BEST'S REVIEW
www.bestreview.com August 2019

Scam Sophistication

The warnings about cybercrime need to be taken seriously. As scammers have become more cunning, vigilance is important.

By
Alan S. Rutkin

While some courts strain to find for policyholders, many courts are enforcing the clear coverage restrictions in the cyber area.

My wife and I received an email—our youngest son was asking us to wire money because he had been mugged. We threw it out because we recognized it as "spoofing." (Our son is too mean to be mugged.)

These scams, however, have preyed upon people with kindlier children, and now they're preying on corporations.

Scammers send emails to CFOs. The emails are made to appear to be from CEOs. The fake CEOs instruct real CFOs to make certain payments. And the payments go to the scammer.

Spoofing has now become an insurance coverage and underwriting issue.

Some insurers are writing exclusions for fraudulent transfer requests. A federal court recently addressed these provisions and found for the insurer. The case is worth noting—*Tidewater Holdings Inc. v. Westchester Fire Insurance*, from the Western District of Washington this past May.

The insured's accounts payable clerk received an email directing the clerk to make a payment. But, the writer was a scammer. The payment was stolen.

The insured sought coverage for its loss.

The insurer denied based on an exclusion: "[T]he Insurer shall not be liable for any loss resulting from any Fraudulent Transfer Request."

The policy defined fraudulent transfer request as "the intentional misleading of an Employee, through a misrepresentation of a material fact which is relied upon by an Employee, sent via an email…."

The policyholder challenged the exclusion as ambiguous.

But, the court found the language clear and enforced the exclusion.

Readers of this column know that I have suggested that the case law on cyber coverage issues falls into four categories: authorization, causation, act and injury. (The mnemonic is acai, like the berry.) Acai captures this case; it's a case about the "act." Acai also captures the other cases involved.

The insurer had cited two other insurance coverage decisions involving spoofing, and read both cases to establish a broad proposition that spoofing is simply not covered. The court, however, took an "acai-like" approach and read the cases more narrowly.

One case the insurer cited was *Taylor & Lieberman*, from the Ninth Circuit. The court saw the "C" in acai and read this as a causation case.

Another case the insurer cited was *Aqua Star,* from the Western District of Washington. There, the court saw the first "A" in acai and focused on the authorization issue.

What are the lessons drawn?

First, warnings on cybersecurity may be dire, but they are appropriate. Scammers have become clever and sophisticated. Vigilance is critical.

Second, while some courts strain to find for policyholders, many courts are enforcing the clear coverage restrictions in the cyber area.

Third, this area is complicated by the fact that we have many insurers writing policies, but the market has not yet landed on common terms. But, you can make sense of this area if you sort the cases into these four buckets: authorization, causation, act, and injury.

Keep acai in mind both at the breakfast table and at your desk. 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*.