BILLING SCHEMES

Purchasing & Accounts Payable Fraud

Lowers Risk Group – Risk Mitigation White Paper Series

LowersRiskGroup™

Protecting People, Brands, and Profits

(540) 338-7151 | www.lowersriskgroup.com

BILLING SCHEMES: PURCHASING AND ACCOUNTS PAYABLE FRAUD

BACKGROUND

The purchasing and accounts payable processes are so closely integrated, and the controls so overlapping, that they must be discussed together. For a purchasing fraud to be successful, the perpetrator must know the checks and balances and weaknesses in both the purchasing and the accounts payable systems in order for the fraud to succeed. Consequently, the discussion of fraud in these two areas will be discussed under the more generic term "billing schemes."

According to the *2012 Report to the Nations on Occupational Fraud and Abuse* published by the Certified Fraud Examiners Association, billing schemes are the most common of the fraudulent disbursement schemes. These scheme types made up 50% of all cases identified at the time of the survey. Such schemes are highly profitable for the perpetrator, with a median loss of $100,000, making them the second most expensive form of fraudulent disbursement behind check tampering, which has a median loss of $143,000.[1]

TYPICAL /EXPECTED PURCHASING/ACCOUNTS PAYABLE PROCESSES

1. A request is initiated by an authorized purchasing agent to add a vendor to the "Master Vendor List." The request is sent to the designated person in the Finance Department.

2. A "due diligence" investigation is conducted and documented by the Finance Department regarding the vendor (company or person). This investigation should include, but not be limited to, the following:

    - Verification of the tax ID number or Social Security Number,
    - Verification of incorporation status & identity of officers through the state's office of incorporation,
    - Fictitious name filing,
    - Business license,
    - D & B report to verify business credit, UCC filings, and

[1] Association of Certified Fraud Examiners, 2012 Report To The Nations On Occupational Fraud and Abuse.

- Verification of address and telephone number through database/Internet sources.

3. Purchase request initiated and approved by authorized individual.

4. Purchase order completed, purchase order number assigned, and purchase of goods or services made. Purchase order number is given to vendor and should be included on the invoice from the vendor.

5. Goods are received or service completed.

6. If physical item, goods received are matched to the shipping document (Bill of Lading) and the purchase order.

   - If item is a physical asset, the asset department is notified and the item is assigned an inventory number, tagged, and added to the inventory record before release to the requestor.
   - If item is supply or production inventory, inventory levels are adjusted accordingly.

7. Verified shipping document is sent to accounts payable by the Receiving Department.

8. Invoice for payment of shipped goods is received by accounts payable from the vendor.

9. Vendor is verified by accounts payable against the Master Vendor List. The invoice and shipping document are compared to the purchase order.

10. Check to the vendor is created by accounts payable clerk.

11. Check, invoice, shipping document, and purchase order are provided to the authorized check signer for review prior to check signing.

12. The check run is reconciled daily by someone other than the accounts payable clerk who produced the checks. All checks issued or voided are accounted for and compared to the purchase order and the shipping and receiving documentation. In addition, a physical inventory is conducted daily of all blank checks.

COMMON VULNERABILITIES

1. Controls over additions and changes to the Master Vendor List are often weak. In some cases a phone call from a department manager is all that's required. In other cases, the purchasing agent is able to add names to the vendor list. Such changes in the Master Vendor List rarely produce an exception report.

2. Due diligence on new vendors is often minimal.

3. Auditing controls surrounding vendors who supply "consulting" services or advertising services are often weak. (See AUDITING module for further discussion).

4. Cost considerations have resulted in lower staffing levels, decreased separation of duties, over-reliance upon computerized systems, and increased volume of transactions.

5. In order to reduce costs, companies often forego costly pre-employment screening. As a result, individuals might be hired who have less than desirable backgrounds.

6. Some of the computerized Purchasing and Accounts Payable software is flawed, and employees can find and exploit these weaknesses in the internal controls. And while the programs are normally customizable to increase the required controls, many companies do not have the time, resources, or expertise to modify the systems as they need to be. Without modification, the systems often have weaknesses that can be easily exploited.

7. Most Accounts Payable and Purchasing systems do not produce automatic exception reports that result in "red flag" notifications to auditors and managers. Instead, the variance reports that are available must be requested and then analyzed.

8. With the increase in computerization and integration of systems, Receiving personnel often have access to the computerized purchase order and can view it on line. In such instances, Receiving personnel can record receipt of items that matches the purchase order, rather than having to conduct a "blind count" and merely document the results. This increases the risk of counts not being made, or theft of overages in shipments.

9. In almost all systems, procedures exist for issuing checks in an emergency that allow controls to be by-passed.

10. Most computerized accounts payable and purchasing systems allow critical information to be changed after a purchase order is written without producing an audit trial or exception report, i.e.., unit price, quantity.

11. Computer access controls and user rights and responsibilities are often weak, thereby permitting compromise of the systems.

12. Collusion between employees and vendors, with the vendor giving kickbacks to the employee, is a frequent event and often difficult to detect if the employee is in a key position.

ESSENTIAL CONTROLS

PURCHASING:

1. Purchasing policies and procedures have been incorporated into a written document.[2]
2. Levels of authority have been published throughout the organization that specify who is permitted to approve purchases, for what items, and for what amount.
3. Approved purchase requests are required for all purchases over a specified dollar amount.[3]
4. A numbered purchase order system has been implemented and is followed. The numbers are secured against unauthorized access and use.
5. An approved vendor list has been established.[4]
6. Persons authorized to approve purchases or issue purchase order numbers should not able to make changes to the approved vendor list.
7. Competitive bids are required for all purchases over a specified dollar amount.
8. Purchasing personnel may only offer or accept nominal gratuities.[5]
9. Purchasing databases and/or bills of lading are immediately documented with the details of all goods received.
10. Received property is added to inventory records as soon as possible.[6]
11. Bills of lading and signed receipts for goods are forwarded to Accounts Payable within one business day.

---

[2] The document is current and contains all essential control elements contained herein. Written policies are essential to ensure uniformity of practices and to establish management's clear intent.

[3] Most organizations have a dollar amount established, i.e., $100, and any items under that limit do not require a purchase request. In such instances, the purchaser would typically submit his or her receipt and get reimbursement for the purchase. But the limit, whatever it is, should be established in writing and any purchases over that amount should require an approved purchase request.

[4] An approved Master Vendor List is a critical control element. Most vendor/purchasing frauds involve manipulation of weaknesses in this control function. The list must be tightly controlled and monitored. (1) Changes to the approved vendor list cannot be made without a formal review and acceptance procedure. (2) An adequate due diligence should be conducted prior to adding vendors to the approved vendor list. (3) Changes to the approved vendor list should automatically generate an exception report that is reviewed by auditing and by management.

[5] Corporate guidelines should be in place that clearly define the limits.

[6] Received property, particularly high value goods, should be properly safeguarded until they are released to the end user. Items that are physical assets should be tagged with property identification labels (preferably bar coded for ease of inventory), and released to an asset manager for distribution to the end user.

ACCOUNTS PAYABLE:

1. Accounts Payable policies and procedures have been incorporated into a written document. The document is current and contains all essential control elements contained herein.

2. Bills of lading for goods received are matched against the invoice and the approved purchase order.

3. Invoices are not paid for partial shipments. Adequate controls are in place to ensure partial shipments are not paid.

4. Adequate controls are in place to prohibit the payment of duplicate invoices.[7]

5. Accounts payable staff members have "read only" capability on purchase order screens for on-line systems. They cannot modify vendor name, payment address, item, quantity, price, or specifications.

6. Accounts payable staff has no capability to modify approved vendor lists.[8]

7. Procedures are in place to follow-up on unmatched open purchase orders, receiving reports, and invoices, and to resolve missing, duplicate, or unmatched items.[9]

8. Checks used by accounts payable staff are adequately secured and under dual control. Keys to the check storage area are not kept on the premises.[10]

9. All boxes of blank checks remain sealed until required to be open for daily use.

10. All checks used by the accounts payable department are consecutively numbered.

11. A perpetual inventory is kept of all blank checks stored and used by the accounts payable department. Unused checks from the daily supply are returned to the inventory and accounted for.[11]

---

[7] In automated systems, the computer should flag & prevent payment of duplicate invoices. In manual systems, labor-intensive processes are required to ensure duplicate invoices are not paid.

[8] This function should always be separated from the accounts payable function (and the purchasing function). It should normally reside in the Finance Department, but no one who can issue a check should be able to add to or modify the Master Vendor List.

[9] Failure to follow-up on such items increases the probability that bogus purchase order numbers will be used, that received goods will be stolen, or that duplicate invoices will be paid.

[10] Risk assessments often reveal that keys to check storage areas are "hidden" in desk drawers and that numerous people know the location of the key. This increases the probability that checks will be stolen and used directly, or stolen and subsequently reproduced in larger quantities.

[11] The perpetual inventory should be designed and documented so that at any point in time a physical inventory can be easily conducted and all blank checks, including working stock, can be accounted for readily.

12. Monthly inventories of blank checks are conducted under dual control. The results of the physical inventory are reconciled with the perpetual inventory.

13. Levels of authority have been established for check signing, including when dual signatures are required; the established levels appear reasonable for the type of business.

14. Persons signing checks are presented with the documentation to support the checks (i.e., bill of lading, invoice, or statement).

15. Daily reconciliation is made between the checks written, checks voided, the check inventory, and (where possible) the computer record of all checks issued. A supervisor or manager that is independent of the accounts payable staff member(s) who processes invoices for payment performs the reconciliation.[12]

16. If mechanical check signers or signature plates are used, the equipment is properly secured under dual control when not in use.

17. Access to the Accounts Payable software program is properly restricted and controlled.

18. Emergency payments requiring handwritten checks are not processed by Accounts Payable personnel. Supervisory personnel must be involved and the process should be fully supported with adequate documentation.

19. A monthly reconciliation of the checking account used by Accounts Payables is performed; a person who has no access to checks, signature plates, or Accounts Payable software programs conducts the reconciliation.

20. Cancelled checks are secured in the same manner as blank checks.[13]

COMPENSATORY MEASURES

1. If a master vendor list is developed and maintained outside an automated system, access to the list must be extremely limited and tightly controlled. If the list is kept on a PC hard drive or a network file server, the file should be password protected and encrypted if possible. Any hard copies of the list should be kept in a burglary resistant storage container that is locked at all times. Similarly, documentation supporting changes to the master vendor list (i.e. the due diligence results, etc.) should be comparably protected. This list should be subject to scheduled and unannounced audits by management and the auditing department.

[12] It is essential that the daily reconciliation be performed and that it is independent. A common weakness is the relegation of the reconciliation function to the same person who writes the checks.
[13] This is necessary in order to prevent scanning of signatures and duplication of check paper.

2. If purchase order numbers are developed and maintained outside an automated system, access to the numbers should be controlled in the same manner as the master vendor list and the issuance of the numbers subject to similar audit procedures.

3. Where purchasing authority is not centralized, some of the compensatory measures are as follows:

    - Policies and procedures must be developed from a centralized source, i.e., Finance Department. The policies must contain direction on the following as a minimum:
        - Levels of purchasing authority,
        - Who must approve what types of contracts for goods and services and at what dollar level,
        - Procedures for adding to or changing the master vendor list and the level of due diligence required,
        - Purchase order number controls,
        - Shipping and receiving controls,
        - Inventory controls and inventory reconciliation,
        - Acceptance of gifts or gratuities, and conflicts of interest.
    - Policies and procedures must be in writing and must be kept current.
    - All locations that manage their own purchasing function should be subjected to an internal audit review at least annually.
    - The audit staff should be equipped with fraud detection software, such as ACL, and receive special training in its use. The software should be used during any audit review.

CASE STUDY #1

Lowers & Associates staff worked on a case where a dishonest employee had discovered how to manipulate a vendor file called up to enter a new invoice for payment. She had discovered that she could enter the invoice information (invoice number, date, dollar amount, due date, PO number, etc.) and then change the vendor name to any vendor – Acme Mortgage (who held the note on her house)...American Express....L.L. Bean...anyone. And that's the name that would be printed on the check.

When the check run was printed in the afternoon, she was responsible to pull the checks from the printer and she simply pocketed the manipulated payment. Later, she returned to that vendor file and changed the name back to the correct name of the vendor.

But what about the cancelled check after the good folks at L.L. Bean, for example, deposited it? Because the company was on a positive pay system with the bank, it was retained at the bank and imaged and never returned to the company. The check register electronically transmitted to the bank said "O.K. to pay check 1234 in the amount of $345.00." So the bank did.

The only place that payment appeared with the name "L.L. Bean" was in a printed copy of the check register. And our faithless employee simply removed that page after each check run. But even if she didn't, who "in this age of mega databases" would ever look at the check register? If they had, they would have discovered a missing page however the register was automatically purged from system storage in the interest of preserving file space.

Now the software package did contain a report feature that would produce a variance report whenever a vendor name was changed. But the company never switched it on because they didn't have enough people to review the report.

So, the beauty of her scheme was that she didn't have to generate any false invoices. She didn't have to set up a shell company to handle the checks. She didn't even need a bank account. She didn't have to manipulate the monthly statement or reconciliation. She simply made the checks payable to her own vendors rather than the company's vendors.

How did she get caught after stealing about $300,000 in one year? Interestingly, she had been terminated about 10 weeks before this was discovered because her supervisor had found $600,000 in undeposited checks in her desk during an absence. She was caught because she used vendor accounts that delivered tangible goods to the company. Two inventory managers felt too much inventory was being charged to them and asked for a printout of vendor payments charged to their general ledger codes. They saw payments to a particular vendor that were in even dollar amounts of $1,000, $500, etc. This was very unusual. When they asked to see the corresponding invoices, there were none. When they asked to see the checks, copies were retrieved from the bank and the problem was discovered.

Her chances of being caught would have been lessened if she had used GL codes for expense items (legal expenses, executive retreat or training, etc.) rather than tangible inventory.

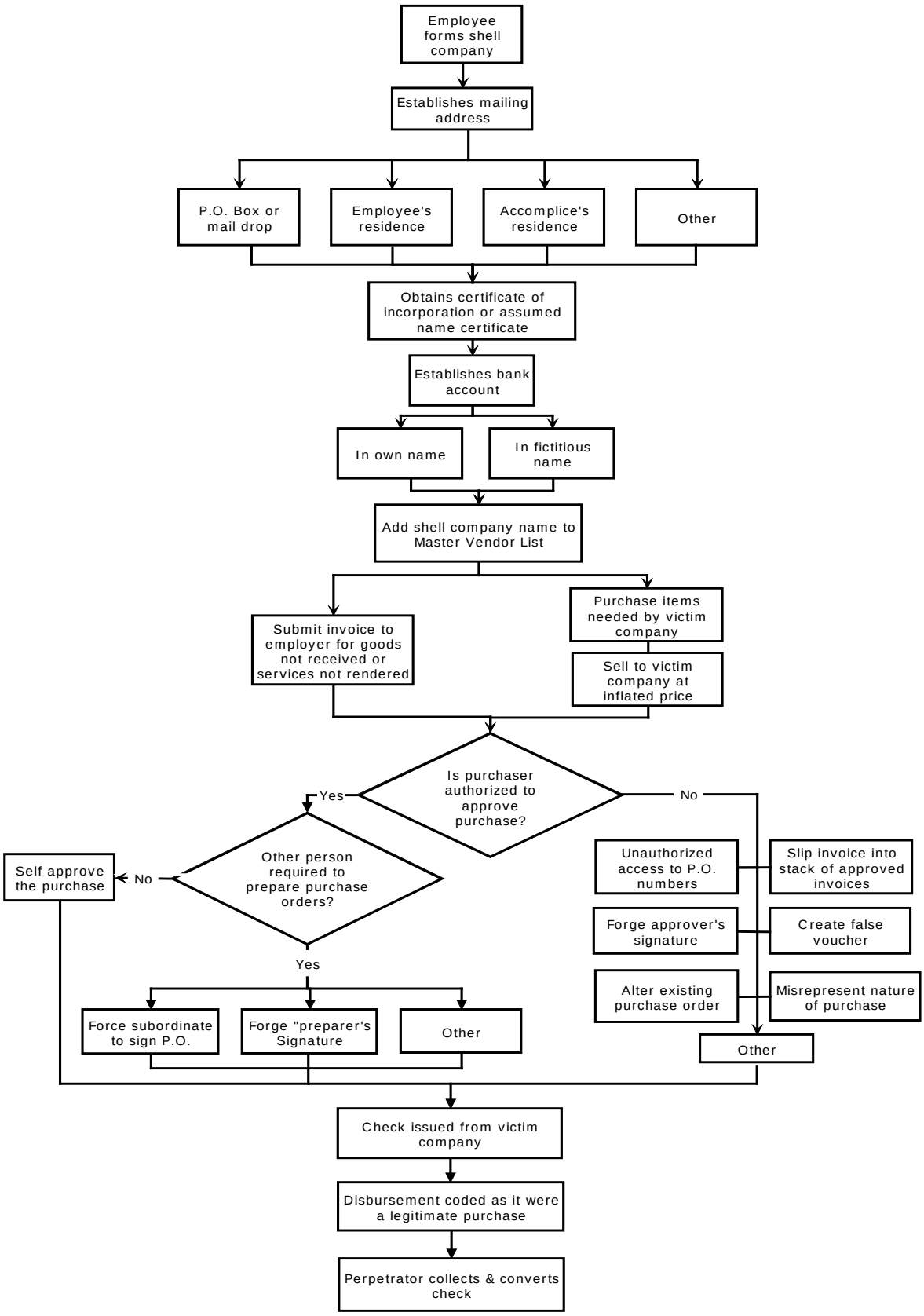
CASE STUDY #2

A warehouse foreman and a parts ordering clerk conspired to purchase approximately $300,000 of nonexistent supplies. The parts ordering clerk would initiate 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.[14]

CASE STUDY #3

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. He 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 $1 million.[15]

[14] Wells, Joseph T., Occupational Fraud and Abuse, Obsidian Publishing Company, Austin, Texas, 1997, pages 230-231 , page 239
[15] Wells, Ibid., page 240


Employee forms shell company
Establishes mailing address
P.O. Box or mail drop
Employee's residence
Accomplice's residence
Other
Obtains certificate of incorporation or assumed name certificate
Establishes bank account
In own name
In fictitious name
Add shell company name to Master Vendor List
Submit invoice to employer for goods not received or services not rendered
Purchase items needed by victim company
Sell to victim company at inflated price
Is purchaser authorized to approve purchase?
Yes
No
Other person required to prepare purchase orders?
Self approve the purchase
No
Yes
Force subordinate to sign P.O.
Forge "preparer's Signature
Other
Unauthorized access to P.O. numbers
Slip invoice into stack of approved invoices
Forge approver's signature
Create false voucher
Alter existing purchase order
Misrepresent nature of purchase
Other
Check issued from victim company
Disbursement coded as it were a legitimate purchase
Perpetrator collects & converts check

LOWERS RISK GROUP – Fidelity & Crime White Papers

There are three conditions that are present when fraud occurs: Opportunity, Incentive, and Rationalization. The information contained in these papers demonstrates examples of vulnerabilities and how applying essential controls can significantly reduce the risk of fraud.

ABOUT LOWERS RISK GROUP

Lowers Risk Group combines the services of three industry-leading companies – Lowers & Associates, Proforma Screening Solutions, and Wholesale Screening Solutions – to create a complete risk management service offering for organizations of all shapes and sizes. Employed in concert or on a standalone basis, we excel in providing comprehensive enterprise risk management and human capital risk solutions to organizations operating in high-risk, highly-regulated environments. Our specialized background screening and crime and fidelity risk mitigation services protect people, brands, and profits from avoidable loss and harm. With Lowers Risk Group you can expect an experienced and professional approach to your risk assessment, compliance, human capital, and risk mitigation needs to help move your organization forward with confidence.

Contact Information:

Lowers Risk Group
125 East Hirst Road
Suite 3C
Purcellville, VA 2 0132

Telephone: 540-338-7151
Fax: 540-338-3131
Email: info@lowersrisk.com
Web: www. lowersrisk.com