



Policy Factsheet

Commercial Crime Insurance/ Dishonesty Bond

Overview

Commercial Crime Insurance/Dishonesty Bond protects your organization's assets against loss attributable to dishonest acts.

A policy can also be written to cover actions by those who are not employees, directors, trustees, or volunteers.

Some commercial multiperil policies include protection against theft, and the disappearance and destruction of money and securities inside or outside the premises.

Protection may also be available against robbery and safe burglary inside or outside the premises and, because of computer use and electronic data transfer as a financial transaction medium, computer and wire transfer fraud protection now also exists.

What's Covered

The policy insures property such as office equipment, supplies, computers, and fine art in addition to money and securities.

Your organization's money and securities exposure extends beyond petty cash on hand and may include bank and investment accounts.

The policy should be written to cover the acts of people outside of the traditional definition of employee, such as volunteers.

Two major protections that such insurance covers are employee dishonesty and forgery or alteration.

Employee Dishonesty

This protects your organization against loss of money, securities or other property arising from the dishonest acts of an employee and should be written to protect directors, trustees, and volunteers.

Employee dishonesty insurance can protect checking and other financial accounts, donations, plate collections, and other contributions; and income from daycare, tuition, and other sources.

Forgery or Alteration

This protects your organization against loss arising from third-party forgery or alteration of checks, drafts, promissory notes, or similar instruments made or drawn by the policyholder or its agent.

That's why it's important to arrange enough protection for the once-in-a-lifetime dishonesty scheme that most churches find unimaginable.

FAQs

Q: *What should I do if I suspect a theft?*

A: Discuss your suspicions with the church's management body and in the financial committee before taking further steps, which could include reaching out to Church Insurance, the district attorney, or a local prosecutor. Many policies require that the church cooperates with law enforcement for coverage to apply.

Q: *What systems can we implement to mitigate the threat of theft?*

A: Church leaders should put safeguards and protocols in place to prevent theft and to ensure suspicion doesn't fall on honest people if a crime occurs. Form a committee dedicated to handling financial issues and reach out to members who have financial skills and fraud prevention experience. If you represent a small parish that doesn't have access to financial specialists, use software accounting packages to help identify suspicious transactions and bring in a professional outside auditor to perform random spot audits. Letting your members know that these safeguards are in place can be a deterrent. An annual independent audit conducted by an outside CPA can uncover financial discrepancies and electing a new treasurer each year can also thwart a thief. Be careful not to grant too much authority to the treasurer, whose role is to manage money, not to handle it. Not allowing a single individual access to cash or records mitigates the opportunity for theft. All cash records should be verified and double-checked. In addition, all accounts should be reconciled by someone who does not have check-signing authority and all checks for \$1,000 or more should be countersigned.

Q: *Are background checks worthwhile?*

A: Yes. A person is a risk if a background check turns up convictions for theft or reveals that the individual is in serious financial difficulty. Consult your state and federal laws with respect to employment practices before conducting a background check on any volunteer or taking any action based on the result of a background check.

Q: *Is each incident of theft treated as a separate claim?*

A: Embezzlers can be clever and usually won't steal large amounts at once. Generally, thefts occur over a long period—perhaps even years. Therefore, in applying policy limits and deductibles, typically all losses attributable to an individual perpetrator or dishonesty pattern will be treated as a single occurrence, regardless of the number of dishonest acts or time span involved.

Q: *What are common types of theft?*

A: Some common ways people steal from organizations include:

Falsifying payroll: Thieves create phantom employees or independent contractors. To prevent this, make sure pay stubs go to a second person who does not process payroll.

Wage advances: Be careful to track wage advances to prevent employees from being overpaid.

Stolen checks: Look for checks that are out of serial number order. Also, the check writer should not be the person responsible for reconciling the bank statement.

Unauthorized credit card use: The cardholder should not also manage the church's credit card statements. Monthly statements should be delivered unopened to the treasurer, who should not have a church credit card.