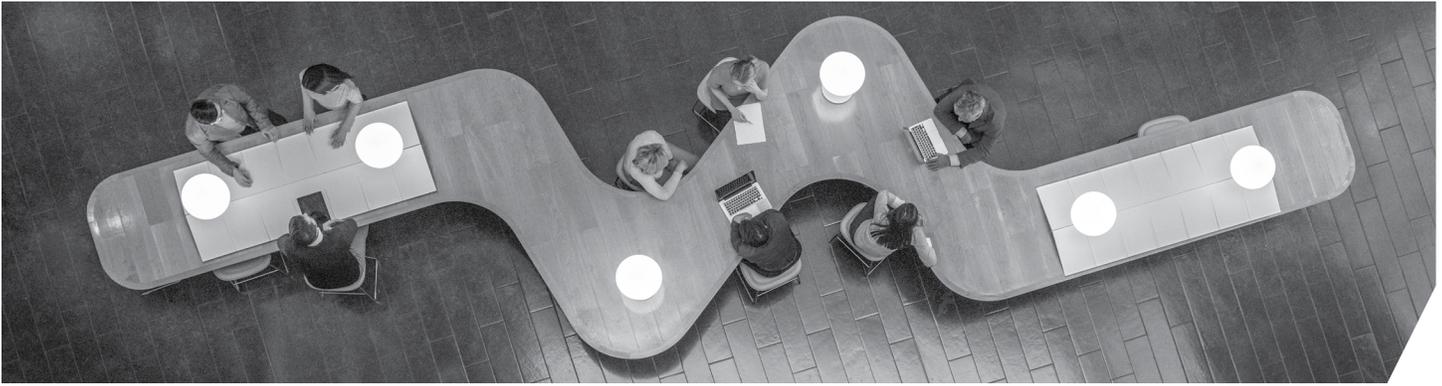


Answering the Top 5 Questions on Commercial Crime Insurance

We all know that commercial crime insurance is designed to protect businesses from financial losses caused by criminal acts, especially those involving employees or third parties. But what are underwriters looking for when an insured completes an application? And what types of claims are the most common? We recently sat down with Mary Henderson, Amwins National Professional Lines Practice Leader, and the commercial crime underwriting team from Old Republic Professional to get the answers.



1 What information do carriers look for on the application?

Carriers are looking for complete applications, submitted prior to renewal, so they can evaluate the following:

-  **Company locations:** Different states may have different rating plans and depending on the nature of the business, specific amendments may be required. International exposures may require a higher deductible.
-  **12 months of experience:** This helps determine the financial stability of the company. Any reorganization required by law, material weaknesses or “going concern” as stated by an auditor could be flagged.
-  **Details on mergers, acquisitions, consolidations or divestitures:** This helps the carrier determine if the company is implementing the same type of internal controls across entities, specifically to ensure that money isn’t being embezzled or hidden. It’s also important to disclose any employee access to client money, computer systems, payroll or accounting systems.
-  **Processes and procedures for accounts payable:** Carriers will ask how reimbursements are processed, specifically if receipts are requested and second approvals are required.
-  **Internal audits:** Carriers will want to know how the company reports fraud and if they have an internal audit department. Inventory control will also be examined.
-  **Bank account controls:** Carriers are looking for accountability and the appropriate segregation of duties. For example, are monthly reconciliations completed on all bank accounts and are there processes in place to ensure that a financial transaction isn’t handled by a single person from beginning to end?
-  **Vendor controls:** Carriers are looking for transparency. They want to know about the competitive bidding process and ensure that vendor experience is verified, etc.

2 How do crime policies differ from other liability agreements?

Crime policies are generally written on a discovery basis, meaning the loss must be discovered by the insured during the policy period. This contrasts with a loss sustained form where the loss must be sustained by the insured during the policy period.

Crime policies are occurrence based. There is a full limit available for each occurrence/loss, unlike management liability and professional lines policies that have an aggregate limit. The policy also defines what constitutes an occurrence or loss.



③ What types of claims are covered under each insuring agreement?

Each agreement will determine what coverage is available to the insured. Most commercial crime policies will offer coverage for:

 **Employee Theft:** This coverage helps protect insureds against theft of their money, securities or other covered property due to theft by an employee, acting alone or in collusion with others. Client coverage, once an extension of coverage granted to risks with employees performing services on a client site, has become its own coverage grant under Employee Theft and is offered on a standard basis.

 **Forgery or Alteration:** Forgery typically includes the alteration of or signing another person's name on a written instrument with the intent to deceive. This coverage includes:

- Negotiable Instruments Coverage to help protect the insured from direct loss caused by the forgery of any negotiable instrument (e.g., check, draft, promissory note, etc.) made or purporting to have been drawn upon the insured.
- Corporate Credit Card Coverage helps protect the insured from direct loss resulting from forgery of any written instrument required in connection with any charge card, credit card or debit card issued by a third party to the insured or its employees for business purposes.

 **Premises:** This coverage helps protect the insured against:

- Loss resulting directly from theft of money or securities by someone physically present on the premises at the time of the loss
- Loss or damage to property where an insured does business resulting directly from an actual or attempted robbery
- Loss of or damage to property in a locked safe or vault resulting directly from actual or attempted safe burglary
- Destruction or disappearance of money or securities within or from the premises

 **In Transit:** This coverage helps protect against loss resulting directly from:

- Theft of money or securities while being transported outside the premises from one person or place to another by an insured within the custody of any employee, a messenger or an armored car company
- Destruction or disappearance of money or securities committed by a third party while in transit
- Loss of or damage to property located outside the premises directly from an actual or attempted robbery while in the care and custody of an armored motor vehicle company or messenger, while being conveyed by the armored motor vehicle company or messenger, or while temporarily housed within the living quarters of a messenger



3 What types of claims are covered under each insuring agreement? Continued...



Funds transfer fraud: This coverage helps protect against loss resulting directly from the transfer of money and securities from the insured's account to a person, place or account beyond the insured's control or issued without the insured's knowledge or consent.



Computer transfer or "hacking" fraud: This coverage helps provide protection for loss following a network intrusion of the insured's computer system by a third party. This may include covered property transferred, paid or delivered to a person, place or account beyond the insured's control and without the insured's knowledge or authorization.



Money orders and counterfeit currency fraud: This coverage helps protect against loss resulting directly from: good faith acceptance in exchange for merchandise, money or services; post office, express company or bank money orders if such money order is not paid upon presentation or in the regular course of business; and counterfeit paper currency of any country.



Social Engineering: This coverage helps protect the insured from loss resulting directly from an unauthorized transfer of money or securities made by an employee of the insured acting on a fraudulent instruction that was purported to be issued by a vendor, client or employee. [You can learn more about how crime and cyber liability policies respond to social engineering claims here.](#)



④ What types of claims are not covered under each insuring agreement?

Each agreement will determine what coverage is available to the insured. However, most commercial crime policies will not offer coverage for:



Digital Currency: Under commercial crime policies coverage is limited to loss of money, securities and property which are defined terms. While digital currency may be an accepted currency in use in some states (e.g., California), it does not fit within the definition of money because it does not have a face value.



Non-Fungible Tokens: Non-fungible tokens, or NFTs, are blockchain-based tokens that each represent a unique asset like a piece of art, digital content or media. However, NFTs do not fit within the definition of money, securities or property. There is a general lack of consensus on the value of the NFT at any given time and while the definition of securities includes the word “tokens,” NFTs were not contemplated when the definition was created. Many carriers have explicitly stated by way of endorsement that the word “tokens” in the definition of securities does not include NFTs.

⑤ What types of claims are we seeing the most?

The most reported type of loss under a crime policy is employee theft. Social engineering claims come in a very close second. The most common social engineering loss is business email compromise. The largest losses come from fictitious vendor schemes. In these types of losses, the imposter claims to be an authorized vendor for a company. The imposter emails the accounts payable department with new wiring instructions for upcoming payments, along with a new call-back number and email addresses for verification. The department then acts on the instructions and sends the money to the imposter. Generative AI is also impacting how fraud is conducted. For example, a Hong Kong multinational corporation transferred \$25M to an imposter who held a video call featuring deepfakes of the company’s top management.

Takeaway

Employee theft is more common than people realize. Even trusted, long-term employees can commit fraud. And while internal controls can help reduce risk, they don't necessarily eliminate it. Commercial crime policies pick up where property, general liability and even cyber policies leave off and can help transfer risk of fraud off the balance sheet.

Amwins professional lines brokers have the expertise and market access to find solutions for your clients. As a trusted partner and extension of your team, their top priority is to secure the best product for you and your clients as efficiently as possible. We package the quote for you, making you look good to your clients and freeing you up to grow your business. Contact your **Amwins broker** today.

Insights provided by:

- Mary Henderson, Amwins National Professional Lines Practice Leader

CONTACT

To learn more about how Amwins can help you place coverage for your clients, reach out to your local Amwins broker.

LEGAL DISCLAIMER

Views expressed here do not constitute legal advice. The information contained herein is for general guidance of matter only and not for the purpose of providing legal advice. Discussion of insurance policy language is descriptive only. Every policy has different policy language. Coverage afforded under any insurance policy issued is subject to individual policy terms and conditions. Please refer to your policy for the actual language.

Courtesy of Amwins Group, Inc.

