Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

A Policyholder's Guide To Commercial Crime Coverage

By **Jeff Sistrunk**

Law360, Los Angeles (April 4, 2016, 11:05 PM ET) -- In today's ever-shifting digital landscape, companies are being targeted by increasingly sophisticated fraudulent schemes, such as a "phishing" scam that cost tech company Medidata Solutions $4.8 million, raising questions about whether commercial crime insurance policies can keep up.

Here, experts discuss key provisions of commercial crime policies and how policyholders can ensure they are tailored for maximum coverage.

Computer Fraud

Technology has made it possible for fraudsters to convincingly pose as a company's executives, vendors or customers, making it easier for them to induce unsuspecting workers into transferring money through so-called phishing email scams.

Some insurance carriers have recently interpreted the language in computer fraud provisions found in crime policies to extend only to hacking crimes involving direct access to a computer system by an individual with malicious intent. Disputes over such language indicate that policyholders may face pushback if they seek coverage for complex fraud schemes under a traditional crime policy, according to experts.

"The fundamental question is whether crime policies are keeping up with the times," said Greg Podolak, head of Saxe Doernberger & Vita PC's cyber risk practice. "Is the crime carrier agreeing to take on the risk of some of these more intricately designed, newer schemes?"

In one case, Chubb Corp. unit Federal Insurance Co. has denied coverage for a $4.8 million loss that Medidata Solutions suffered when the clinical research technology company's employees were tricked into wiring $4.8 million to an overseas account. The insurer is **contending** that coverage is unavailable because Medidata's policy only covers losses resulting from hacking into a computer system, not voluntary transfers perpetuated by manipulation, which is known as "social engineering."

To avoid disputes over crime coverage for fraudulent transfers induced through social engineering schemes, policyholders can take one of two routes, according to experts.

A number of carriers offer a tailored social engineering endorsement that expressly covers incidents where policyholders fall for phishing schemes and transfer money out of their own accounts or one they

control for customers. In addition, some separate cyber-specific policies have a coverage provision addressing instances of fraud resulting from social engineering.

Policyholders should also be wary of provisions in crime policies that narrowly define who a fraudster must be posing as when trying to induce a fraudulent transfer and try to negotiate for a more expansive definition, experts say.

"Some policies require that the party committing the fraud be posing as an executive officer," said Reed Smith LLP partner Traci Rea. "But in many cases, someone may be posing as a vendor, client or lower-level employee. You want coverage for any situation where an individual is posing as anyone in a fraudulent way."

Employee Dishonesty

Companies of all sizes, particularly financial institutions, constantly face the specter of employee theft. When it comes to insurance coverage for theft and other acts of employee dishonesty, there are several areas that commonly result in disputes between policyholders and carriers.

In a lot of cases, an employee of a company will coordinate a fraudulent scheme along with one or more individuals outside of the company.

Policyholders should try to negotiate favorable language in a crime policy's employee dishonesty provision so the policy will cover the acts of any third parties involved in an employee's scheme, according to experts.

"One of the key things you're going to want to look for is language that includes coverage for acts by third parties with whom the employee is in cahoots," Rea said. "You want the broadest possible coverage to address scenarios where an employee is acting in concert with others."

Carriers may also deny coverage for employee theft based on the scope of a crime policy's definition of an "employee."

In a recent, now-resolved case, Zurich American Insurance Co. disclaimed coverage for Success Healthcare LLC's claim for $10 million in losses stemming from payroll theft, in part based on its argument that the alleged fraudster did not constitute an employee under Success' crime policy.

A Florida magistrate judge disagreed, finding that although the accused fraudster couldn't be considered an employee under a subsection requiring that he be directly compensated by Success, he could potentially qualify as a "leased employee" or one "employed by an employment contractor."

To avoid coverage denials, policyholders should attempt to negotiate the broadest possible definition of an employee, experts say.

Ransom and Extortion

With the uptick in the number of cyberattacks employing ransomware — a form of malware that blocks users from accessing their computer systems and forces them to pay a ransom fee to regain access — insurance coverage for ransom and extortion costs is becoming an important consideration for companies, according to experts.

"With this information age and the ability of different players to access data, extortion coverage is becoming more and more important," Rea said.

The surge in cyberextortion claims has led to a debate among carriers as to whether coverage is available under traditional kidnap, ransom and extortion provisions in crime policies or whether such coverage should be circumscribed to cyber-specific policies.

Some insurers may contend that traditional crime policies don't extend to cyber-related extortion incidents, so it may be necessary to acquire specially tailored cyber coverage for those risks, experts say.

"If there are any gaps, you should ensure they are picked up on the other side," Rea said.

Generally, cyber policies will cover a company's costs from losses associated with extortion through electronic means, according to Anderson Kill PC shareholder Joshua Gold.

"When you're dealing with ransomware claims or other claims where there is a threat to steal data or disclose data, a cyber policy is supposed to pay that loss and expenses associated with the extortion approach," Gold said.

--Editing by Christine Chun.
