents, the school knew that it had been victimized. In the meantime, the employee had bought nearly $8,000 worth of unnecessary equipment.

**Altering Existing Purchase Orders**

Purchase orders can also be altered by employees who seek to obtain merchandise at their employer’s expense. In Case 1334, for example, several individuals conspired to purchase over $2 million worth of materials for their personal use. The ringleader of the scheme was a low-level supervisor who had access to the computer system that controlled the requisition and receipt of materials. This supervisor entered the system and either initiated orders of materials that exceeded the needs of a particular project or altered existing orders to increase the amount of materials being requisitioned. Because the victim organization had poor controls, it did not compare completed work orders on projects to the amount of materials ordered for those projects. This allowed the inflated orders to go undetected. In addition, other employees involved in the scheme were in charge of receiving deliveries. These employees were able to divert the excess materials and falsify receiving reports to conceal the missing items. In addition, the victim institution did not enforce a central delivery point, meaning that employees were allowed to pick up materials from the vendors in their personal vehicles. This made it very easy to misappropriate the excess merchandise. The supervisor’s ability to circumvent controls and initiate false orders or alter genuine ones, though, was the real key to the scheme.

**False Purchase Requisitions**

Another way for an employee to get a false purchase approved is to misrepresent the nature of the purchase. In many companies, those with the power to authorize purchases are not always attentive to their duties. If a trusted subordinate vouches for an acquisition, for instance, busy supervisors often give rubber stamp approval to purchase requisitions. Additionally, employees sometimes misrepresent the nature of the items they are purchasing in order to pass a cursory review by their superiors. For example, in Case 1015, an engineer bought over $30,000 worth of personal items. The engineer dealt directly with vendors and was also in charge of overseeing the receipt of the materials he purchased. He was therefore able to misrepresent the nature of the merchandise he bought, calling it “maintenance items.” Vendor invoices were altered to agree to this description.

Of course, the problem with lying about what one is buying is that when delivery occurs, it is the perpetrator’s personal items that arrive, not the business items listed on the purchase requisition. In the case discussed above, the problem of detection at this stage of the crime was avoided because the engineer who made the fraudulent purchases was also in charge of receiving the merchandise. He could therefore falsify receiving reports to perpetuate the fraud. We have also encountered cases in which fraudsters in the purchasing department enlisted the aid of employees in the receiving department to conceal their crimes.

Another way to avoid detection at the delivery stage is to change the delivery address for purchases. Instead of being shipped to the victim company, the items the employee buys are sent directly to his home or business. In a related scenario, an accounts payable supervisor in Case 592 purchased supplies for her own business by entering vouchers in the accounts payable system of her employer. Checks were cut for the expenses during normal daily check runs. To avoid problems with receiving the unauthorized goods, the perpetrator ordered the supplies from the vendor and had them shipped directly to a client of her side business.

**Personal Purchases on Credit Cards or Other Company Accounts**

Instead of running false invoices through accounts payable, some employees make personal purchases on company credit cards, purchasing cards, or running accounts with vendors. As with invoicing schemes, the key to getting away with a false credit card purchase is avoiding detection. Unlike invoicing schemes, however, prior approval for purchases is not required. An employee with a company credit card or purchasing card can buy an item merely by signing his name (or forging someone else’s) at the time of purchase. Later review of the card statement, however, may detect the fraudulent purchase. In invoicing schemes we saw how those who committed the frauds were often in a position to approve their own purchases. The same is often true in credit card and purchasing card schemes. A manager in Case 446, for example, reviewed and approved his own credit card statements. This allowed him to make fraudulent purchases on the company card for approximately two years.

Of course, only certain employees are authorized to use company credit cards or issued purchase cards. The manager in Case 446 above, for instance, had his own company card. Employees without this privilege can make fraudulent purchases with a company card only if they first manage to get hold of one. To this end, company cards are sometimes stolen or “borrowed” from authorized users. A more novel approach was used by an accountant in Case 1481, who falsely added her name to a list of employees to whom cards were to be issued. She used her card to make fraudulent purchases, but forged the signatures of authorized cardholders to cover her tracks. Since no one knew she even had a company card, she would not be a prime suspect in the fraud even if someone questioned the purchases. For over five years this employee continued her scheme, racking up a six-figure bill on her employer’s account. In addition, she had control of the credit card statement and was able to code her purchases to various expense accounts, thereby further delaying detection of her crime.

An executive secretary in Case 521 used her access to the statement for a different purpose. After making hundreds of thousands of dollars’ worth of fraudulent purchases on corporate cards, this employee destroyed both the receipts from her purchases and the monthly credit card statements. Eventually, duplicate statements were requested from the credit card company, and the fraud was discovered. The fact that no statements were received by the company therefore led to detection of the scheme. Some fraudsters, having destroyed the real copies of credit card statements, produce counterfeit copies on which their fraudulent purchases are omitted. By taking this extra step, the fraudster is able to keep his employer in the dark about the true activity on the account.

**Charge Accounts**

Some companies keep charge accounts with vendors with whom they do regular business. Office supply companies are a good example of this kind of vendor. Purchases on charge accounts may require a signature or other form of authorization from a designated company representative. Obviously, that representative is in a position to buy personal items on the company account. Other employees might do the same by forging the signature of an authorized person at the time of a fraudulent purchase. In some informal settings, purchases can be verified by as little as a phone call, making it very easy to make fraudulent purchases.

**Returning Merchandise for Cash**

The cases we have discussed in the fraudulent purchases section to this point have all involved the false purchase of merchandise for the sake of obtaining the merchandise. In some cases, however, the fraudster buys items and then returns them for cash. The best example of this type of scheme in our survey was Case 1510, in which an employee made fraudulent gains from a business travel account. The employee began by purchasing tickets for herself and her family through her company’s travel budget. Poor separation of duties allowed the fraudster to order the tickets, receive them, prepare claims for payments, and distribute checks. The only review of her activities was made by a busy and rather uninterested supervisor who approved the employee’s claims without requiring supporting documentation. Eventually, the employee’s scheme evolved. She began to purchase airline tickets and return them for their cash value. An employee of the travel agency assisted in the scheme by encoding the tickets as though the fraudster had paid for them herself. That caused the airlines to pay refunds directly to the fraudster rather than to her employer. In the course of two years, this employee embezzled over $100,000 through her purchases scheme.

**Preventing and Detecting Personal Purchases on Company Credit Cards and Purchasing Cards**

The most important step in preventing credit card and purchasing card fraud is conducting thorough reviews of each card statement. This duty should be performed by someone independent of those who have signature authority on the account. During review, a business purpose should be verified for each listing on the statement, and the person who incurred the expense should be required to provide original support for the expense.

To prevent falsifications of the statement, organizations should direct the card issuer to send two copies of the statement to two different individuals within the organization. Both individuals should reconcile the statements separately and then compare the results. In the case of credit cards, it is advisable to establish spending limits for credit card users in order to prevent large abuses.

Card statements should be compared with employee expense vouchers for duplications, and card expenses should be monitored for any unexplained increase in purchasing levels. Excess purchases can be traced to a particular cardholder, and that person can be interviewed to determine the reason for the increase.

**Proactive Computer Audit Tests for Detecting Billing Schemes 1**

| Title  | Category  | Description  | Data file(s)  |
| --- | --- | --- | --- |
| Perform a trend analysis of vendor payments. | All | Special note should be given to vendors that have had minimal purchases in prior periods, yet have large payments in current periods. | * Invoice payment
 |
| Identify duplicate payments based on various means. | All | Duplicate payment tests can be enacted on the vendor, invoice number, and amount. More complicated tests can look for instances in which the same invoice and amount are paid, yet the payment is made to two different vendors. Another advanced test is to search for same vendor and invoice when a different amount is paid. | * Invoice payment
 |
| Summarize debit memos by vendor, issuer, and type. | All | Debit memo trends that appear unusual should be investigated as attempts to cover unauthorized payments. | * Invoice payment
 |
| Summarize accounts payable activity by general ledger account, sort from high to low, and review for reasonableness. | All | Expense account trends that appear unusual should be investigated as attempts to cover unauthorized payments. | * Invoice payment
* General Ledger distribution
 |
| Extract manual checks and summarize by vendor and issuer. | All | Manual checks are more prone to abuse and therefore should be scrutinized, especially if a particular issuer is drafting the majority of manual checks. | * Check register
 |
| Extract all purchases having no purchase order and summarize by vendor and issuer. | All | Purchases having no purchase order are more prone to abuse and therefore should be scrutinized, especially if a particular issuer is drafting the majority of payments without purchase orders. | * Invoice payment
 |
| Extract all round-dollar payments. | All | Round-dollar payments have a higher likelihood of being fabricated and, therefore, fraudulent. | * Invoice payment
 |
| Calculate the ratio of the largest purchase to next-largest purchase by vendor. | All | By identifying the largest purchase to a vendor and the next-largest purchase, any large ratio difference may identify a fraudulently issued “largest” check. | * Invoice payment
 |
| Compare check register to invoice payment file to identify any checks with no related system invoices. | Shell Company | Check payments that do not appear on the invoice register may be an attempt to hide unauthorized payments. | * Invoice payment and check register
 |
| Match vendor master file to accounts payable invoice file. | Shell Company | Identify payments to a potentially unapproved vendor by joining the vendor to the invoice file on vendor number. The joining of these two files should be done in an “unmatched” format so that only those vendor numbers in the invoice file not appearing in the vendor file are shown. | * Vendor master
* Invoice payment
 |
| Extract vendors having no telephone or tax ID number. | Shell Company | Vendors without this information are more prone to abuse and should be scrutinized. | * Vendor master
 |
| Identify vendors added during the period under review. | Shell Company | The issuers of new vendor additions should be reviewed using this report to determine whether a particular issuer is drafting the majority of vendor additions. | * Vendor master
 |
| List all vendors having an address that is not designated as a business address. | Shell Company | The identification of whether an address is legitimately a business address can be done using some software databases. | * Vendor master
 |
| List all vendors who had multiple invoices immediately below an approval limit (e.g., many $999 payments to a vendor when there is a $1,000 approval limit), highlighting a circumvention of the established control. | Shell Company | Invoices below an approval limit may be an attempt to circumvent a management review. | * Invoice payment
 |
| Match the vendor master file to the employee master file on various key fields. | Shell Company | Compare telephone number, address, tax ID numbers, numbers in the address, zip code, and post office box in the vendor file to those in the employee file, especially those of employees working in the accounts payable department. | * Vendor master
* Employee master
 |
| Review payments having little or no sequence between invoice numbers. | Shell Company | Employees developing shell companies often invoice the company with no gaps in invoice sequence, highlighting that the victim company is the shell company’s only customer. | * Invoice payment
 |
| List payments to any vendor that exceed the twelve-month average payments to that vendor by a specified percentage (e.g., 200%). | Shell Company and Non-Accomplice Vendor | Large payments are unusual and should be scrutinized as potentially fraudulent. | * Invoice payment
 |
| Extract vendor payments that are a specified percentage (e.g., 200%) greater than the last largest payment to that vendor. | Shell Company and Non-Accomplice Vendor | Large payments are unusual and should be scrutinized as potentially fraudulent. | * Invoice payment
 |
| Sample vendor open invoices for confirmation with vendor. | Non-Accomplice Vendor | Vendor invoices may remain open on the subledger when the vendor believes such invoices have been paid. | * Invoice payment
 |
| Extract SIC codes from card payments normally associated with personal purchases. | Personal Purchases | Personal purchases with company cards may be a sign of abuse. | * Procurement card
 |
| Extract multiple charges of the same product type (using SIC code) below a predefined card expense limit. | Personal Purchases | Charges below an approval limit may be an attempt to circumvent a management review. | * Procurement card
 |
| Summarize card use by employee and sort from high to low. | Personal Purchases | High usage of credit or purchasing cards by certain employees may be a sign of abuse. | * Procurement card
 |
| List all vendors with differing billing and delivery addresses. | Personal Purchases | Company purchases sent to a delivery address different from the billing address may signal personal purchases made on account of the company. | * Vendor master
 |
| Extract all delivery addresses that do not correspond to company locations. | Personal Purchases | Company purchases should normally be sent to known company locations. Shipments to other locations are a potential sign of fraud. | * Vendor master
 |

**Summary**

Billing schemes may be loosely defined as frauds in which an employee causes the victim organization to issue a fraudulent payment by submitting invoices for fictitious goods or services, inflated invoices, or invoices for personal purchases. Billing schemes are among the most costly, and the most common, forms of occupational fraud. These frauds generally fall into one of three categories: shell company schemes, non-accomplice vendor schemes, and personal purchases schemes.

A shell company is a fictitious entity set up for the sole purpose of committing fraud and may be nothing more than a fabricated name and an account number or a post office box that an employee uses to collect disbursements from false billings. Shell company schemes usually involve the purchase of fictitious goods or services, although in pass-through schemes a shell company might supply a real product or service by simply acting as the middleman between a real vendor and the victim organization, inflating the purchase price along the way.

In non-accomplice vendor schemes, a fraudster overbills his organization using the invoices of a legitimate vendor that is uninvolved in the fraud. This can be accomplished by producing counterfeit copies of a legitimate vendor’s invoices, or by simply running an invoice through the payables system twice and keeping one of the resulting disbursements. A distinct subcategory is the pay-and-return scheme, in which a fraudster intentionally overpays an invoice and steals the excess payment when it is returned by the vendor.

An employee may make personal purchases with company money or using company credit cards or purchasing cards. In the first case, the employee purchases a personal item and runs the invoice through the accounts payable system; in the second, the employee makes personal purchases using company credit cards or running accounts with vendors.

**Essential Terms**

Billing scheme

A scheme in which a fraudster causes the victim organization to issue a fraudulent payment by submitting invoices for fictitious goods or services, inflated invoices, or invoices for personal purchases.

Shell company

A fictitious entity created for the sole purpose of committing fraud.

Collusion

A situation in which two or more employees work together to commit fraud by overcoming a well-designed internal control system.

Pass-through scheme

A subcategory of a shell company scheme in which actual goods or services are sold to the victim company, with the fraudster acting as a middleman and inflating the prices of the goods or services.

Pay-and-return scheme

A fraud in which an employee intentionally mishandles payments that are owed to legitimate companies, then steals the excess payments when they are returned by the vendor.

Personal purchases scheme

A category of billing scheme in which an employee simply buys personal items with his company’s funds, credit card, or purchasing card.

**Review Questions**

|  |  |
| --- | --- |
| 4‑1 | (Learning objective 4-1) What are the five categories of fraudulent disbursements, and where did billing schemes rank in terms of frequency and cost in the *2009 Global Fraud Survey*?  |

|  |  |
| --- | --- |
| 4‑2 | (Learning objectives 4-2 and 4-3) How is the term *billing schemes* defined, and what are the three categories of billing schemes covered in this chapter?  |

|  |  |
| --- | --- |
| 4‑3 | (Learning objective 4-4) What is the purpose of a shell company, and how is it normally formed? |

|  |  |
| --- | --- |
| 4‑4 | (Learning objective 4-5) There are four ways that fraudulent invoices are approved for payment. What are they? |

|  |  |
| --- | --- |
| 4‑5 | (Learning objective 4-5) Why does collusion among employees in the purchasing process make it very difficult to detect billing schemes?  |

|  |  |
| --- | --- |
| 4‑6 | (Learning objective 4-6) Why do most shell company schemes involve the purchase of services rather than goods? |

|  |  |
| --- | --- |
| 4‑7 | (Learning objective 4-7) What is a pass-through scheme, and how does it differ from a typical shell company billing scheme? |

|  |  |
| --- | --- |
| 4‑8 | (Learning objective 4-9) What is a pay-and-return scheme? List three examples of how this type of fraud can be committed. |

|  |  |
| --- | --- |
| 4‑9 | (Learning objective 4-10) How does an employee use a non-accomplice vendor’s invoice to generate a fraudulent payment? |

|  |  |
| --- | --- |
| 4‑10 | (Learning objective 4-12) How does an employee make personal purchases on company credit cards, purchasing cards, or running charge accounts?  |

**Discussion Issues**

|  |  |
| --- | --- |
| 4‑1 | (Learning objectives 4-3 and 4-4) In the case study of Cheryl Brown, the administrative assistant at a Southeastern medical school, what type of billing scheme did she commit?  |

|  |  |
| --- | --- |
| 4‑2 | (Learning objectives 4-8, 4-11, and 4-13) Explain how separation of duties contributes to the prevention and detection of billing schemes.  |

|  |  |
| --- | --- |
| 4‑3 | (Learning objectives 4-8 and 4-14) List and explain at least four proactive audit tests that could be performed to help detect a shell company scheme.  |

|  |  |
| --- | --- |
| 4‑4 | (Learning objectives 4-4, 4-5, and 4-8) What are some of the ways shell company invoices can be identified? |

|  |  |
| --- | --- |
| 4‑5 | (Learning objectives 4-4 and 4-7) Sharon Forsyth worked in the purchasing department of a retail store. She was in charge of ordering merchandise inventory and various supplies for the organization. She purchased merchandise through a fictitious shell company and then resold it to her employer at an inflated price. What is the name for this type of fraud?  |

|  |  |
| --- | --- |
| 4‑6 | (Learning objective 4-9) Karen Martinis was responsible for opening mail, processing vendor claims, and authorizing payments. She was involved in a scheme in which she either double-paid vendor invoices, paid the wrong vendors, or overpaid the right vendors. What type of billing scheme is being described in this case?  |

|  |  |
| --- | --- |
| 4‑7 | (Learning objective 4-9) What type of internal controls can be utilized to help prevent pay-and-return billing schemes? |

|  |  |
| --- | --- |
| 4‑8 | (Learning objective 4-12) In terms of classifying frauds under the fraud tree system, how does a scheme in which an employee fraudulently orders merchandise for his personal use differ from a scheme in which an employee steals merchandise from his company’s warehouse?  |

**Endnotes**

1Lanza, pp. 48–50.

Principles of Fraud Examination, Third Edition Chapter 4: Billing Schemes

ISBN: 9780470646298 Author: Joseph T. Wells CFE, CPA

Copyright © John Wiley & Sons Inc. (2011)