Social engineering fraud

Will your crime or cyber insurance policy respond?

December 2018

LOCKTON®

Authors

Marie-France Gelot
Senior Vice President
Insurance and Claims Counsel
646.477.4601
mgelot@lockton.com

Mark Weintraub
Vice President
Insurance and Claims Counsel
404.460.0772
mweintraub@lockton.com

A recent series of coverage decisions by the courts has caused confusion among insureds, leaving many unsure as to which type of insurance policy covers cybercrimes, notably social engineering fraud (SEF) claims, and what policy enhancements are necessary to assure coverage. One reason for the confusion is the informal term "cybercrime" inadvertently combines two distinct policy lines, cyber and crime. The recent decisions concern the latter. This paper examines how cyber and crime policies traditionally operate, how carriers are responding to the increase in frequency and severity of cybercrimes, the impact of recent appellate court decisions confirming coverage for SEF claims under crime policies, and what policyholders can expect going forward.

Cyber vs. crime: Separate policies, separate risks

Policy wording and exclusions are designed to keep one policy line from covering risks intended to be covered by another. Cyber and crime are no different. Cyber traditionally covers risks associated with privacy and the loss or theft of personally identifiable information, like Social Security numbers and other confidential data. Crime usually covers the theft of money and certain property.

Another way to understand the coverage provided by cyber and crime policies is not to focus on the manner of the theft but on the loss. For example, a claim where a hacker uses the internet to infiltrate a company's computer system to steal money would be covered by a crime policy. Conversely, a claim where someone breaks into a car and steals an unencrypted laptop containing personal information of employees would be covered by a cyber policy.

While the coverages available under these policies should not and do not overlap, there can be exceptions, particularly with SEF which can potentially be covered under both crime and cyber policies.

Crime policies have distinct insuring agreements that cover cybercrimes

Crime policies have several insuring agreements that cover different types of risks. While crime policies are best known for their coverage of employee theft, two other traditional insuring agreements are the computer fraud and funds transfer fraud (transfer fraud) coverages. The wording for these insuring agreements differ among insurers, but typically transfer fraud covers fraudulent instructions delivered to a bank that causes a wrongful transfer of funds. Computer fraud covers thefts accomplished solely through electronic means. For many years, these insuring agreements sufficed to cover traditional crime risks, but then technology became ubiquitous, cyber criminals grew inventive, and SEF, also known as business email compromise, was born.

Social engineering fraud

SEF broadly refers to widespread scams used by criminals to trick, deceive and manipulate victims into giving out confidential information and using that information to transfer funds. The prevalence of SEF claims noticeably increased about five years ago as cybercriminals grew more sophisticated. They evolved from "Nigerian Prince" emails to elaborate schemes that spoofed emails from coworkers (often senior level executives, such as the CEO or CFO of a company), vendors and customers. SEF claims took on many guises, but all involved fooling an insured (via a counterfeit email) into sending a payment to an account controlled by the criminal instead of the believed intended recipient.

Today, fraudsters engaged in these scams are well organized and have done their research. Victims of SEF range from small businesses to large multinational organizations, across a wide range of industries and geographies. By the time the scam is discovered, it is often too late for the bank to stop payment, the money has disappeared, and the company is unable to recover it. SEF has now become the second most frequent type of claim reported to crime carriers, behind traditional employee theft.

By the time the scam is discovered, it is often too late for the bank to stop payment, the money has disappeared, and the company is unable to recover it.

Coverage for SEF claims can be contentious

SEF scams continue to alarm both the corporate world and law enforcement authorities because they have been so rampant and effective, leading to six-, seven- and even eight-figure losses for the victim companies. Some policyholders look to their crime policies' transfer fraud and computer fraud insuring agreements to recoup these losses, with mixed results. Early on, a few insurers had existing crime wording that captured SEF losses, depending on the specific facts of the claim. However, most insurers have consistently taken the position that SEF claims are not covered, even if the policy wording is ambiguous and susceptible to coverage. Declining insurers usually make the following arguments:

Transfer fraud only covers fraudulent instructions delivered directly to a bank by a third party. It does not cover the common SEF situation where fraudulent instructions are first delivered to an insured who then, not knowing that the instructions are fraudulent, sends them to a bank.

Computer fraud only covers computer crimes where funds are stolen without a human go-between, like introducing malware to a system that automatically empties a bank account.

SEF theft constitutes a "voluntary parting of money" because the insured who unknowingly approves the fraudulent transfer has actual authority to do so.

SEF constitutes an "indirect loss" because it is a two-step crime that requires an independent intervening cause (e.g., employees executing the transfer) and not a direct theft by the criminals.

Because SEF losses are severe and coverage under the transfer fraud and computer fraud clauses is often unclear, insureds have challenged these denials. In 2015, one insurer, seeking to avoid future disputes, created an endorsement that expressly covers these claims, but its caps coverage to less than full limits. Since then, virtually every insurer has followed suit and now provides some form of express SEF coverage, although limits and premiums vary widely.

More conservative insurers offer lower sublimits for these claims, generally $50,000-$250,000, depending on the insured. Additionally, coverage may be subject to meeting certain underlying conditions, such as automatic callbacks and other verification procedures. Other carriers, particularly underwriters in the London market, have recently begun to offer full limits for certain insureds, subject to more stringent underwriting. Such policies provide broad crime coverage, including SEF, on an "all risks" basis, meaning that the loss is covered unless specifically excluded. This new form of crime coverage may prove to be most beneficial to insureds as crime risks continue to evolve and increasingly complex theft schemes are devised to keep up with modern technology.

US Circuit Courts rule SEF claims are covered

Not long after insurers began offering express SEF cover, Medidata Solutions, Inc. filed a lawsuit against its insurer seeking coverage for a $5 million SEF loss that had been denied under transfer fraud and computer fraud insuring agreements. The SEF scam involved a phony email looking as though it came from the company's president (inclusive of the president's corporate photo) to a Medidata employee who, based on the instructions in the email and a follow-up telephone call with a phony attorney, transferred funds to a third party.

In 2017, the trial court ruled in favor of Medidata, holding that its SEF claim was covered. The 2nd Circuit Court of Appeals affirmed that ruling in July 2018. The court held that the fake email scenario triggered the computer fraud insuring agreement because it concerned a computer-based attack that manipulated Medidata's email system via a spoofing code which consisted of fraudulent entry of data into the computer system. The court also held that the employee's reliance on the spoofed email was the proximate cause of Medidata's losses and therefore sufficiently direct for there to be coverage.

Shortly after the Medidata decision, the 6th Circuit issued an even more policyholder-friendly ruling in American Tooling Center v. Travelers. In that case, the company's vice-president emailed one of its Chinese vendors asking for its invoices. In response, it received a spoofed email, purportedly from the vendor, instructing the company to send payment for several legitimate outstanding invoices to a new bank account. The company wired more than $800,000 to the fake vendor's account. The court reversed the district court ruling in favor of the insurer. They held that there was computer fraud since the impersonator sent the company fraudulent emails using a computer. The court also held that the spoofed vendor email scenario constituted a direct loss to the insured because the computer fraud was an immediate cause of its loss.

These decisions make clear that SEF claims are likely covered even if a crime policy does not have express SEF coverage.

Cyber policies may also trigger in the event of an SEF

As mentioned above, cyber policies cover the compromise of private information and consequences of an attack on computer systems. A breach of a company's computer system, like in the Medidata case, would trigger the breach event coverage under a cyber policy that covers forensic, legal and other expenses. If the breach results in lost property belonging to a third party, liability and defense coverage may also apply.

Some cyber policies include coverage for computer fraud or "cyber deception," which encompasses SEF, though the coverage is typically sublimited to $250,000 or less. Such coverage would be triggered in addition to or alongside the crime policy coverage for an SEF claim. Unless one policy was specifically written to provide the coverage on a primary basis over the other and depending on the wording of each policy's "other insurance" clause, the policies would most likely share the loss proportionately, up to each of their respective SEF sublimits. While some logistical issues could arise by having two policies cover the loss, the benefit to having two available limits to pay for a potentially large SEF is obvious.

In an SEF scenario like the one with Medidata, a policyholder having purchased both crime and cyber coverages could potentially trigger both the breach event coverage and cyber deception coverage of its cyber policy and the computer fraud coverage of its crime policy.

Insurers already reacting to recent SEF decisions

While the Medidata and American Tooling Center policyholder rulings are helpful, they likely come too late to make a material difference to insureds who previously suffered an SEF loss, and they should not be viewed as justification to avoid purchasing SEF coverage.

There are several points policyholders should be aware of when evaluating whether or not to purchase SEF coverage:

- These decisions will only apply to cases within those jurisdictions, so coverage lawsuits in other circuits could have different outcomes.
- The decisions are subject to the factual circumstances of those claims and do not ensure coverage for all SEF claims in those jurisdictions.
- Express SEF coverage has been available since 2015, and insurers have refined the coverage and adjusted the sublimits since then. Where there is evidence that a policyholder could have purchased SEF coverage and chose not to, courts may view coverage with a more critical eye.
- The specific policy language and definition of computer fraud or transfer fraud in every policy is key. Not all policy wordings are created equal, and some are more open to interpretation than others.
- Immediately following these decisions, at least one major crime carrier has announced that it will be expressly excluding SEF coverage under its crime policies by endorsement. We expect such endorsements to be added at every crime renewal going forward and anticipate other carriers will follow suit.

The bottom line is that obtaining express SEF coverage is a more certain strategy for a policyholder than battling insurers for coverage under different insuring agreements. In time, we can hope that crime insurers will become comfortable enough with the SEF risk that coverage for this modern crime will become ubiquitous and uniformly subject to full policy limits for all policyholders.

- RISK MANAGEMENT
- EMPLOYEE BENEFITS
- RETIREMENT SERVICES

LOCKTON.COM

KC: 51562