Controlling Embezzlement

By Frank W. Abagnale

"If you make it easy for people to steal from you, they will."

Over the years I have found this simple principle to hold true. If you do not want to be a victim of check fraud, use highly secure checks and Payee Positive Pay. If you do not want to be embezzled, implement internal barriers and conduct regular and thorough unannounced audits.

Embezzlement has ranked as America's Number One financial crime for more than 30 years, and will likely hold that distinction for many years to come. In most embezzlement cases, basic internal financial controls would have prevented or substantially reduced the loss.

Most crimes committed are crimes of opportunity. Following is a summary of the better controls to deter embezzlement. In developing this list of recommendations, I have solicited the comments and experience of John Drew, MBA, CPA and former Executive VP & Chief Practice Officer of Loder Drew & Associates, and current mayor of Providence, Utah; and Greg Litster, president of SAFEChecks and a former 18-year senior-level banker.

Review hiring procedures for permanent and temporary positions to keep people with questionable backgrounds out of your organization. Your procedures should require that references be thoroughly checked, with particular attention paid to dates and any time gaps in a resume. When filling positions in sensitive areas, consider hiring an outside firm to conduct complete background checks. Use bonded temporaries in financial functions. Consider that over 90 percent of embezzlers have never been arrested or convicted of a crime, so a criminal background check will not give you the information you need.

Prevent ghost employees and improperly altered pay rates by restricting access to the personnel master file records. Adding new employees or changing pay rates should also require supervisory approval and supporting documentation. Supervisory reviews and independent audits are essential.

Mailroom personnel must have clean backgrounds. Internal procedures must be established to discourage theft of incoming or outgoing checks. Many companies that have been victims of check fraud from altered payees have traced the source of the original checks to their own mailroom. If your organization is well known, consider replacing the name on disbursement envelopes with a post office box. That post office box should be established specifically and solely to receive checks that are returned as undeliverable.

Protect the accounts payable and procurement functions by restricting access to the vendor master file records. Changing or adding new vendors should require supervisory approval and supporting documentation. All new supplier entries should be reviewed by someone independent of the buying and payment processing functions. The review should always include a telephone call to the supplier using a number obtained from an external directory source, and should include verification of the name, address, and Federal ID number.

Create Audit Trails. Access to the master file records should be password protected and restricted by job function. Computer systems should create an audit trail of all changes made to the master file records, including who made them and who approved them. A report detailing the changes should be printed and reviewed regularly by someone independent of the person or persons making the entries. These reports are sometimes referred to as an "access matrix." A comparison of the access authority of each employee should be part of this review. A standard “access profile” should be determined for each position and master file records restricted to such. Employees that terminate should be deleted from access immediately. Reassigned employees should have their access modified immediately. Any unusual or suspicious activity should be investigated immediately. Most computer systems are designed with these capabilities, but companies rarely utilize them. Programming access reports is not a difficult task.

> *Example:* In a recent case, a major manufacturer caught an accounts payable supervisor who had edited a supplier record in the master file before accounts payable checks were printed. The employee had access to set up and edit records in the supplier master file, but the oversight function was not in place. The vendor’s name had been changed to the employee’s mortgage company, along with a reference to his loan number. The fraud was discovered only after the check was returned by the mortgage company to the manufacturer. Normally, mortgage companies accept large principal payments outside of regular monthly payments only with specific written instructions to do so. Since the employee could not intercept mailing of the payment, a written note was not included and the check was returned.

Separate the accounts receivable and banking functions. Receipts and deposits must balance each day, and the functions should be performed by different people to prevent fraudulent endorsements. Payment processing, check disbursement and bank reconciliations should also be performed by separate groups. If these duties are not separated, a dishonest employee could issue a check to him- or herself or to a co-conspirator, remove the check from the bank statement and adjust accounting records to hide the embezzlement.

Section 3-405 of the revised Uniform Commercial Code (UCC) makes it very clear that employers have sole responsibility to properly manage this area. The UCC adopts the principle that the risk of loss for fraudulent endorsements by employees who are entrusted with the responsibility with respect to checks should fall on the employer rather than on the bank that takes the check or pays it, if the bank was not negligent in the transaction. It is based on the belief that the employer is in a far better position to avoid the loss by care and choosing employees, in supervising them and in adopting other measures to prevent forged endorsements on instruments payable to the employer.

Segregate Processing of Returned Checks. *All checks that are returned by the recipient or by the Post Office as undeliverable* should be given to someone independent from the check disbursement function. Under no circumstances should they be returned to the original processor. An independent person should be designated to handle these returned check exceptions and investigate the reason for the return.

> *Example:* An uncashed disbursement check was returned to an accounts payable clerk for disposition because she originated the invoice entry. The clerk put the check in her desk and forgot about it for several months. Upon cleaning her desk, she discovered the returned check. When she checked the paid history, she realized the supplier had returned the check when it was determined to be a duplicate payment of an invoice. She also noticed that the payee name had been printed slightly below “Payee” on the check. With a bit of effort, she managed to align the check and insert her name above the original payee in a print similar to the original, along with a “or” designation following her name. The fraud was caught by an accounts payable auditor searching for duplicate payments who was asked by the supplier to furnish proof of duplicate payments by providing copies of both cancelled checks.

Never Include Account Number or Authorized Signatures in Correspondence. *Credit application forms* sent to a new supplier should include the name and phone number of the company's account officer at the bank, but not the bank account number. The correspondence should also not be signed by an authorized signer on the account. You have no control over who handles this information once it is mailed or faxed, and it could be used for fraudulent purposes. Supplied with a company's account number and armed with the ability to scan the signature, a forger could easily pass a check that would pay at the bank, even if the amount is large and the bank verifies the signature. Today's banking system is automated and very few checks pass human eyes.

Always Mail Supplier Checks. *Checks should always be mailed directly to the vendor and* <u>*not*</u> *returned to the originating department, division, branch office or requestor.* In many companies, the operations people want to see the check for an invoice or check request. In effect, these people want assurance that a payment is sent, not trusting their accounts payable department. Often we find operating departments that try to maintain their own record of disbursements, duplicating what the accounting system already has created. This duplication of effort is not necessary. The issue is either lack of visibility of payment activity or lack of trust. If this is the problem, a solution should be reached that does not involved returning the check to the original requestor.

Returning checks to the originator can be an open invitation to fraud. I have heard numerous stories of employees who made special arrangements with suppliers that are unethical. These have included exchanging a check for a free lunch, a kickback in some form, or other inappropriate actions involving the supplier-customer relationship. At the extreme, we have seen checks altered to be cashed or deposited by someone other than the intended recipient.

> Example: An employee of a company was caught altering the payee name on checks designated for charitable contributions. Because the charity didn't send invoices and counted only what it received, total when contributions were within budget, nothing was missed.

Return Blank Checks to Secure Storage after Check Runs. *Empty the printer tray of blank checks* after a check run and return them to be secured cabinet. Often there are left-over checks from a prior check run that were not returned to secure safekeeping. Someone from the cleaning crew or another employee might find these checks in the printer tray when authorized employees are absent or after hours, and use them from criminal purposes. This control seems so obvious, yet is frequently overlooked.

> Example: A major apparel maker in a northwestern state recently fell victim to a scam involving the theft of a few blank checks left in the printer tray after a check run. There was puzzlement initially over how the checks had been stolen. A review by an independent audit firm determined the inappropriate practice of checks left in the printer tray as the source of the missing checks.

Eliminate the Use of Self-Correcting Typewriters. *Never use a self-correcting typewriter for manual checks.* There are still organizations that use old-fashioned typewriters to issue emergency or manually generated checks. The black shiny ribbon used in those old, self-correcting typewriters is made of polymer (a form of plastic) and is designed to be lifted off for correction. The polymer can be lifted off the check with Scotch Magic Brand tape without damaging the check surface at all. Employees know when a self-correcting typewriter is being used to issue a check; a dishonest employee may take advantage of it.

> Example: In one situation, after obtaining an authorized signature on a check, the employee inserted the check back into the same typewriter to remove the name and replace it with another name. The fraud was identified when an auditor was looking at cancelled checks and noticed the payee name on the check and the name on the check register were different.

If a typewriter is used to issue checks, it is imperative that the ribbon be a fabric ribbon, not a polymer ribbon. Fabric ribbons contain ink that is pounded into the fibers of the paper and cannot be lifted off. However, the ink can be dissolved in acetone after about three hours.

If a manual check must be issued, the safest method is to hand write the check using a Uniball 207 gel pen. The ink in a Uniball 207 pen cannot be lifted off or dissolved in chemicals.

Safeguard All Unissued Checks. *Safeguard Zero Amount checks and checks to be voided.* The word "Void" should immediately be written or stamped to render the document unusable. All such checks that include a manual or facsimile signature should have the signature removed. These checks should also be locked away until voided in the system. A person other than the accounts payable processor who entered the transaction should handle such checks for voiding. Too often these checks are left on desks or in in-boxes. They are often more "live" than blank check stock and require minimal alteration for someone to commit fraud. Employees know that a replacement check was issued and the check to be voided will likely not be missed.

Destroy Obsolete Check Stock *Obsolete check stock* should be shredded or rendered unusable in some manner as soon as possible. Often, when new bank accounts are opened or when highly secure check stock replaces old checks, boxes of old checks are found sitting outside the locked cabinet where the new checks are maintained. On some occasions they are even stacked in a warehouse on a pallet. The justification often is that there is no concern for checks drawn on an account that has been closed.

Obsolete checks are still negotiable instruments. They are very much "live" checks and must be kept under lock and key until they can be shredded under dual custody. While the bank account the obsolete checks are drawn on may be closed, the checks themselves appear genuine, and are genuine, and the company would be considered negligent and responsible for any loss that came from those uncontrolled checks, especially under the holder in due course provision of the Uniform Commercial Code. Ironically, the new checks that are securely locked up often have the new security features such as what SAFEChecks offers, while the obsolete checks uncontrolled may be more easily forged.

Shred All Negotiable Documents in Dual Custody using a cross-cut shredder, or use a bonded shredder. One person acting alone should not be placed in a position to steal or to be accused of stealing a check that was taken by another.

Frank W. Abagnale is one of the world's most respected authorities on the subjects of forgery, embezzlement and secure documents. For over 40 years he has lectured to and consulted with hundreds of financial institutions, corporations and government agencies around the world, including the FBI.

Mr. Abagnale believes the punishment for fraud and the recovery of stolen funds are so rare that prevention is the only viable course of action