

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?

› Is the check paper similar?

› Are all the characteristics of a legitimate check present?

Once tellers and backroom personnel have been trained, there is more training to do.

CUSTOMER TRAINING

Customers - both consumer and commercial - should be part of the arsenal to combat check fraud. Training should explain to customers the various types of check fraud, the magnitude of the problem, their exposure to loss, and actions they can take to prevent fraud. Such training can take place through brochures that are mailed with account statements or are conveniently located throughout the bank. Bank personnel should also be encouraged to speak at local organizations such as Chamber of Commerce or Rotary Club meetings, as well as to personally visit and educate commercial customers.

With respect to consumer accounts, customers should be advised:

- › Promptly and closely examine account statements. Explain that under the new Uniform Commercial Code (UCC), the bank is not solely responsible for check fraud.
- › Report forged checks immediately to the bank.
- › Report lost or stolen checks immediately to the bank; the bank will assist in notifying third-party databases with respect to the stolen or lost checks.
- › Close unused accounts.
- › Keep all checks and statements in a secure place.
- › Reorder checks only through the financial institution. Buying checks through mail order houses is an invitation for potential fraud.
- › Do not give checking account numbers to anyone.
- › Do not have driver's license or social security numbers preprinted on checks.
- › Verify that a check order is complete when received.
- › Destroy checks from closed accounts.

Commercial customers should be advised:

- › Implement positive pay or reverse positive pay if available.
- › Use highly secured check stock that contains multiple layers of security features.
- › Print checks using large font. Criminals can easily erase words and numerals in small type and cover those erasures with larger font.
- › Avoid using multiple colors and sizes of checks that are to be drawn against the same account. This will hamper the backroom personnel because they will not be able to identify a fraudulent item based solely on the fact that it does not look like other items.
- › Annual reports should not contain the actual signatures of executive officers, as they can be scanned and reproduced on counterfeit checks.
- › Implement hiring practices to filter out people with a history of fraud or dishonesty.
- › Keep all check stock in a secured and locked facility with limited employee access. Cleaning crews should not have access to this area.
- › Reconcile bank statements and promptly report any discrepancies.
- › Implement dual controls so that those responsible for accounts payable are not also responsible for reconciling accounts. Establish dual controls so that new vendors cannot be added to accounts payable systems by one individual. Rotate personnel in financially sensitive roles.
- › Enforce mandatory vacation policies for those responsible for financial assets or record keeping.
- › Physically inventory check stock at least quarterly to account for every check.
- › Encourage direct deposit of payroll to employee accounts.
- › Order check stock from reputable dealers and verify the accuracy of all shipments.

The training set forth above may appear to be a daunting task. Initially it may be. With time, however, it will be refined and streamlined, resulting in less of a burden. Moreover, significant benefits will be reaped.

DEFEND YOUR BANK AGAINST CHECK FRAUD

- ›› Assign new tellers a mentor and a "go-to person."
- ›› Train tellers and backroom employee on the elements of a good check and common warning signs of check fraud.
- ›› Train all staff to be on the lookout for and report any suspicious activity.
- ›› Advise customers to promptly and closely examine account statements and report any issues to the bank immediately.



We know community banks.

Progressive insures over 1,700 banks nationwide. Available coverages include:
Directors & Officers Liability | Employment Practices Liability | Internet Banking Liability | Privacy Liability
Financial Institution Bonds | Excess Deposit Bonds | STAMP Surety Bonds

For more information, call 800-274-5222 to talk with one of our experienced underwriters, or visit banks.progressive.com.