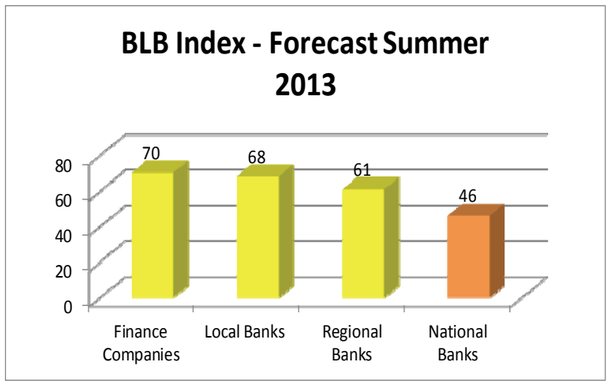
BLB-(Bank Lending Barometer): Lending Picks Up, With Super Low Rates

Lending to small businesses particularly credit worthy customers has sky rocketed in the last three months. Moreover, rates on loans have dropped to levels I have never seen in my career-low 3's. Yes that is correct; I have seen some rates at 3.25% with a 7 year balloon with businesses with good credit. Bankers I have talked to are getting nervous; they fear a torrent of refinances at rates of 5.0% down to this 3.25%. Good credit risks refer to the following: Debt service coverage ratio above 1.30; adequate collateral coverage; good management track record and good credit reports.

Businesses that have fair credit risks can get lower rates too. These fair credit risks can expect rates to be around 5.0%. Also, businesses that have poor credit risks can look for rates in the 6.0 % to 7.0% range. Likewise, finance companies (including leasing companies) are doing deals in the 6% to 7% range.

Bank Lending Barometer



Score	Lending	Description
76-100	Jackpot	Here's the Money! We'll do the paperwork later.
51-75	OK	Let's see what we can do.
26-50	Tight	I would lend you the money, but underwriting is killing most of my deals now.
0-25	Very Tight	I know you have 100% cash pledged for the loan, but we don't have the money.

Gregory A. Barford, CPA, PC
BUSINESS & FINANCIAL ADVISORS

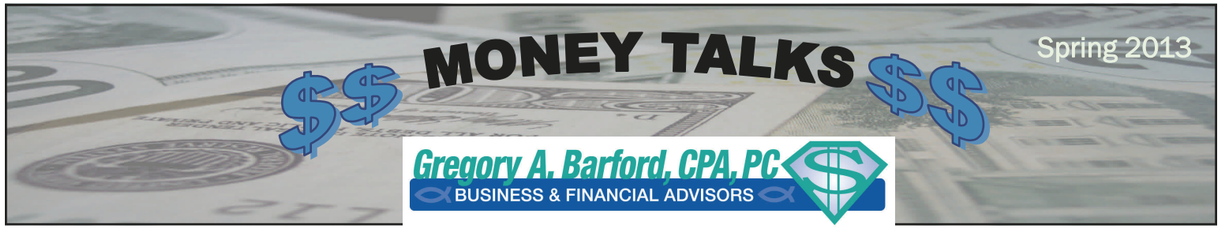
Integrity ... Competence ...Communication ...
Solutions for your business, financial, and accounting needs.
Let's focus on the profit potential of your business!

11801 Fingerboard Road, Suite 11
Monrovia, MD 21770
Phone: 301.865.4648 • Fax: 301.865.0305
e-mail: gab@gabcpa.com
www.gabcpa.com

Publication Information

Publisher: Gregory A. Barford
Writer:: Gregory A. Barford

Money Talks is a controlled circulation publication of Gregory A. Barford, CPA, PC. To get copies, contact the Publisher at (301) 865-4648. All materials in this newsletter are protected by copyright law and cannot be reproduced by any means without the express permission of the Publisher.



INSIDE

Employee Theft & How To Protect Yourself

In the last year, three of our clients were hit by thefts of money by bookkeepers who worked for them. In one of the cases we recovered all of the funds stolen. The other case is in the process of being recovered, and the final case we were called into too late and no recovery of funds is possible. There seems to be a pickup in theft recently. Prior to this year we would run into a theft every 2 or 3 years. In talking with law enforcement officials, employee thefts have been skyrocketing since the 2008 recession began.

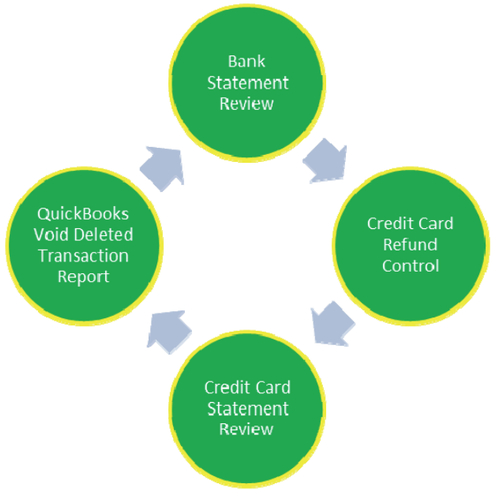
The above mentioned thefts were forgeries dealing with the bank accounts. However, there are other possible thefts of company property that can occur with inventory, supplies and other assets. Therefore, this issue will focus on preventative steps that every business can take to minimize possible losses. In addition, we will make recommendations on the amount of insurance a business should carry for employee thefts. Likewise, we will tell you what steps should be taken when you suspect a theft of assets.

"Now wait a minute here", you are saying. "Greg, don't you look for employee thefts? Why do we need to do this?" Our engagements are not designed to look for employee thefts or weaknesses in your internal control system. The costs to look for these thefts or weaknesses can be expensive. Even in audits that we perform, there is no absolute guarantee that a theft can be discovered. The only sure way to search for theft is to look at every transaction which is time consuming and expensive. Thus, having good internal controls and follow up procedures are good preventive measures.

Most employee thefts are discovered by accident, and it is possible for an employee to take a little bit of money over a long period of time without being detected. If the business owners involved in the above thefts had key accounting safeguards and completed major control checks, the thefts would have been stopped much sooner or may not have occurred at all.

Key Accounting Safeguards

- ☐ Do not use signature stamps or sign blank checks and do not give anyone access to online bill pay through your bank.
- ☐ Use multiple signatures on checks over a certain dollar amount.
- ☐ Do not use a company stamp for the payee line on customer checks. Always have the customer fill this in.
- ☐ Make sure QuickBooks users cannot delete or change existing transactions.
- ☐ Use computer based accounting software for every type of financial transaction. No manual, handwritten transaction systems.
- ☐ Employee dishonesty insurance needs to be at least $50,000 or perhaps more.



Major Control Checks

The point in performing these control checks is to detect fraud and forgeries. In addition, another subtle message is sent to your staff that you are reviewing financial transactions on a regular basis which can discourage theft. These control checks can be done in 1 to 2 hours a month. Your spouse could be a very good person to use for this task. Our firm can also do these activities.

Bank Statement Review

A review of your monthly bank statement before it is given to the bookkeeper is vital. This will prevent the bookkeeper from removing a forged check or debit memo. Look at every single check to make sure it is your signature, the vendor looks familiar, and the amount of the check is reasonable and has not been altered. Signature stamps should never be used for checks. Look for online payments to vendors that are not familiar to you or in multiple payments (multiple online payments to the same vendor might suggest someone's personal expenses).

Banks make it easy to download statements on the computer. However, not all banks download copies of the checks. Most downloads of the checks are a tedious process on line of having to click each check to review it. Contact your bank to have them run your checks on a letterhead page with multiple checks on one page. If the bank cannot do this, consider receiving the statement by mail, even paying for this service. It is that important.

Credit Card Refund Control

Credit card machines have the ability to put through refunds to customers credit cards. Thus, it is also possible for an employee to put through their own credit card refund through the machine. I have seen at least two cases in the last few years of this, and I suspect that this may be more of an issue. In most business I go to and test this feature, the refund goes right through. A simple solution here would be to password protect the machine to issue refunds. The person who signs the checks should be the person to enter the password in the credit card machine. Also, review your credit card merchant statement and look at the refunds issued and make sure the staff can provide supporting detail.

Credit Card Statement Review

The popularity of purchasing products and services via credit card continues to grow. However, the controls to account for these transactions do not exist to a large extent. Moreover, virtually all businesses have good documentation to support writing checks. Writing a check and charging on a credit card have the same result – the bank account is decreased. Therefore, the same controls need to apply to both. Every credit card charge needs to be supported by an invoice from the vendor and reconciled to the credit card statement every month. Moreover, each charge needs to be entered into QuickBooks separately and reconciled every month.

QuickBooks Void/Deleted Transaction Report

An employee puts in a check to himself, forges the check, and then deletes the check from QuickBooks. Another phony check is entered into QuickBooks to cover up the forgery. There is a report that can be run in QuickBooks that lists transactions that were voided or deleted. Moreover, the report can list the person that actually changed the transaction. Explanations need to be obtained for any voids or deleted transactions.

Suspicions of Theft

The first thing to do when you suspect theft is to contact our office. Secondly, do not mention to anybody there was a theft or accuse anybody of theft. We will gather information and document the theft properly so that the police can press charges and obtain recovery from banks and insurance companies. Police do not like to investigate thefts from businesses and will only pursue the perpetrator when it is laid out to them on a silver platter. We had one prospective client that pursued the theft on his own and did a poor job of presenting the information to the police, and the police would not press charges. In most cases, we get the police to press charges for cases involving theft of money and credit card refunds and charges.

Once the proper evidence is gathered, a decision has to be made whether to prosecute or recover the money from the person who committed the theft. If a bank or insurance company will reimburse the theft in full, prosecution needs to occur. If no recovery is available from the bank or insurance company, consideration needs to be given to confronting the employee with the theft and give the employee the option of paying the company back in full or face the full force of the law. We have recovered two large sums of money from ex- employees using this option. It is amazing how these ex-employees can come up with this money. The employee in any case has to be terminated no matter what; no second chances for theft.

Other Types of Theft

Two of the other types of common theft are cash sales and inventory. One of the problems with cash sales is that the transaction might not get rung up at all. A customer paying with cash, and no receipt is given to the customer, can be fertile ground for the employee to take the cash and put in their pocket. Moreover, a little bit of cash taken over a long period of time is hard to catch. A camera system is a good tool to have here that looks over the register. Periodic reviews of the camera tape can help to insure that employees will think twice about stealing cash. Many retail businesses have significant amount of cash shorts at the end of the day when the register is closed out. It is important to track down why these shorts occur and eliminate them. It is amazing how moving one person off the register can eliminate cash shorts.

Theft of inventory is another potential area of employee theft. Having a good perpetual inventory system works well here (perpetual inventory is a computer based system that says you should have 12 of an item on the shelf and when you go count that item there is 12 on the shelf). This perpetual system will show when you have a shortage of product. Tracking down the theft here is a little more challenging to determine which employee or customer is taking the product. Camera systems can be of some help here. However, I have found the best source of information of who may be stealing inventory are other good employees and customers. Over the years my clients have gotten calls from their customers telling them a certain employee was trying to sell them product at discounted prices outside of the business.

Other Analytical Tools

The best analytical tool I found to spot potential theft areas is to run a profit and loss report and look at each expense as a percentage of sales. For example, if sales are flat and margins have not changed and inventory levels have not changed; why would purchases as a percentage of sales go up from the previous period? I have observed that if transactions are coded accurately in QuickBooks, the expenses as a percentage of sales is very predictable. We have had two cases in the last few years where the expenses percentage were slightly out of line, and it was determined that the employees were stealing supplies.

Obama Care Insurance Update 2014

Regulations are still being written for health care coverage for businesses that have more than 50 full time employees. The employer is going to have to contribute a certain percentage towards employees health care coverage or pay a fine. These regulations may be finalized at the end of the summer into the fall. It is not yet clear. Moreover, there could even be a one year delay in the implementation date. We will keep you updated.