By
Alan Rutkin

Hacking Discovered, Losses Not Covered

Insight: A computer crime isn't claimable under a commercial policy's forgery endorsement.

Computer crime has become a frequent news story. Hackers break into corporate systems. In some instances, hackers take information about individuals and then steal from these individuals. In other instances, hackers steal from the target company itself.

As I've written in this space for many years, when a new type of loss emerges, insurance coverage issues inevitably follow. Hacking is an example of new losses creating new coverage issues. A recent case from a federal district court in Atlanta addressed these issues.

In *Metro Brokers v. Transportation Insurance Co.,* thieves inserted a virus into a policyholder's computers. The virus copied keystrokes. With this information, the thieves learned the credentials for the policyholder's bank account. The thieves then logged into the bank account and stole nearly $200,000.

To recover this loss, the policyholder made an insurance claim. The insurer disclaimed. The case revolved around two points: First, was the claim covered under the policy's endorsement for forgeries? Second, was coverage barred by exclusions for "malicious code" and "system penetration?"

Was an electronic transfer essentially a check?

The court found for the insurer, in a case that presented a very interesting analysis.

The forgery coverage added coverage for the "forgery" of "any check, draft, promissory note, bill of exchange or similar promise…." The policy defined forgery as "signing the name of another person … with the intent to deceive." The court seemed to accept that logging into computers was effectively a "signing." The key question was whether an electronic transfer was the type of instrument that was covered. Was an electronic transfer essentially a check, draft, promissory note or one of the other listed items? The ruling found that the forgery coverage applied to negotiable instruments, and electronic transfers are not negotiable instruments. In reaching this conclusion, the court was persuaded by the fact that the insurer offered other coverage for claims involving electronic transfers.

The court then considered whether to apply the exclusions for malicious code and system penetration. The policyholder argued that the computer virus was not the cause of the loss; a human thief had to act on the virus. The judge was entirely unpersuaded by this argument. All thefts involve a human element. What's more, by its terms, the exclusion applied to instances where the virus caused the problem, "directly or indirectly." The exclusion went on to say that "loss or damage is excluded regardless of any other cause or event."

The reasoning of this case ultimately may be more important than the specific decision. The court needed to decide whether electronic transfers were similar to negotiable instruments. More generally, the court needed to compare new devices to old devices.

Much of the law concerning computers will evolve through this process. We'll see many courts considering whether new devices are similar to old devices. Stated differently, courts will need to identify the old device that is most similar to the new device, and then see how the law treated that old device. Only one thing is completely certain. As computer crime grows, computer-related claims will, too. BR

Best's Review *columnist Alan Rutkin is a partner at Rivkin Radler in Uniondale, N.Y. He can be reached at* alan.rutkin@rivkin.com