Legal Intelligencer
https://www.law.com/thelegalintelligencer/2019/10/03/cookin-with-quickbooks-common-schemes-and-how-to-prevent-them/

Commentary

Cookin’ With QuickBooks: Common Schemes and How to Prevent Them

Asset misappropriation involves either the theft of inventory or other assets, or more commonly, the theft of cash, which includes actual cash on hand and fraudulent disbursements.

By **Heather L. Wilson** | October 03, 2019 at 12:29 PM

Heather Wilson of Marcum.

Each year the Association of Certified Fraud Examiners issues a Report to the Nations, a global study on occupational fraud and abuse (ACFE report to the nations). Occupational fraud or internal fraud is broadly defined as "… the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the organization's resources or assets." Stated differently, it is the fraud that is committed by an entity's own officers, directors or employees. It is the largest and most prevalent fraud threat against an organization. Asset misappropriation is the most common scheme representing 89% of the cases studied, with a median loss of approximately $114,000.

Asset misappropriation involves either the theft of inventory or other assets, or more commonly, the theft of cash, which includes actual cash on hand and fraudulent disbursements. Two of the most common and costliest types of fraudulent disbursements schemes are check/payment tampering and billing schemes. Check and payment tampering includes schemes such as the diversion of legitimate vendor payments through fraudulent endorsements, the altering of payees to fraudulent individuals, and authorized maker schemes, where an employee with signature authority writes fraudulent checks for his own benefit. Billing schemes include the creation of fictitious vendors and the subsequent payments to these vendors.

The longer a fraudster's scheme goes undetected by management, the greater the related loss, which can grow exponentially. At the onset of an embezzlement, a certain level of apprehension exists, where the fraudster tests out the waters to make sure they aren't going to get caught. Once they become more confident in their scheme, the fraud begins to grow. Over a three-year period, the median loss doubles approximately every six months.

Duration	**Percent of Cases**	**Median Loss**
6 months or less	27%	$30,000
7 – 12 months	19%	$75,000
13 – 18 months	10%	$125,000
19 – 24 months	13%	$200,000
25 – 36 months	11%	$400,000

Frauds are more likely to occur in smaller organizations, with 28% of victim organizations having less than 100 employees. Smaller organizations have fewer resources to implement the appropriate controls to prevent or minimize potential fraudulent acts. Additionally, the median loss related to these frauds is approximately double than that of organizations with greater than 100 employees.

It is important to be aware of common fraudulent disbursement schemes, how they are carried out, and how you can prevent them. If you do become a victim, it is imperative to catch the scheme early in order to limit the loss exposure.

The Mind of a Fraudster

Perpetrators of occupational fraud are generally motivated by three factors:

- The opportunity to commit the fraud;
- A perceived financial need; and
- The ability to rationalize their fraudulent activities.

This is commonly known as the fraud triangle. The opportunity element poses a particular threat to smaller organizations and makes these entities vulnerable to asset misappropriation.

QuickBooks and Small Organizations

In my experience many smaller businesses use QuickBooks for accounting purposes. QuickBooks is a widely popular, user-friendly general ledger package, with over 5.6 million customers, and is geared toward small and midsized organizations. QuickBooks provides customers/clients with the ability to track income, expenses and balance sheet accounts, as well as produce readily available financial reports. It also has the ability to accept business payments, manage and pay bills, and perform payroll functions.

QuickBooks’ success in penetrating and providing the small-business market with a user-friendly accounting package has simultaneously exposed the package to manipulation by unscrupulous persons intent on perpetrating fraud against their employers. Throughout my career, I have investigated many asset misappropriations. Not surprisingly given its popularity, many of these investigations have involved the manipulation of QuickBooks entries to conceal illegal activities.

The Manipulation of QuickBooks

According to the ACFE data, small business organizations may be more frequent victims of occupational fraud schemes. These schemes can include the use of fictitious vendors, altered payees or the use of legitimate vendors to pay personal expenses.

My experience with these schemes and the manner in which the QuickBooks record was manipulated to conceal the activity is discussed in more detail below.

- **Fictitious Vendors**

An employee who has access to the purchases and accounts payable function in QuickBooks has the ability to create new vendors, legitimately or otherwise. Basic information is needed to create a new vendor, such as business name and contact information.

An employee could set up a fictitious vendor and divert payments to his own address or P.O. Box, and endorse the checks over to himself. He could also set up a bank account in the name of the fictitious vendor and deposit or cash the diverted funds. The diversion of funds is even easier with electronic payments, as opposed to checks. In this instance, an employee would set up the fictitious vendor and send payments electronically to a bank account that he set up.

Another important aspect to be aware of in QuickBooks' vendor set-up function is the "print on check" feature. This feature allows an employee to set up what appears to be a legitimate vendor and enter a different name on the print on check field. For example, a new vendor is set up for ABC Plumbing and the print on check field is entered as Jane Smith. All checks would be printed to Jane Smith, but the transactions in QuickBooks would appear as ABC Plumbing.

- **Altered Payee**

Altered payee schemes involve changing the name of the payee in order to misappropriate the funds. An employee that has access to both the purchases and accounts payable function in QuickBooks, could easily manipulate the payees. For these schemes, an employee could access the vendor information section, edit an existing vendor name to an altered name, print the fraudulent checks, and then change the vendor name back to the original vendor information.

- **Use of Legitimate Vendors**

In continuing with the previous discussion, for legitimate vendors, an employee could access the vendor information section, alter the print on check field to a fraudulent name, and print the fraudulent checks, thereby diverting the funds.

Additionally, the employee could utilize legitimate existing vendors to pay expenses for his own benefit. This could be done through corporate credit cards, reimbursements of employee expenses, and other expenses such as telephone, cell phone, utilities or cable expenses. The employee could add a payment to the legitimate vendor, include his own account number, and divert the payment.

How to Detect and Prevent These Frauds

- **Individual User Names and Passwords**

Even in small organizations, each user should have a unique login and password. QuickBooks has an audit trail function that allows a user to review accounting transactions, including any subsequent additions, deletions or modifications to that transaction. The audit trail identifies the date and time when the transaction was last modified and the user who made the modification, and details the changes made to that transaction in bold. The use of one admin user account does not allow activity to be traced to a specific person when using the audit trail function. I have investigated numerous frauds over my 20-plus year career, and I believe the most significant improvement that QuickBooks has made is that the audit trail function is now an automatic feature that cannot be disabled. Prior to the 2006 version of QuickBooks, users could turn off the audit trail feature, making the tracing of the fraudster’s activity impossible. Additionally, as with any login and passwords, users should not share user accounts, and employees should be required to change passwords at regular intervals.

- **Restricting Access**

Employee access should be restricted within QuickBooks for specific functions, thereby creating a segregation of duties. When setting up new users or editing access for existing users, restrictions for different areas can be customized by selecting no access, full access, or selective access. To reduce the threat of asset misappropriation, an employee’s access should be limited so they do not have access to create and edit vendors, enter bills, and create payments. Having access to all three areas would give the user unfettered ability to manipulate payables.

- **Attaching Support to Transactions**

When entering vendor bills in QuickBooks, supporting documentation (such as invoices) should be required to be uploaded to provide third-party backup for those transactions. This makes the review of questionable transactions easier, as the transaction and all supporting documentation is centrally located.

- **Review of the Audit Trail**

As previously discussed, QuickBooks contains an audit trail function that allows an individual to review all transactions, and any subsequent additions, deletions or modifications to that transaction. Many times the fraudster is not even aware of the audit trail function, which makes uncovering the fraud easier. In my experience, management does not regularly review this report and may not be aware of its existence. The audit trail report should be reviewed on a regular basis, and any abnormal transactions investigated.

- **Elimination of Audit Trail**

Although the audit trail is an automatic feature that can’t be turned off, be aware that the condense data utility provides a path to circumvent it. The intention of this utility is to reduce the overall size of your QuickBooks file. It consolidates most, but not all, transactions into singular journal entries dated based on the last day of the month. However, since this utility removes detailed transactions from your company file, they are also removed from the audit trail report. Additionally, beginning with the QuickBooks 2019 version, the condense feature provides an option to leave the detailed transactional data and remove the audit trail information.

The only users able to utilize the condense data utility are the admin user and the external accountant user. To protect against the elimination of the audit trail, limit access to the admin login and require all users to have individual logins and passwords. Additionally, remember that if you fall victim to unauthorized data condensing, original transactional data is preserved in any previous backups or archived data copies created.

- **Closing Accounting Periods**

Financial activity should be closed out at the end of each accounting period to eliminate the opportunity for fraudulent transactions to be posted to a prior period, which may go unnoticed by management.

Conclusion

It is important for small business owners and managers to be aware of common occupational fraud schemes and how QuickBooks can be manipulated for fraudulent purposes. By arming your management team with a few prevention and detection techniques, you may be able to avoid these frauds. However, if your company does become a victim, an experienced forensic accountant can assist in unraveling the scam and identifying the loss exposure and potential avenues of recovery.

Heather L. Wilson *is an advisory services director in the Philadelphia office of Marcum, a national accounting and advisory firm with offices in major business markets throughout the United States, as well as overseas. She can be reached at* ***heather.wilson@marcumllp.com****.*