The Chubb Primary Commercial Crime Insurance

Protection against theft by employees and outside criminals, including hackers and imposters

CHUBB®

Protection for Insureds and their Clients' Assets

Unfortunately, embezzlement, theft and employee dishonesty are exposures for all businesses and organizations. No one and no company is immune.

Losses caused by the social engineering of employees and the impersonation of trusted business partners are increasing and show no signs of abating.

The pace of innovation continues to rise rapidly, bringing with it new ways for criminals to exploit companies with even the best internal controls.

Key Features

- Loss Discovered policy form
- Coverage for theft caused by all classes of employees, as well as natural person independent contractors, with no identified employee or police notification requirement
- No owner or operator exclusion
- Blanket coverage available for employee theft of client's funds and other property, with no collusion exclusion
- ERISA Fraud or Dishonesty coverage for employees serving as plan officials of ERISA employee benefit plans
- Streamlined coverage for loss of funds and property resulting from unauthorized access by hackers into the insured's computer systems including mobile applications and customer web-based portals
- Coverage for loss due to fraudulent transfer of funds through impersonation of employees, vendors and customers
- Investigative expenses for all insuring clauses, as well as computer investigative expenses for losses caused by hackers and impersonators
- Broad subsidiary coverage including entities for which the organization maintains management control
- Full one-year discovery and reporting provision

Coverage Highlights

The Chubb Primary Commercial Crime Insurance provides the following insuring clauses:

- Employees & Plan Officials
  - Employee Theft
  - ERISA Fraud or Dishonesty
  - Client Theft
- Premises & In Transit
- Forgery
- Computer Systems Fraud
- Funds Transfer Fraud
- Social Engineering Fraud
- Money Orders and Counterfeit Currency Fraud
- Claim and Computer Investigations Expenses
  - Claim Expenses
  - Computer Investigation Expenses

Target Audience

- All commercial risks of all sizes are eligible, including:
  - Publicly-traded companies
  - Privately-held companies
  - Not-for-Profit organizations
  - Healthcare organizations

Why Chubb?

Leadership

Chubb is the largest underwriter of Crime and Fidelity coverage in North America, according to the Surety and Fidelity Association of America, a position held since 2001.

Chubb offers a full suite of complementary insurance solutions for a wide range of business risks, including directors and officers liability, employment practices liability and property and casualty coverages.

Endurance

Chubb's financial stability and ability to pay claims rate amoung the best in the insurance industry, as attested by Standard & Poor's and A.M. Best Company, the leading insurance rating services.

Contact Us

To learn more about commercial crime insurance and social engineering coverage, visit www.chubb.com or contact your local agent or broker.

What is Social Engineering?

When an impostor posing as a vendor, client or authorized employee persuades an employee to authorize a transfer of funds, social engineering has occurred. Ironically, digital technology makes it increasingly easy for criminals to create flawless duplicates of official corporate forms, letterheads, and emails. But social engineering can also take place via a phone call—for instance, a criminal impersonating the CEO might persuade the CFO to authorize a large, fraudulent transfer of funds.

Social engineering isn't just responsible for the biggest rise in frequency of commercial crimes. It's also behind a significant uptick in commercial crime losses. According to the FBI[1], losses from what it calls business email compromise doubled between May 2018 and July 2019, to more than $26 billion.

Common examples of social engineering include:

1. An impostor, pretending to be a trusted vendor or supplier, tricks Accounts Payable into using a new account for bill payment
2. A criminal, pretending to be an employee, tricks Payroll into routing salary into a fraudulent new direct-deposit account
3. A stranger impersonates a senior executive, either by voice or email, and pressures an employee into making an illegal transfer

1. FBI Data can be accessed at https://www.ic3.gov/media/2019/190910.aspx

Chubb. Insured.℠