

Fiduciary Dishonesty - Steps to combat Dishonesty in your Organization

One of the most frequent Organization thefts is check forgery committed by the one trusted person assigned to handle all the finances of an organization. This person may commit fraud by:

- Having check signature authority
- Getting blank checks signed by the Organization officer
- Forging the signature on checks
- Alters the check after the Organization officer has signed it

Steps to Combat Dishonesty

An organization suffers dishonesty losses because criminals find opportunities to commit crimes. Risk control measure to prevent losses should focus on deterrence and detection and include the following:

- Institute sound personnel policies
- Institute physical controls
- Institute computer controls
- Institute procedural controls
- Institute managerial controls
- Investigate and prosecute crimes

Managerial Controls

- Establish a climate or atmosphere within an organization that deters crime or assists in its detection.
- Emphasize that dishonesty will not be tolerated and all criminals will be vigorously prosecuted.
- Educate participants about the organization's crime loss exposures, the risk control measures that have been implemented, and the ways participants can reduce dishonesty losses.
- Projecting a tough attitude toward crime to participants can help an organization avoid becoming a target for criminals.

Procedural Controls

The organization officer or the outside accountant should get the unopened bank statements and canceled checks each month and independently review the payees, amounts, signatures, and endorsements on each check.

IMPORTANT NOTICE - The information and suggestions presented by Philadelphia Indemnity Insurance Company in this Technical Bulletin are for your consideration in your loss prevention efforts. They are not intended to be complete or definitive in identifying all hazards associated with your business, preventing workplace accidents, or complying with any safety related, or other, laws or regulations. You are encouraged to alter them to fit the specific hazards of your business and to have your legal counsel review all of your plans and company policies.



- Require checks to be countersigned by two responsible officials for amounts over \$500.00.
- Limit the endorsement of checks, by anyone other than the owner / officer, to deposits for credit only.
- Delegate the responsibility for receiving checks and cash to someone other than the person who records incoming funds.
- Mail statements to outside accounts (if applicable) directly at least monthly.
- Make sure employees responsible for ordering goods and supplies are not the same ones responsible for receiving them or paying for them.
- Do not give the person who has the authority to write off bad debts the authority to make a credit sale or loan.
- Divide financial responsibilities and functions so that no one person controls all aspects of a transaction.
- Consider rotating employees who jobs involve substantial opportunity for employee theft.
- Conduct regular, unannounced audits by both internal and external auditors.
- Key control program should be implemented. Maintain records of participants who have keys with duplicates prevented by controlling the master.
-
- Restrict access to computer files so only authorized personnel have access to sensitive information and programs.
- Document master date change by requiring authorized signatures, limiting access to serially numbered forms, and retaining the authorization document until the updating is verified.
- Require limits to be stated on the face of computer generated checks issued by the organization to ensure that a large disbursement cannot be made without executive approval. For example, a check might carry the message “Not Valid For More Than \$200” or “No Paycheck Exceeds \$2,500.”
- Cross check totals/serial numbers to ensure all required transactions have been performed but unauthorized transactions have not.

IMPORTANT NOTICE - The information and suggestions presented by Philadelphia Indemnity Insurance Company in this Technical Bulletin are for your consideration in your loss prevention efforts. They are not intended to be complete or definitive in identifying all hazards associated with your business, preventing workplace accidents, or complying with any safety related, or other, laws or regulations. You are encouraged to alter them to fit the specific hazards of your business and to have your legal counsel review all of your plans and company policies.

Detecting Dishonesty

Embezzlement, forgery and counterfeiting succeed only if the victims do not recognize that a crime has been committed. Following an audit trail of receipts, computer records and other documents, a dishonest employee may be traced.

If you do suspect a participant of dishonesty, don't accuse or confront the person without proof. If you have reasonable suspicion your lawyer may suggest that you do the following:

- Ask the person to explain.
- Be ready to assist law enforcement by compiling detailed reports of the crime.

Here's a list of examples you should definitely **not** do:

- Do not detain or restrain someone. False imprisonment is against the law, and charges can be brought against you if you force a person to remain somewhere (e.g., your office) and there was no reasonable basis for the action. Depending on the situation and the employee you're dealing with, there may also be an element of personal danger involved in trying to detain someone. Contact the authorities or your attorney for specific advice if this situation comes up.
- Do not defame the person.
- Do not threaten to prosecute if you are not sure that you are going to bring charges.

It *is* recommended that just like any other crime, employee dishonesty should be prosecuted as a Loss Reduction measure as part of your Risk Management Program. Persons planning to commit crimes generally do not anticipate that they will be caught. They may perceive that your organization is an easy target if they believe they will not be detected and prosecuted. Changing a criminal's perception of the organization may deter or prevent the crime from occurring.

IMPORTANT NOTICE - The information and suggestions presented by Philadelphia Indemnity Insurance Company in this Technical Bulletin are for your consideration in your loss prevention efforts. They are not intended to be complete or definitive in identifying all hazards associated with your business, preventing workplace accidents, or complying with any safety related, or other, laws or regulations. You are encouraged to alter them to fit the specific hazards of your business and to have your legal counsel review all of your plans and company policies.