

Employee Theft: How to Keep It Out Of Your Business

by Virginia Davidson Hearey
Calfee Halter & Griswold LLP.

Employee theft robs businesses of billions of dollars a year, primarily through check writing, deposit, cash skimming and false invoice schemes. Half of frauds are discovered by a fellow employee by accident, another third by internal whistleblowers. More than 80% of frauds are discovered from within, yet less than 10% of small businesses have anonymous fraud reporting systems or policies. Less than one fifth conduct surprise audits or anti-fraud training.

Who commits fraud?

You have heard it before: the embezzler in your midst is the person you least suspect. Trust ("We treated her just like family"), opportunity (access to cash and checks) and rationalization ("just this once" becomes a way of life) combine to create a powerful temptation.

Pay attention to the employee who:

- › refuses to take vacation, seldom leaves his desk, or hoards data;
- › feels unappreciated. Management "owes" her, and she will extract her due by other means;
- › lives beyond her means; why does your bookkeeper wear \$500 shoes?
- › endorses paychecks to a third party or commercial check casher;
- › through no fault of his own, suffers financial hardships caused by layoffs, health crises or family dependents.

[back cover >>](#)

PROGRESSIVE INSUREDS SHARE \$5 MILLION IN PROFITS

Total Distribution Tops \$63.5 Million Since 1991. Banks that are ABA members and insured by Progressive automatically become owners in the American Bankers Professional and Fidelity Co., Ltd (ABPFIC) and receive profit-sharing checks based on the program's successful results. "Our program is the only one of its kind that distributes profits directly to member banks," said ABPFIC Chairman John Manor. "True to the mutual concept, ABPFIC members benefit from their company's profitability. That is a major achievement for our company and a valuable benefit for ABA members."

E-COMPLIANCE TRAINING AVAILABLE

More than 23,000 bank employees are now enrolled in online courses offered through ABA's free Frontline Compliance Training Program. The members-only program, launched in the fall of 2007, leverages ABA's existing e-learning infrastructure and compliance expertise to address a challenge many bank CEOs share: training staff in order to ensure bank compliance. The program includes over 70 courses, as well as printable reports on all completed training that banks can provide examiners. To learn more about Frontline Compliance Training or to sign up for a free Webinar on the training, go to www.abafrontline.com.

SIGN UP FOR ABA BANK RISK NEWS E-BULLETIN

Security officers, compliance officers, branch managers or any senior executives of ABA-member banks concerned with issues of fraud, theft, robbery, identity theft, electronic intrusion or other such issues may receive, free, this monthly summary of useful information, tips and case studies. ABA members can simply go to www.aba.com and click on ABA E-mail Bulletins and follow the instructions. Or call 1-800-BANKERS.



The Best Defense Against Check Fraud: Training

[see insert >>](#)

We know community banks.



For more loss control information or to view this SafeTalk[®] newsletter online, visit banks.progressive.com.

Coverages are provided by Progressive Casualty Insurance Company, Mayfield Village, Ohio and may not be available in all states. Coverage descriptions were prepared for educational purposes only and are not a guarantee of coverage. Please consult the respective policies for complete descriptions of coverage.



After the 9/11 attacks, the Federal Reserve cut interest rates in order to spur the economy, which was already in the midst of a recession. This response helped generate a housing boom that banks, investors, and homeowners greatly benefited from until 2006. Over this period of time, an artificial increase in home values was created, which encouraged more investment and growth in this market. Moreover, non-conventional mortgages, such as interest-only and ARMs (Adjustable Rate Mortgages) became more common in the marketplace. These trends continued to go unchecked until the market began to collapse in 2006. Fortunately, the majority of our community banks did not engage in these risky practices. Nevertheless, many banks are experiencing spikes in past due loans as a result of the rippling economic effects of the collapse.

The housing market collapse began with the meltdown in the subprime mortgage market, which led to an unfolding of events that burst the so-called “housing bubble” that most of the country experienced. Suddenly, subprime borrowers could no longer afford to make their mortgage payments once the ARMs reset at a higher rate. The market quickly unraveled. Eventually, these same problems plagued even prime borrowers and housing prices plummeted. The housing bust has even affected banks that upheld more conservative underwriting standards, since many regions in the United States are also experiencing economic problems that extend beyond the housing market. As a result of the combination of these factors, many banks have experienced an increase in past due loans, which have resulted in an increasing number of foreclosures. Consequently, these banks may also face a greater chance that their borrowers will sue directors, officers, and/or employees of the bank, and/or the bank itself. It is expected that lender liability lawsuits alleging claims such as those for predatory lending, deceptive trade practices, truth-in-lending violations, etc. will be on the rise this year.

As a banker, you may be asking yourself what you can do to avoid being the target of lender liability suits.

The recommendations below are based on claims that we have experienced over the years.

► **Exercise Proper Oversight.** Overall, lax standards led to the rise and fall of the mortgage market. A combination of deficiencies, including the lack of oversight of mortgage brokers, the lack of financial documentation (like borrower’s proof of income), and more relaxed underwriting, created an “anything goes” type of environment. The end result of these factors allowed many borrowers who did not have the means to make long-term payments secure mortgages at higher levels than they would have ordinarily qualified for. In retrospect, it is easy to see how this environment would eventually collapse. These events can now serve as a reminder to banks and other lenders that proper controls are essential. Remember that the five “Cs” of credit are an integral tool to use during the underwriting process:

1. **Capacity.** How is the borrower going to repay the loan? It is important for lenders to appropriately verify the borrower’s income and other sources of cash flow since this serves as the primary source of repayment. Some lenders did not adequately review their borrowers’ sources of income, which helped lead to the problems the industry is facing today.
2. **Capital.** How much capital does the borrower have? This review should consist of analyzing the borrower’s personal net worth, plus equity in the property. A higher net worth individual will obviously be able to handle loan payments better in the event of a reduction in income. Equity is also important because a higher amount of equity correlates to an improved chance that the loan will be paid.
3. **Collateral.** What is the value of the real estate? Banks must rely on appraisers for this information, so it is important that the appraiser be independent and use reliable data. During the housing boom, many appraisers purposely inflated real estate values, so it is crucial that banks thoroughly examine their independent appraisers. Additionally, lenders should ensure that their loan to value ratios are reasonable and also consider the possibility of fluctuating housing values.
4. **Conditions.** What are the events surrounding the loan? Bankers must consider external factors, such as the overall local economy, housing market, etc. This “C” has had a profound impact on how the banking industry has operated given the mortgage collapse and other economic issues that our economy is facing. Banks must be careful and weigh this factor against the other four “Cs” because, in retrospect, it appears that some lenders focused more on this area and not enough on the others, which helped precipitate the market collapse.
5. **Character.** Is the potential borrower a good loan candidate? An analysis of the borrower’s employment and credit history should be conducted to help determine the likelihood of repayment. Since this is the most subjective area of the five “Cs,” it is important for lenders to know their customers.

The bottom line is that it is essential that lenders maintain good documentation across the board and make prudent decisions.

- **Beware of using teaser rates.** Over the past few years, many lenders have attracted borrowers by using teaser rates, which are typically below-market interest rates designed to entice consumers. While this may be a common technique among competing banks, it does increase the lender liability potential dramatically because teaser rates can be considered misleading and even deceptive if rate changes are not properly disclosed to borrowers.
- **Educate borrowers.** Consumers need to understand the financial implications when ARMs reset. In 2007, in an effort to promote consumer education, the federal financial regulatory agencies introduced illustrations on ARMs for

Wire Transfer Coverage – Do Not Forget Your Bond Requirements

by **Amber Brown**, Senior Underwriter

In this age of information technology, most banks regularly allow customers to fax, phone or e-mail funds transfer requests in order to provide them with immediate access to funds. Financial institutions are governed by several doctrines, including the Uniform Commercial Code and the Federal Reserve's Regulation E, which outlines the financial institution's responsibilities in executing funds transfer requests.

For example, under the UCC, Section 4A-201 defines the required security procedures and Section 4A-202 outlines the authorization and verification duties of both the bank and the customer.

Regulatory agencies also routinely review wire transfer controls as part of the examination process.

The purpose of this article is to remind banks of the bond carrier's requirements for wire transfer coverage.

Like the regulatory agencies, all bond carriers have some type of control requirement in place in order to trigger fraudulent wire transfer coverage. Many carriers require banks to perform call-back verification for wire transfers over a specified amount and some carriers even require that the call-back be recorded. Most, if not all, carriers also require that banks have wire transfer agreements in place with each customer for certain wire transfer requests.

Progressive's computer systems coverage requires that a written agreement be in place for transfer requests received by fax, phone or e-mail, which allows the bank to rely on such

instructions. This agreement must also include the names of persons authorized to make these requests.

Furthermore, the bank must have an established instruction verification mechanism in place. This can be accomplished through the establishment of a PIN, password, or similar type of security mechanism.

Lastly, banks must verify wire transfers over \$100,000 by a call-back according to a prearranged procedure.

Although this is not an insurance carrier requirement, funds transfer agreements should also address other areas of contractual obligations, like funds availability, insufficient funds, errors, etc., in order to establish the liability of both the bank and the customer. The agreement will serve as a contract and, therefore, should comprehensively address all aspects pertaining to the wire transfer.

Ultimately, the contract will be referenced in the event there is a dispute involving a wire transfer, so it is important to have a strong agreement in place.

Proper wire transfer controls will produce immeasurable benefits, including improved trust between your bank and your customers. Without strong controls in place, a fraudulent wire transfer could be executed which may weaken the customer's relationship with the bank. The customers would suffer from the financial devastation of getting funds stolen from their account. This event could cause the customer to place blame on the bank, which in turn, could lead to costly litigation and damage to the bank's reputation.

At the end of the day, good controls will benefit both your customer and your bank by acting as a safeguard against fraud.

About Amber Brown, Senior Underwriter: In addition to over 3 years with Progressive, Amber was a bank examiner for the Federal Reserve. For questions or information, Amber can be contacted at 800-274-5222 or amber_m_brown@progressive.com.

Meet Mike Poremba, Progressive's On-Site Review Specialist



Mike has been with Progressive's Professional Liability Group for over 20 years, wearing many hats: from underwriter to loss control specialist to on-site review consultant. He has conducted over 500 on-sites in his 20 years! Recently, his responsibilities are system administration/design and monitoring of our insured banks' financial condition using quarterly call report information.

Mike graduated from John Carroll University with a degree in finance in 1979 and the Stonier School of Banking in 1993.

Prior to joining Progressive, Mike was a Commissioned National Bank Examiner with the OCC. He spent three years at BankOne Cleveland in the loan review department. In his spare time, Mike rides mountain and road bikes.

Mike knows community banks.

Mortgage Meltdown Lessons Learned *continued*

financial institutions to utilize as an educational tool for consumers, which make it easier for banks to educate their borrowers. Other methods of consumer education can include one-on-one lending counseling, seminars for first-time home buyers, or other similar programs.

- › **Work with borrowers.** The easiest way to avoid lender liability suits is to work with the borrower before commencing foreclosure proceedings, whenever possible. In 2007, the federal regulatory agencies issued guidance

urging financial institutions to identify and work with borrowers who were at risk of defaulting on their mortgage in order to avoid unnecessary foreclosures. More recently, the government has announced a plan, Project Lifeline, designed to help homeowners and some of the country's largest banks work towards a solution to avoid foreclosures. These arrangements can be an optimal alternative to costly foreclosure proceedings and can ultimately minimize lender liability suits.

Employee Theft: How to Keep It Out Of Your Business *continued*

Trust, but Verify

Simple controls, applied evenly, can prevent fraud from poisoning a successful business. Although no one measure is right for every business, here are some areas to consider:

- › **Background checks.** More than a third of resumes contain false statements, yet less than a third of employers verify that information. Get written permission to check backgrounds. You will learn about criminal and credit histories, prior employment and education, and verify licenses and certifications. A more extensive check is worthwhile for higher level employees.
- › **Whistleblower policy.** Anonymous tips are more effective than audits, especially in frauds of \$1 million or more. A policy should encourage employees to report, and protect their confidentiality. Make sure new hires know about it. Allow reporting to an immediate supervisor or a second person of the employee's choosing.
- › **Audits, inside and out.** Most frauds begin in the weeks after outside CPAs complete their field work and leave the premises. That is when a designated internal auditor should be especially vigilant. The external CPA's job is not to uncover fraud, but to state whether financial statements are materially accurate. As part of that task, however, the CPA must assess risks, advise as to internal controls, and report significant concerns. It is better if the auditor's report of any such concerns can say that management has corrected the problem.
- › **Bank records.** Consider having bank statements and checks mailed to a new, trusted location without advance notice. You may be surprised at what you learn.
- › **Check writing and approval.** Require that checks be signed by an officer and a co-signer who neither approves the payment nor works in accounting. Keep up with developments in check paper stock. Number check requests. Ensure that deposits go to the proper accounts. On deposit endorsement stamps, spell out the company's full name and omit bank name and account number. Keep checks and deposits under lock and key, and process them promptly.
- › **Cash, credit cards and postage meters.** Require a written receipt for every cash transaction. Consider using random shoppers to see if receipts are frequently voided (a fraud indicator). Do not allow employees to obtain postal money

orders. Make sure postal refunds are credited to the proper account. Shred offers for pre-approved loans and credit cards.

- › **Fraud insurance.** Consider a fidelity bond to cover the company, key employees, and anyone who handles money.
- › **Computer data.** Back it up daily and store it off site.
- › **Outside vendors.** Inventory and supplies are areas ripe for collusion. Reconcile purchase records. Have personnel in more than one department review your company's choice of vendors from time to time. Establish a written conflict of interest policy and require signed certifications of compliance.
- › **Bad debt write-offs.** Keep an eye on upward trends
- › **Mandatory time off.** No exceptions.
- › **Expense accounts.** Establish controls that make sense for your business, and audit them.
- › **Exit interviews.** Schedule them close to departure. Have someone other than the employee's supervisor find out why the employee is leaving, where she is going next, and how she feels the organization can be improved.

If You Uncover Suspicious Activity

Before confronting anyone, get the facts. An attorney, working with a forensic accountant, can quickly and economically freeze accounts, save computer, voice mail and documents, and minimize damage. An independent adviser protects the company's officers from becoming witnesses in any later investigation, and can help you communicate with your employees, the government and the press. Notify your insurance carrier.

If you must question an employee, do it after hours, with a witness present. Depending on the circumstances, you may want a law enforcement officer present. Retrieve any company property.

Done correctly, an immediate investigation can mean the difference between a quick recovery and years of playing expensive catch-up. Fraud in the business world is inevitable. Disproportionate costs of getting back to business are not.

Virginia Davidson Hearey is a partner in the firm, Calfee Halter & Griswold LLP, and serves as chair of the firm's White Collar Defense and Investigations practice. The practice represents and counsels publicly held corporations, public bodies, boards, committees and individuals in federal, state and local investigations, criminal, regulatory and civil prosecutions, and compliance reviews.

The Best Defense Against Check Fraud: Training

Train, train and train again. The importance of continuous front-line training cannot be overemphasized, particularly in light of the high turnover associated with tellers. Tellers who are inadequately trained simply become check processors; educating tellers so they feel they are part of a team to combat check fraud may improve retention rates and increase job satisfaction. The individuals who work in the backroom operations encoding, sorting, sight reviewing and processing checks must also be educated on steps to counter check fraud. Finally, customers, both consumer and corporate, must be educated as to their responsibilities with respect to check fraud.

TELLER TRAINING

Before launching into the specifics of a good teller training program, two concepts should be noted as part of an overall check fraud/teller training program.

First, all new tellers should be assigned a mentor.

The best person for this role would be a teller who has been with the bank for some time and is very familiar with policies and procedures. This person should not only help the new teller learn how to do things, but explain why they are doing things in a particular manner. If tellers know why a particular policy or procedure is required, it will encourage them to think about the policies and procedures in place and to offer suggestions for improvement.

Second, all tellers, not only new tellers, should have a "go-to person."

This person should also be a very experienced individual who has decision-making authority. When a teller's suspicions are raised, he should have someone to go to for advice and who will deal with a customer if the customer becomes angry or demanding. Emphasize to tellers that taking suspicions to the "go-to person" is not frowned upon, but rather, is encouraged. This helps foster an environment where all employees of the bank have a responsibility for, and take interest in, detecting fraud and preventing losses.

Tellers should first be trained on the characteristics of a good check.

If they do not know the characteristics of a legitimate check, they will not be able to spot a bogus one. The following are just some items that should be explained in the training process:

- ▶ Explain what the numbers and symbols in the MICR line represent.
- ▶ The bank address printed on the check should always correspond to the appropriate Federal Reserve District for that bank. The first two digits of the routing/transit number in the MICR line indicate the Federal Reserve District. For example, if the MICR line shows the Federal Reserve District as 04 (Cleveland), but the address for the bank listed on the check is Dallas, suspicions should be raised that this could be a counterfeit check. Counterfeiters will often change the routing number for the Federal Reserve District Office contained in the MICR line so as to delay the processing of the check. This delay allows the criminal to obtain access to the funds before the check is returned as a counterfeit.
- ▶ The check number contained in the MICR line should correspond to the check number in the upper right-hand corner of the check.
- ▶ There are fractional routing numbers contained in the top right-hand corner of checks. The four-digit number on the bottom of the fraction corresponds to the Federal Reserve District number where the check was issued. This number should correspond with the Federal Reserve District number contained in the MICR line.
- ▶ Most checks contain a perforation on at least one side. Tellers should be instructed to look for perforated edges.
- ▶ The numerical dollar amount contained on the check should match the written dollar amount.
- ▶ The check should not be postdated or stale. If so, it would be appropriate to return the check to the customer.

After training tellers on the elements of a good check, train them on other common warning signs of check fraud.

While this list is not exhaustive, some of the more common warning signs are:

- › A check does not have an MICR line at the bottom.
- › The MICR ink feels raised or appears shiny. Magnetic ink is used in the printing of MICR lines. That type of ink is dull and produces images that are flat on the paper, rather than raised and/or shiny.
- › The name and address of the drawee bank is typed rather than printed. Tellers should also check for spelling errors in this area.
- › No printed drawer name and address or a typed name and address.
- › Checks containing indications of erasures, whiteout, alterations or eradications.
- › Checks printed on poor quality paper, which does not resemble legitimate stock paper.
- › Check paper that feels slippery.
- › Check colors that are smeared when rubbed with a moist finger.
- › Checks which contain the word "void" anywhere on the check. Certain check stock will cause this word to appear when the check is reproduced on a copier.
- › Checks which state on the back that they contain certain security features such as watermarks or microprinting. If so, the teller should examine the check for those security features.
- › Checks that are marked "non-negotiable." Such checks are often used in promotional mailings by mortgage companies or finance companies. The teller that is not paying attention to the check, but is simply a check processor, can easily overlook this.
- › The handwriting contained on the payee line is different from the handwriting on the remainder of the check.
- › Something has been added to the check. For example, a check which was originally made payable to one payee may have been altered to make it a joint payee wherein the check can be paid to either payee.
- › The check is payable to a corporation and is either being deposited into an individual's account or being cashed by an individual.
- › Third-party checks. The "go-to person" should always be consulted prior to the teller cashing a third-party check. Frequently, dishonest corporate bookkeepers will intercept checks payable to the corporation, forge the corporation's endorsement, add their own endorsement and deposit the checks into their account. They will utilize different tellers or ATMs for their deposits. Accordingly, it is critical that the backroom personnel be notified so that the account can be monitored to determine whether check fraud is occurring.

Tellers should also be trained on these guidelines for cashing checks:

- › If a teller does not know the customer, personal picture identification should be mandatory. Two forms of identification should be required, as falsified picture identification can easily be obtained.
- › Tellers should be cautious of new customers performing split deposits (depositing a check and receiving a portion of the proceeds back in cash). This is very typical of a fraud scheme.
- › When cashing "on us" checks, tellers should verify that the account on which the check is drawn has sufficient funds and is not a dormant account or flagged for any other reason.
- › Tellers should verify that there is not a stop payment order issued on the particular item.
- › The teller should be trained to be wary of individuals that attempt to distract them while they are reviewing the check. Individuals that attempt to pass bogus checks want the checks scrutinized as little as possible. If the person becomes demanding or unruly, the teller should be instructed to seek assistance from the "go-to person." If the check is bogus and the teller takes that action, the individual will most likely leave the bank.
- › Finally, tellers should be instructed that if they have any suspicions whatsoever, further inquiry is necessary and the "go-to person" should be consulted. It is also important to note that under Regulation CC, additional holds on an item are permitted if there are suspicions as to the validity of the item.

BACKROOM EMPLOYEE TRAINING

Backroom employees must also be trained to detect fraudulent checks. They should receive the same training on the characteristics of a good check as was suggested above for tellers.

If a check kicks out in processing because the MICR line is unreadable, they should be trained to examine the whole check and not simply repair the line.

If suspicions are raised because of the characteristics of the check or the dollar amount, further steps should be taken to verify that the check is legitimate. For example, if the check is "on us," the backroom personnel should be instructed to do more than simply compare the makers' signature against the signature card; they should look at the check as a whole. The same policy and training should hold true for site review/signature verification personnel. The check in question should be compared against low dollar amount checks drawn on that account on that same day or the previous day to determine:

- › Are the colors and type fonts on the checks identical in appearance? A counterfeit check will most likely have a slightly different color or design from the rest of the checks in the batch.
- › Are the check numbers and issue dates in the same range?

