MARSH

FINPRO SPOTLIGHT 101 SERIES

The Basics of Commercial Crime Insurance

Commercial crime insurance provides protection from financial losses related to business-related crime, including theft by employees, forgery, robbery, and electronic crime.

While strong internal protocols can help a company avoid fraud, dishonest employees and external fraudsters can circumvent the security of even the most well-run companies and ones with the most robust controls, leading to potentially substantial financial losses.

Although employees remain the greatest area of concern for organizations, a crime policy generally also covers losses caused by specific acts of non-employees, including:

- Theft, damage, or destruction of money, securities, and/or other property both on the insured's premises or elsewhere (for example, while in transit).
- Forgery or alteration of negotiable instruments, including forging of the insured's signature on business checks.
- Fraudulent manipulation of the insured's computer system, including a hacker transferring funds to an outside account.
- Fraudulent electronic funds transfer instructions sent to the insured's bank purporting to be from the insured.
- Receipt of counterfeit currency by the insured.
- Social engineering fraud (see sidebar).

The consequences of any of the above crimes can be financially devastating for companies and lead to severe reputational harm, making crime insurance an essential part of a company's arsenal. Additionally, the Employee Retirement Income Security Act of 1974 (ERISA) requires any person handling funds of a qualified employee benefit plan to be bonded, a feature that is typically included in a commercial crime policy.

Crime insurance is often referred to as *fidelity insurance* since crime policies cover losses caused by employee theft.

Key Coverage Provisions

Crime coverage can vary by insurer, but policies generally share the following characteristics:

- A typical crime insurance policy is written on a **"named perils"** basis, which means that a loss must fall within one of the categories of crime specified in the policy to trigger coverage.

WHAT IS SOCIAL ENGINEERING FRAUD?

Social engineering fraud — also known as fraudulent impersonation, business email compromise, or impersonation fraud — refers to a variety of techniques used by fraudsters to deceive and manipulate victims into transferring funds.

This type of fraud is typically perpetrated when fraudsters contact an employee via telephone or email and make a request for the employee to wire funds for purposes of an acquisition or to change the bank account details for a vendor. These fraudsters tend to conduct extensive research on their victims before making the request in order to increase their credibility. Their efforts could include piecing together information about the employee or the company from social media and other sources and gaining access to the company's email servers by sending a spam email with malicious code.

Since the perpetrators of social engineering fraud are able to create plausible scenarios, their schemes may not be detected until funds have been wired to bank accounts overseas, and recovery is either impossible or incomplete. Victims range from small businesses to large organizations, across many industries and geographies.

Although standard crime policy forms do not address exposure to social engineering fraud, carriers have created endorsements that provide affirmative coverage. Typically, social engineering coverage comes with a sublimit and sub-deductible, but carriers may be willing to provide multimillion dollar limits in some cases. If your program has excess layers, you should seek to add sublimits in excess policies as well and ensure that the excess drops down to meet the primary policy's sublimit.

- For commercial crime policies, the **limit** is usually not aggregated, applying separately to each and every loss.
- Although **deductibles** apply separately to each loss, a series of acts by the same person or same group of persons are deemed a single loss, and thus subject to one limit and one deductible, regardless of how long the theft continues prior to being discovered. In compliance with ERISA, there is no deductible applicable to losses sustained by benefit plans that are required to be bonded by ERISA.

Coverage Trigger

Commercial crime policies provide coverage in two scenarios:

- Under a "loss discovered" form, coverage applies to loss that is discovered during the policy period regardless of when the act/loss took place, which makes these forms preferable.
- Under a "loss sustained" form, coverage applies when a loss is actually sustained.

Discovery of Loss

There are two instances that trigger the discovery of loss:

- When the insured first becomes aware of facts that would cause a reasonable person to assume that a covered loss has occurred, even if all the facts about the loss are not yet known.
- When legal action is taken against the insured alleging acts that fall within the scope of coverage.

Typically, the insured must provide the insurer with written notice as soon as practicable, but no later than 30 to 60 days after discovery occurs. Usually, the insured must provide a proof of loss within four to six months after discovery. Although most insurers are willing to grant extensions for the filing of proof, the burden of proof of coverage for loss rests solely with the insured.

To aid insureds in developing a robust proof of loss, many policies will provide some coverage for their clients to hire forensic accounts or attorneys. Marsh Risk Consulting's Forensic Accounting and Claims Services Practice can help insureds develop their proof of loss, which could significantly improve a company's recovery under a crime policy.

If possible, "discovery" should be limited to specific departments (for example, risk management and legal teams) or persons (risk managers or general counsel).

What's Typically Not Covered?

Although policies can vary, the following are typically not covered by crime insurance:

- Losses caused by employees after the insured has knowledge of a crime committed by that employee.
- Indirect or consequential losses of any nature, such as business interruption or loss of potential income.
- Legal expenses.
- Expenses incurred in compiling a proof of loss, unless claims/investigative expense coverage is included in the policy.
- Data theft, including theft of a company's data, trade secrets, client lists, or intellectual property.
- Property damage caused by fire.
- Fines and penalties.
- Salaries and bonuses, commissions, fees, and any associated lost income.
- Losses based solely on inventory records.

What Information is Needed to Get a Quotation?

Insureds will need to complete a comprehensive proposal form to help an insurer understand the risks that the business faces. This form will generally require insureds to provide information on:

- Their size, including revenues, number of employees, locations, and geographic spread.
- The industries in which they operate.
- How accessible cash or high-value items are to employees.
- Systems and controls they have in place to prevent losses, including audit and payment request processes.

DIFFERENTIATING YOUR RISK

During the application process, it's important for insureds to demonstrate to underwriters that they represent a "good" risk. That includes a clean loss history, or — in the case of insureds that have suffered losses — evidence of remedial actions taken to prevent future similar losses.

Underwriters also consider the following to be characteristics of a good risk:

- Audited financial statements with an unqualified opinion.
- A reputable external auditor.
- Consistent and stable financial performance over time.
- Positive financial performance relative to peers.
- A robust internal control environment, including:
  - Segregation of duties around flow of funds, including receivables and accounts payable/payroll.
  - Formalized vendor management processes.
  - An independent internal audit function.
- Strong funds transfer controls.
- A whistleblower hotline or mailbox.

For more information, visit marsh.com, contact your Marsh representative, or contact:

KEVIN GUILLET
Senior Vice President
Crime Product Leader
FINPRO, Marsh JLT Specialty
+1 212 345 8095
kevin.guillet@marsh.com

BEN ZVITI
Senior Vice President
FI Cyber/Crime Leader
FINPRO, Marsh JLT Specialty
+1 212 345 4150
ben.zviti@marsh.com

JUSTINE KEARNS
Senior Vice President
FINPRO, Marsh JLT Specialty
+1 212 345 4263
justine.kearns@marsh.com