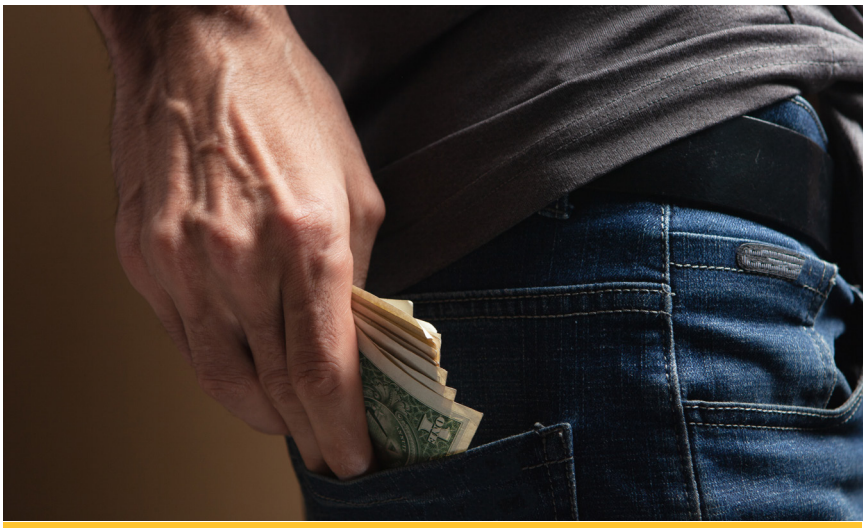
FIDELITY: EMPLOYEE THEFT AND FIDUCIARY RESPONSIBILITY

Every organization has money and assets for which it is responsible. These assets come with fidelity requirements (duties, promises, and expectations) for the officers, members, and organization. Unfortunately, some officers and managers are not always honest and may be tempted to divert money and other financial assets away from your organization for personal gain. Acts like these are known as Fidelity claims.

Fidelity exposures can typically be addressed with the implementation of specific systems providing checks and balances for managing funds. This bulletin offers some best practices for managing financial risks within your organization to help you prevent opportunities for Fidelity claims.

Fidelity Risks

Your organization's funds can be at risk of misuse and embezzlement. Someone inside or outside the organization can commit a fraud or a theft of organizational assets or resources. An employee can embezzle funds, steal office supplies or merchandise, pad his/her expense accounts or create a fictitious company and bill the organization for services never rendered. An outsider can sell bogus merchandise, overcharge the organization for materials or services or entice the organization to make bad investments.



Imagination is the only limit of the ways to defraud an organization. Insurance cannot and does not cover all of these circumstances. Unfortunately, for every control or security system the organization implements, there is always someone smart enough to breach it. Catching wrongdoing before it translates to sizable losses is the key.

Reducing Fidelity Exposures

Directors, managers, chief officers, accountants, administrative assistants, and special event coordinators could become a financial drain on any organization if they do not perform their jobs with fidelity. The real problem for an organization is that when these losses occur, they generally occur over relatively long periods. This may result in staggeringly high losses.

It is important to run annual background checks on any individual involved in a financial receivable or payable transaction on behalf of the organization (including cash, checks and credit cards). This includes individuals who may be responsible for organization assets such as vehicles, property, buildings and investments.

Consider the following risk control methods for reducing Fidelity exposures.

Purchasing, Fund Management and Check Writing

- Require two (2) signatures on checks signed only after written in full. Never sign blank checks or allow the use of signature stamps, even for convenience.
- Have signature cards on file with all financial institutions, and update them annually and anytime there is a change in authorized signors.
- Have an individual who does not have check writing authority receive and reconcile bank statements.
- Audit your financial records annually, utilizing an independent third party.
- Do not permit persons with close personal ties (husband/wife, brother/sister, business partners, etc.) to have control over organizational check writing or reconciliation.
- Require purchase orders and invoices for purchased goods or services. Independently validate receipts of goods and services. Have these compared to written checks or company credit card statements.
- Separate the functions of check writing and deposits.
- Provide regular training on fraud, theft and crime prevention every three years at a minimum. Be aware that some states require annual training for ALL employees. Follow your state's requirements for frequency of training and other training mandates.
- Conduct background checks on all officers and new members.
- Annually review background checks on any individual involved in the handling of organization finances or assets.
- Have all financial policies in writing.
- Review your organization's insurance policy to assure proper fidelity coverage is in place.
- It is also important to make sure those with financial authority at all levels take vacations. In light of the numerous cases seen in the news media, never taking a vacation could indicate someone is hiding fraudulent activity.

Fundraising and Special Events Cash

In addition to the best practices already mentioned, consider the following practices for persons handling funds, especially cash, during fundraising and special events.

- Have a third party present whenever handling cash. This includes not permitting persons with close ties (husband/wife, brother/sister, business partners, etc.) to handle the same cash transaction.
- Use video for security and monitoring cash transactions.
- Whenever possible, have some form of paper trail (ticket stubs, receipts, bill of sale, sign-in sheet etc.) to obtain and confirm a close estimate of the anticipated cash.
- To minimize the amount of cash on hand, pick-up large amounts of cash periodically, documenting personnel involved, times and amounts picked up.
- Have two individuals at a minimum involved in the reconciliation of cash deposits.

Accounting Software, Computers and Related Systems

Many organizations do not have newer computers, computer networks, and sophisticated security measures in place. Instead, they depend on one or more individuals to use their personal computer, internet, and email in the hope of cost-savings.

Consider the following steps to mitigate the risk of losing financial data and the possibility of a fidelity event by implementing the following best practices.

- Use company-owned computer hardware, tablets and licensed software. Assign those machines to organization officials or require work be performed in the organization office.
- Limit use of company-owned computers, hardware and systems for company business only.
- Have all authorized personnel use a unique, company-owned email rather than a personal email account.
- Have individuals use a unique password that is not shared with others. Use a different password for each financial institution.
- Install and utilize antivirus software on any computer or electronic device used for storage of company financial records.
- Password protect and encrypt company wireless connections, if possible.
- Establish a process for regularly backing up data to a separate location on the computer, and two (2) separate physical locations to mitigate catastrophic loss of data.
- Use two-factor authentication.
- Do not conduct transactions on an unsecured/encrypted wireless connection.
- Properly dispose of old, company-owned computer hardware, erase hard disk drive, if possible, and destroy other memory devices.

ADDITIONAL RESOURCES

Fidelity Training - Glatfelter Ministry Care offers online training courses via our Glatfelter University eLearning platform, available free to active Glatfelter policyholders.