Risk Management for Fraud and Other Crime Risks

by Joshua Gold

From thefts of cargo to stolen wire transfers, crime losses abound for policyholders in every industry. Sometimes these losses are caused by criminal gangs, sometimes by computer hackers, sometimes by disgruntled employees, and sometimes a combination of all of the above. No matter what the cause (or identity of the perpetrator), policyholders often have insurance coverage to protect against these risks. But navigating the insurance fine print and an all-too-often adversarial claims process has become a science unto itself. Below are some of the issues that can arise in the insurance context as well as some of the steps that policyholders can take to mitigate the risk of crime-related losses in the first instance.

BE A SMART INSURANCE PURCHASER

Crime losses are a fact of life for most policyholders—irrespective of whether they are large corporations, academic institutions, or not-for profits. Most institutions purchase insurance to protect against losses due to criminal or dishonest acts (e.g., marine cargo policies, business package policies, financial institution bonds, cyber policies, etc.). If money is stolen electronically, policyholders may have insurance coverage under their crime and cyber policies. If freight is stolen while during inland or ocean transit, marine cargo insurance should pay for such losses. Insurance policy language matters, however. In the case of marine cargo, crime and cyber policies, there can exist a wide variety of different insurance policy forms to choose from. Some are much better than others. As such, policyholders should have good and experienced brokers at their side, buying policies that are the least confusing and eschewing those that are exclusion-laden.

Another fact of life is that crime-related losses are sometimes caused by employees and former employees. If theft, dishonesty or fraudulent misconduct occurs due to employee misdeeds, a policyholder may be able to secure insurance coverage under crime insurance, fidelity bonds, property insurance, and directors and officers (D&O) insurance coverage. Again, the quality of insurance will likely come into play. Valuable insurance will be that which severs the misconduct of an employee from the rest of the "insureds" under the policy. Severability in the context of insurance usually comes into play in two instances. First, it is beneficial to have severability in the insurance application. That is, one insured's knowledge and misstatements do not taint insurance coverage for the innocent insureds. Second, it is beneficial to have severability protections built into the insurance policy itself so that exclusions for bad or dishonest acts by one insured do not compromise insurance coverage for other insureds.

AVOID PROBLEMS FROM THE START

It is axiomatic that policyholders should employ smart risk management to guard against external and internal crime threats. For example, in the world of computer-related theft and damage, this means securing the computer systems of the organization as well as the data entrusted to it. To guard against external threats, sound risk management means continuous training of employees to ensure that they practice safe computing. Logging-off, locking their stations when away from their desk and avoiding suspicious emails are a must to minimize the threats from cyber crime. Relatedly, wire transfers should use some system of double-authentication before money is transferred. The wave of losses from fraudulent wire transfer schemes over the past few years has been considerable and certain insurance companies have been defiant in denying insurance coverage from such crime losses.

Other risk management strategies to employ involve restricting employee access to data and system applications. Not all employees need access to all company data and systems. Some data is more sensitive than other data and does not need to be shared across departmental lines or job descriptions.

Last, do not make the bottom line the bottom line. If a deal is too good to be true, then it probably is. Whether it comes to "bargain" cloud computing services being promised, sales of inventory or product that is so, so enticing, or a prospective employee resume that promises a dream candidate, com-

panies should not let such promises of profit/savings obscure their focus. Vetting of such opportunities is still a must and can stem huge, expensive and embarrassing problems down the road.

ADDRESS PROBLEMS WHEN THEY ARISE

If suspicious activity arises, do not ignore it. This is especially true for internal red flags with top producers and senior managers. Many companies, understandably, are loathe to question those employees who are seen as top producers or appear beyond reproach. In the context of crime insurance coverage, remember that if a company is aware of dishonest employee conduct at a certain point in time, the crime insurance company is likely to take an aggressive position that any losses occurring thereafter are uninsured under the "termination" clause of the crime policy. While some courts have rejected insurance company attempts to misuse the termination clause to limit insurance coverage, policyholders are still much better off avoiding such a dispute in the first place.

Similarly, if a loss has occurred, do not delay providing notice to your insurance company. Some policyholders are reluctant to let anyone, including their insurance companies, know that they have been the victims of internal or external fraud. While that may be understandable, policyholders should nonetheless provide prompt notice under any and all potentially applicable insurance policies. Many insurance companies will contest coverage for claims they deem "late", even where no prejudice or other harm has been suffered by the insurance company for the claimed "late" notice.

While crime losses will always remain a risk exposure for many policyholders, smart insurance purchasing and smart risk management can minimize the threat and ultimate harm of such scenarios. ■

***Joshua Gold**, a shareholder in Anderson Kill's New York office and chair of Anderson Kill's Cyber Insurance Recovery Group. He regularly represents policyholders in insurance coverage matters and disputes concerning arbitration, time element insurance, electronic data and other property/casualty insurance coverage issues.*

RISK MANAGEMENT

Reprinted with permission from *Risk Management*.

www.rmmagazine.com