Protection Against Fraud Must Be Specific

Authorized users of a computer system who enter fraudulent information into that system are not 'hackers.'

Computers continue to create new and interesting insurance coverage questions for a number of reasons including the fact that the area involves new acts and new policies. At the start of the summer, New York's highest court addressed these issues in Universal American Corp. v. National Union, and the court enforced the strict language of the policy.

The policyholder, Universal, is a health insurance company. Universal allows its members to submit claims directly into a computerized billing system. For protection against certain fraud, Universal bought an insurance policy for certain dishonest and fraudulent acts. More specifically, it insured against "Computer Systems Fraud Loss resulting directly from a fraudulent (1) entry of Electronic Data or Computer Program, or (2) change of Electronic Data or Computer Program with the insured's proprietary Computer System…."

Universal then suffered $18 million in fraudulent losses. Claims were made and paid for services that were never actually performed. The claims were made by authorized users of the computer system. These users entered false information.

The question then was did the "fraudulent entry" coverage apply to authorized users entering fraudulent information? That is, what did "fraudulent" qualify, the entry or the information?

The court found that fraudulent modified entry. It concluded that the language unambiguously applied to losses incurred from unauthorized access to the computer system and not to losses resulting from fraudulent content submitted to the computer system by authorized users. Hence, the court enforced the policy literally.

By
Alan Rutkin

When seeing claims under policies addressing computer hacking, courts are distinguishing computer 'hacking' from mere computer 'using.'

The court based its analysis on several points.

Looking at the language literally, the fact that the word "fraudulent" was immediately before the word "entry" meant that entry was being modified. This word placement demonstrated that the policy covered a breach of the integrity of the computer system through deceitful and dishonest access. The policy insured against hacking.

The court also looked at the title of the coverage, "Computer Systems," with the subtitle "Computer Systems Fraud." The headings also indicated that the coverage was applying to misuse of the system itself.

Similarly, the court observed that the policy excluded losses resulting directly or indirectly from fraudulent instruments "which are used as source documentation in the preparation of electronic data, or manually keyed into a data terminal." If the policy was meant to cover fraudulent content, such as billing fraud, then there would be no reason to exclude fraudulent content contained in documents used to prepare electronic data, or manually keyed into a data terminal.

The court's decision is consistent with several trends we're seeing in this area.

First and most importantly, many courts are literally and strictly construing the terms of special policies addressing computer-related claims. Courts are seeing many different policy terms and they're reading them closely.

Second, when seeing claims under policies addressing computer hacking, courts are distinguishing computer "hacking" from mere computer "using." Everyone, including people perpetuating crimes, uses computers. People use computers in the commission of their crimes. But, not all users are hacks. To be a hack, you need to break into the computer. 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*