Protect Your Business from Fraud: Keep Your Financial Information Secure

By Joe Woodard
President, Creative Financial Software

More than a quarter of business owners have been victims of fraud, which can result in thousands of dollars in losses to your business and, in some cases, even bankruptcy. To fully protect your business finances, you need to have strong security controls in place in your financial management software.

Do you know where your business might be most vulnerable to fraud?

In this guide, you will learn how to identify various types of fraudulent activities and how to stop these activities before you incur significant loss of productivity or assets. You will also discover ways to keep the sensitive and confidential information in your financial management software safe from the prying eyes of people both inside and outside your business.

Fraud: It's a Bigger Problem Than You Think

Your growing business has to fend off many different kinds of threats: competition, economic changes, and the rising costs of goods or human resources—the list can be long. But one large threat to your business can be a silent, looming killer—fraud.

Fraud comes in a variety of forms, including credit card and check fraud as well as employee theft. Some of the most common types of employee fraud include stealing assets either directly or through kickbacks from third parties. Some specific examples include: taking bribes from customers/suppliers, claiming undue overtime, stealing company secrets, or embellishing an expense account.

Regardless of the nature of the fraudulent activity, the propensity for loss is tremendous. According to a survey of small and medium businesses conducted in October 2007, more than a quarter of business owners have been the victim of fraud.*

Fraud can threaten the stability of a business by resulting in significant financial losses. According to the survey, business owners who were victims of fraud had lost an average of $38,000 each—and four in ten had lost more than $50,000.

The Association of Certified Fraud Examiners (ACFE) reports the typical business will lose an average of 6 percent of revenues from employee theft alone. The ACFE *Report to the Nation on Occupational Fraud and Abuse* reveals that small businesses suffer disproportionate losses (compared to large corporations) due to the limited resources they have to devote to detecting fraud. Unfortunately, your own employees can significantly harm or even destroy your business. A U.S. Chamber of Commerce survey reports that one-third of business bankruptcies are due to employee theft.**

The good news is that business owners can—and are—fighting back. According to the October 2007 survey, business owners are starting to combat fraud, with 66 percent saying they have taken actions to protect their business against fraud in the past five years. It is imperative for you to join these businesses and protect yourself from fraud.

Identifying Fraud

Fraud exists in many forms. Both your employees and third parties can defraud your company. In many fraudulent scenarios, a company's employees work with outside parties to steal assets or company secrets. Unfortunately, employee fraud is one of the most difficult to detect and can occur right under your watchful eye.

According to research conducted by the National Small Business Administration, business owners that reported fraud were not usually the first to notice the fraudulent activity. Instead, their banks tended to make the discovery after reviewing financial information provided to them by the business' owners.

Employee fraud can take on many forms, including:

- Stealing money or goods
- Falsifying checks or payroll, including creation of phantom employees
- Misusing company credit card accounts
- Taking bribes or kickbacks from suppliers or customers
- Claiming overtime when it is not due
- Embellishing expense accounts
- Providing false information about the company to creditors or investors
- Stealing and selling company trade secrets
- Giving friends or relatives unauthorized discounts on company merchandise or services

Combating Fraud: Establish Controls

Even employees who are honest can be tempted when they see large sums of money right in front of them. This is especially true if the business owner has not implemented any access controls or set up shared control over the business finances.

One of the most important ways to fight—and detect—fraud in your business is to set up shared responsibilities for the business' financial management. Access to financial assets and information, including your accounting system, should be restricted and carefully controlled. Do not allow this to be a one-person task; make sure you have a separation of duties where no single employee has too much responsibility within the system.

There are many ways to share the financial management duties. You can outsource to a bookkeeping firm and/or request quarterly analyses of your financial system by a CPA or other accounting technology expert. Within your company, you should divide the financial responsibilities among the management team. For example, you can hire a part-time employee or bookkeeper who is responsible for payroll processing only and perhaps a few other disconnected tasks such as creating invoices or entering bills. This is highly preferable to having one person who manages all aspects of your accounting.

As you establish access controls, you should define and document your method for assigning access to your employees. If you are not deciding access rights yourself, assign a specific employee to be responsible for this area of your business. Be sure to review the assignments each quarter and approve with your signature.

One area to pay particular attention to is the control of documents from vendors. The bill payment process should be as follows:

1. The AP clerk who handles bill payments should provide a list of all unpaid bills to management.
2. Management marks which bills to pay and how much to pay for each bill – if not the full amount.
3. The AP clerk creates the bill payments and clips each bill payment to the bill(s) from the vendor. The AP clerk hands the packet to management for check signing.
4. As management signs each bill payment, the signer reviews the source documents from the vendor and stamps each bill as paid or each line item on the bill as paid. The signer can also use permanent ink to note the bill. This "defacing" of the bill is critical to ensure no accidental or intentional re-payment to vendors.
5. The AP clerk mails each bill and staples the bill payment stub to the "defaced" bill document. If the bill is partially paid, the AP clerk makes a copy of the bill and staples the stub to the copy and then files the original, partially paid bill in the AP folder for the next check run.

While this may seem like a lot of busy work, it is worth the effort. With this type of system control, businesses can have a single person input and pay bills without increasing the risk of fraud. You can also take this process and apply the concept to other areas of the business (e.g. invoicing for sales orders or creating paychecks from timesheet detail).

In addition to access controls, you can implement other processes that will help you fight fraud. Some best practices to consider:

- Add a signature line on your financial statements that include the author's initials and a date/time stamp
- Configure your network so only certain printers can print certain types of forms
- Only allow financial reports to be printed from certain printers
- Protect against payroll fraud by using direct deposit, regularly checking payroll records, and hand-delivering paychecks.

Combating Fraud: Assess Your Accounting System

In addition to establishing process controls, evaluating your accounting system is another important step toward preventing fraud. The financial information stored in your accounting system or financial management software is one of the key areas you need to protect.

To fully protect your confidential business information, you need to have strong access restrictions in place. Those access restrictions will protect your business not only from outsiders, but also from your own employees. If numerous employees use your financial management software, the access restrictions in your software become even more critical. Multi-user environments pose an increased risk of employee fraud or breach of confidentiality.

Some financial management applications offer several layers of security that can protect your business from fraud. One such application is QuickBooks Enterprise Solutions, which addresses security and helps you fight fraud in multiple ways, including:

1. User (Employee) Access Permissions
2. Always-on Audit Trail
3. Undeposited Funds Account (allows one employee to enter customer payments and other to enter bank deposits from customer payments)
4. Closing Date and Closing Date Password
5. Closing Date Exception Report
6. Previous Bank Reconciliation Reports
7. Various Company Preference Settings (e.g. to save transactions when printing)
8. Voided/Deleted Transactions Report
9. Customer Credit Card Protection and Customer Credit Card Audit Trail Report

Deploying QuickBooks Enterprise Solutions—and learning how to use each of these features—can help your business fight fraud.

User (Employee) Access Permissions

The best way to fight employee fraud is by setting appropriate access privileges within your accounting software. This type of function allows you to limit access for specific employees to specific tasks, including payroll processing and reporting. QuickBooks Enterprise Solutions helps you separate access to financial transactions and reports with its highly specific user permissions and controls.

By using this feature, you have the ability to give your employees permission to effectively do their jobs, yet still protect your sensitive information. If you set up roles and permissions correctly, Enterprise Solutions will keep every employee within their assigned areas of the program without any daily monitoring on your part.

You can use controls to distribute your workload and keep up with growth in your business. You have the control over what you allow people to do in your QuickBooks Company file. Using permissions and roles will not only reduce worry about fraud, but it will also keep your employees focused on the areas you have assigned to them.

The QuickBooks file administrator has control over which users can access which areas of the program—and what level of control each user will have in his or her assigned area. The file administrator can specify distinct access levels to more than 115 entitlements within 11 QuickBooks functional areas. Access levels include:

- View only
- Create
- Modify
- Delete
- Print

Enterprise Solutions contains 14 pre-defined roles (including the administrator role) that make setting up user permissions relatively easy. In the software, the administrator can highlight any role to see a description of the role's function, along with the users assigned to the role.

The administrator has the ability to control access to all lists (e.g. Customer, Item, Vendor) and to specific report groups (e.g. Company & Financial, Sales, Jobs).

The administrator can also control access to data in individual bank accounts. For example, some businesses may have two checking accounts: operating and payroll. The administrator can grant a user access to enter and view transactions in the operating account and prohibit the same user from entering or viewing data in the payroll account register.

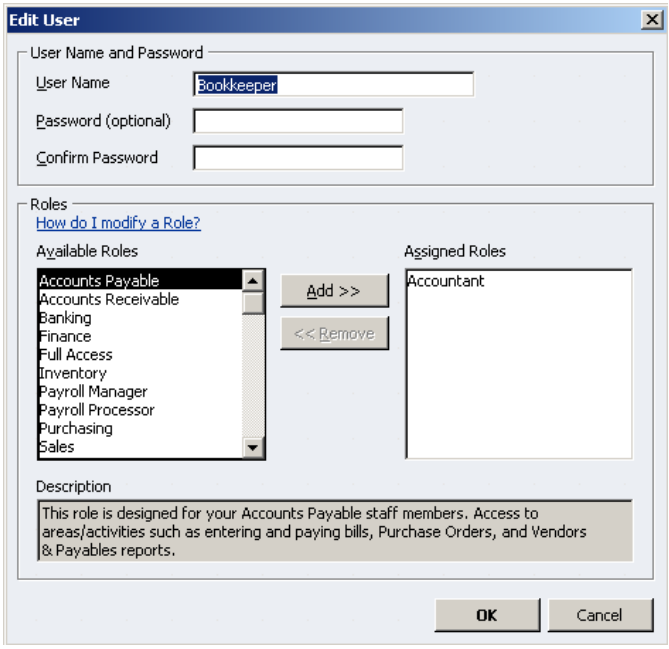

Figure 1, Assigning User Roles

The 14 predefined roles in Enterprise Solutions are:

- Accountant
- Accounts Payable
- Accounts Receivable
- Administrator
- Banking
- Finance
- Full Access
- Inventory
- Payroll Manager
- Payroll Processor
- Purchasing
- Sales
- Time tracking
- View-only

Using roles, you can define a user's permission in extreme detail.

For example, in one area the user may have permission to view information, but not create, modify, or delete. In another area, the same role may have permission to view and create but not modify or delete.

To set up good checks and balances, you need to divide responsibilities and tasks. For example, a recommended practice is

to have one employee who enters invoices and another employee who enters receipts/credits. You should avoid having the same user process both of these transaction types.

If preferred, the administrator can add new roles to the list. In that case, it is advisable to start by duplicating an existing role. Once the role is duplicated, you can modify the duplicate role to suit your specific needs. Using this approach, you leave the existing roles intact but can save yourself work by borrowing permissions from an existing role.

Permissions Access by Users

Areas and Activities	Ann Young	Bookkeeper	John Smith
Accounting	None	Full	None
Asset Accounts	None	Full	None
Edit Closed Transactions	None	Full	None
Equity Accounts	None	Full	None
General Journal	None	Full	None
Liability Accounts	None	Full	None
Manage Fixed Assets	None	Full	None
Working Trial Balance	None	Full	None
Banking	Mixed	Mixed	Mixed
Bank Accounts	None	Full	None
Checks	None	View	None
Credit Card Accounts	None	Full	Full
Credit Card Charges	None	View	Full
Deposits	Full	View	None
Loan Manager	None	None	None
Online Banking	None	None	None
Reconcile	None	Full	None
Transfer Funds	None	Full	None
Centers	Mixed	View	Mixed
Customer Center	Full	V-VB	View
Employee Center	View	View	View
Vendor Center	None	View	Full
Company	Mixed	Mixed	Mixed
Billing Solutions Sign Up	None	None	None
Company Information	None	None	None
Company Preferences	None	None	None
Enter Vehicle Mileage	Full	None	None
Find All Transactions	None	Full	None
Planning & Budgeting	None	Mixed	None
Business Planning & Analysis	None	None	None
Set Up Budgets and Forecast	None	Full	None
Print Labels	Full	None	Full
Remote Access	Full	Full	Full
Set Closing Date & Password	None	Full	None
Set Up Online Banking	None	None	None
Synchronize Contacts	Full	None	None
Customers & Receivables	Full	Mixed	Mixed
Accounts Receivable Accounts	Full	Full	None
Assess Finance Charges	Full	None	None
Billable Time and Costs	Full	None	None
Change Item Prices	Full	None	Full
Credit Card Refunds	Full	View	None
Credit Memos	Full	View	None
Estimates	Full	View	None

Figure 2, Permissions Report

After you set up roles in Enterprise Solutions, you can create users. When you create a user, you assign a role and a password to the user. You can create, edit, and delete users as necessary.

Once your permissions are set up, you can print a very useful report on the permissions granted to each user. Using this report will help you identify modifications you want to make to any given role. The report lists all the areas and activities in QuickBooks Enterprise Solutions for which you can assign permissions, along with a column for each user and that user's permission for each area.

Always-on Audit Trail

Another means to detect fraud is the always-on Audit Trail in Enterprise Solutions. The software automatically tracks all the additions, deletions, and modifications made to transactions in the Company data file. This record of tracked changes—the Audit Trail—ensures that an accurate record of your financial data is maintained.

The Audit Trail tracks any change to a transaction that impacts financial reports (including classes and jobs) as well as any change that impacts management information such as names, dates (including shipping dates and aging) or bank reconciliation detail.

If you change any of the information in the list below, the change will create an entry in the Audit Trail:

- Transaction date
- Document number
- Payment terms
- Sales rep
- Shipping date
- Modifying user
- Account
- Class
- Associated name
- Amount
- Quantity
- Unit price
- Item
- Payment method
- Due date
- Reconciliation status
- Posting status
- Billed date
- Transaction type
- Line-Level discount information

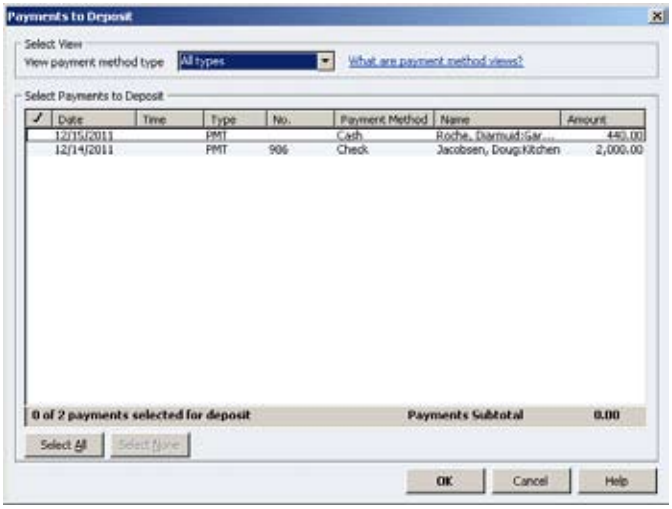

Figure 3, Undeposited Funds Account Detail

Undeposited Funds Account

In addition to roles and permissions and the Audit Trail, Enterprise Solutions offers many other ways to detect fraud. For example, it automatically adds an Undeposited Funds account to your Chart of Accounts the first time you receive a payment for an invoice or enter a sales receipt. Enterprise Solutions uses this account to hold money you've collected from customers until you deposit it in a bank account.

In Enterprise Solutions, you can use the Undeposited Funds account as the default. If you set your Sales and Customers preferences to use the Undeposited Funds account as the default "deposit to" account, then any payments you receive from customers will automatically go into this holding account until you deposit the payment into a bank account. The Undeposited Funds account acts as a holding account, similar to holding money in a drawer, until you make a deposit to your financial institution.

As you use the Undeposited Funds account, remember to divide the tasks associated with payments and deposits between employees.

For instance, one user should be assigned to process customer payments and another user to enter deposits. As mentioned earlier, this separation of duties is a key way to prevent fraud.

Monitoring the balance in this account is also important. The Undeposited Funds account should contain only a "normal" business cycle of money. That means:

- If your business makes deposits daily, then only one day's worth of deposits
- If your business makes deposits weekly, then only an average of one week's deposits.

This account is a key management control, as you can always look for that "normal" amount of money to be in this account. Monitoring this account can help you find different types of fraud and also accurately record customer payments and deposits.

Closing Date Password

In addition to the controls mentioned, Enterprise Solutions offers other ways to monitor changes made in your accounting system. With Enterprise Solutions, you can set a closing date and password to prevent and/or monitor changes to prior periods. You can prevent changes to prior periods in two easy steps:

- Select the closing date, such as end of a period or end of a fiscal year
- Set a closing date password to prevent changes to a closed period

Also, you can edit user access to protect the closed period.

You can use Enterprise Solutions to print a report that lists any changes that were made in the prior period. You can choose from two different formats: by Account or by Transaction Date.

Figure 4, Set a Closing Date and Password

Figure 5, Closing Date Exception Report

Closing Date Exception Report

One of the key reporting tools in Enterprise Solutions that will allow you to detect fraudulent activity is the Closing Date Exception report. You can track changes made to transactions and quickly find errors by using the Closing Date Exception report.

In QuickBooks, the administrator can choose to close the books at the end of each year, each quarter or even each month. For each QuickBooks user, the administrator can then restrict access on three levels: 1) The administrator can prohibit users from entering, modifying or deleting transactions in the closed period, or 2) the administrator can require a special closing date password for a user to enter, modify or delete transactions in the closed period.

If preferred, the administrator can remove the password or change it. The Closing Date Exception Report would reveal the details of any changes made on or before the closing date. This could potentially detect fraudulent activity, such as a change in a transaction amount or the void or deletion of a transaction. Like the Audit Trail Report, the Closing Date Exception Report identifies the name of the user who entered, modified or deleted each transaction with a date and time stamp.

Previous Reconciliation Reports

Another key way to detect fraud is to keep accurate banking reconciliation reports and carefully review your reconciliations. Enterprise Solutions allows you to prepare Previous Reconciliation reports. These static Previous Reconciliation reports (stored as Adobe Acrobat PDF files) show the exact detail of your cleared and uncleared transactions that you marked when performing bank reconciliations. This report can be coupled with the Reconciliation Discrepancy report that allows you to track all of the changes your users make to reconciled transactions.

This is important for internal controls, because the person doing the bank reconciliation should be different from the users/employees

who enter cash disbursements (e.g., checks, bill payments, sales tax payments, paychecks, and payroll liability payments) and banking deposits—especially for deposits that contain customer payments.

If there are fraudulent activities around the disbursement of cash, the user performing the bank reconciliation will be in a position to detect this fraud. If users attempt to modify transactions that a user reconciled—after the reconciliation is completed—their changes will post to a very specific report. Also the beginning bank balance on the bank reconciliation window will no longer tie to the bank.

The person doing the bank reconciliations can refer to the static reports to show that the accounts did indeed tie to the bank at the time of the reconciliation. The company can use a combination of the static bank reconciliation reports, the Previous Reconciliation Discrepancy report, the Voided/Deleted Transaction report, and the Audit Trail report to locate the exact actions of the fraudulent users and which user performed the action.

Company Preference Settings

Many company-level Preference settings in Enterprise Solutions help to protect your business from fraud. One preference to pay particular attention to is "Save all transactions when printing."

By ensuring that all transactions are saved when printing, you can avoid specific types of fraud. Here's an example of how fraud could occur if a user/employee could print a transaction without saving it:

> An employee could create and print an invoice to a customer, and then send it (or hand it) to the customer, but never hit "save" in QuickBooks Enterprise Solutions. So when the customer pays the business for the services or goods, there is no record of the transaction anywhere in the financial management software. The employee can then pocket the money, and the transaction goes undetected.

The upside is that QuickBooks always saves paychecks as they are printed. But for other transactions, such as invoicing, the Save When Printing feature has to be specified as a Company Preference in the software.

Voided/Deleted Transactions Report

Enterprise Solutions also gives you a Voided/Deleted Transactions report. You can use the Voided/Deleted Transactions Report to easily review changes and detect errors. This report is similar to the Audit Trail, but shorter and somewhat easier to use.

This is an important report as it deals solely with voided or deleted transactions. This report can help shine a light on devious activity, as deleting a transaction should be a rare occurrence in your accounting system and is a common activity associated with fraud. If you notice that a particular person has deleted multiple transactions, take note and investigate.

For example, here's a real-world fraud case that involved an employee who modified deposits to steal money owed the business:

> This particular business provided music and art lessons to students. The employee would accept a customer payment, and then post the payment to the customer account. The employee would then enter a discount on the Receive Payments window offset to some catch-all account such as Opening Balance Equity, an account that has a significant overstated or understated balance for most companies. Cost of Goods Sold and income accounts carry large balances, too, so employees may try to bury activity in the detail of those accounts as well.

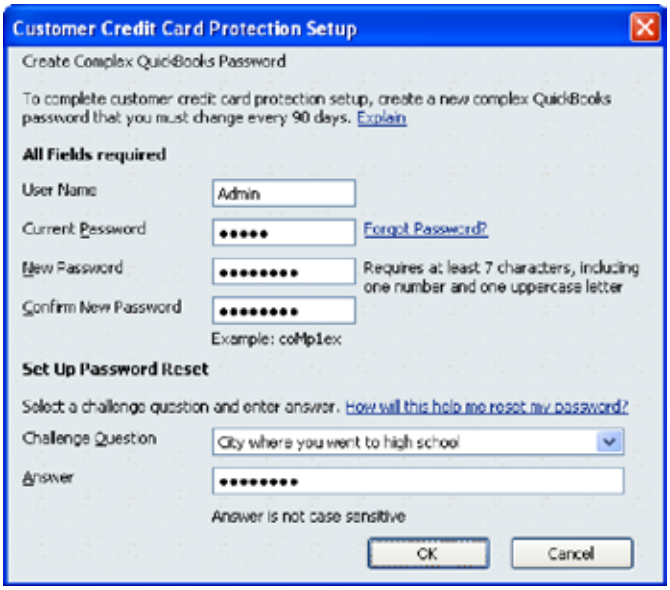

Figure 6, Customer Credit Card Protection

Customer Credit Card Protection

Enterprise Solutions allows you to protect not only your business finances, but other important information such as your customer's credit card numbers. The software gives you several layers of customer credit card protection, which include using complex passwords to access credit card numbers. It also includes a new report, the Credit Card Audit Trail report that tracks usage, including the viewing, of customer credit card numbers.

If you process credit cards using QuickBooks Merchant Services or if you store credit card information in the Payment tab of the Customer Setup window in QuickBooks, you need to comply with security standards governed by the PCI DSS (Payment Card Industry Data Security Standard). Failure to do so could result in severe fines if the credit card information should fall into the wrong hands.

The QuickBooks Customer Credit Card Protection feature requires the QuickBooks administrator user to enter a complex QuickBooks password that is at least seven characters and includes at least one upper-case letter. To comply with PCI DSS, QuickBooks will prompt you to change the password every 90 days.

When you select the Company drop-down menu and then select Customer Credit Card Protection, QuickBooks displays the window in Figure 6. When you setup the more complex password, you also enter a challenge question and answer.

Note: You can set up complex passwords for additional users with access to credit card information. However, you cannot use the QuickBooks Customer Credit Card Protection Feature to regulate the passwords for these users. Instead, the administrator can either reset each user's password or can set an office policy requiring users to change their passwords every 90 days—to comply with PCI DSS.

The Customer Credit Card Audit Trail tracks each time a QuickBooks user enters, displays, edits, or deletes credit card information. The report also tracks each time a QuickBooks user makes changes to the QuickBooks Merchant Services subscription. Only the administrator can view the Customer Credit Card Audit Trail, and QuickBooks does not allow you to filter or memorize the report. Also, the Customer Credit Card Audit Trail is available only if you enable the Customer Credit Card Protection feature.

Take Action Today

You should now have a better understanding of the many ways you can protect your business against fraud. You have also learned that QuickBooks Enterprise Solutions contains multiple layers of security and access controls that empower you to save your business from costly employee theft and fraud.

By implementing the access controls available in Enterprise Solutions, you can avoid creating an environment that is susceptible to employee theft and fraud. Using the many different security tools available in Enterprise Solutions will also help you keep a watchful eye on the flow of your money.

To learn more about security, access controls, and other key features in QuickBooks Enterprise Solutions, visit http://www.qbes.com or call 1-866-379-6635 to speak with an Enterprise Solutions consultant.

About the Author

Joe Woodard, an Advanced Certified QuickBooks ProAdvisor, is President of Creative Financial Software (CFS) an accounting software consulting practice in Atlanta, Georgia. In addition to consulting with small and mid-sized businesses, CFS provides advisory services to CPA firms and other QuickBooks ProAdvisors across the country. Joe is a national trainer on QuickBooks Software and has trained over 18,000 accounting professionals and end users on QuickBooks over the past 10 years. Recently, the CPA Technology Advisor recognized Joe Woodard as one of the 40 most influential accounting technology consultants under the age of 40 in the country. Visit CFS at http://www.cfsatlanta.com

Footnotes

*"Small Business Fraud Custom Study among Small Business Owners" Conducted for SunTrust Banks/National Small Business Association/Edelman, October 17, 2007 http://www.nsba.biz/docs/fraud_survey.pdf

** "Eight Tips to Prevent Employee Fraud and Theft," Allbusiness.com http://www.allbusiness.com/human-resources/workplace-health-safety-security/3935-1.html

