BOVIS KYLE
BOVIS, KYLE, BURCH & MEDLIN

INSURING AGAINST CYBERCRIME: SUPERIMPOSED RISK

By Gregory R. Veal November 30, 2018

Most computer fraud endorsements are intended to cover losses caused directly by hacking. But what happens when an employee willingly, although unwittingly, transfers funds to an outsider who infiltrates the insured's network?

Insurers, responding to the market's demand, now offer (for a price) social engineering fraud coverage — as distinct from computer fraud coverage. Social engineering coverage specifically and expressly contemplates that an outsider will use a computer to induce action by a recipient, which then results in the loss.

With the availability of coverage for each of these separate risks, courts should have no need to superimpose one coverage over the other.

Unfortunately, if you deal with computer crime coverages, you may have heard of the *Medidata* case. In that case a federal judge in the Southern District of New York, affirmed by the Second Circuit Court of Appeals, decided that a computer fraud policy covered loss involving a social engineering scheme. *Medidata Systems, Inc. v. Federal Insurance Company*, 268 F. Supp. 3d 471 (S.D.N.Y. 2017), *aff'd,* 729 Fed. Appx. 117 (2d Cir. 2018).

After *Medidata* some may ask whether the distinction between computer fraud and social engineering coverages has been completely eliminated.

The good news is that *Medidata* should not have wide influence or application. (The District Court's decision has been cited only once, for a different point, and the Circuit Court's decision was a summary order and does not have precedential effect.) Close attention to the specifics of the fraudulent scheme and the computer fraud policy language will be necessary, as will education of insureds and courts about the scope of insurance available and the difference between hacking and social engineering coverages.

Loss resulting directly from a hack should be addressed by the computer fraud insuring agreement or rider, while loss resulting directly from a duped employee's conduct falls under social engineering coverage.

In *Medidata* the computer fraud endorsement covered "direct loss" resulting from fraudulently induced transfer of funds resulting from any "entry of Data into" or "change to Data elements or program logic of a computer system."

The outside fraudster in *Medidata* modified e-mails inserted into the insured's computer system and fraudulently induced employees to initiate wire transfers to the outsider's account.

The policy was intended to cover losses caused directly by hacking incidents. Since the fraud in *Medidata* involved wire transfers initiated by employees, the loss would ordinarily have been considered indirect. The insured expected broader coverage, and the courts obliged.

The fraudster's alteration of computer code in the spoofed e-mails, which then were sent within the insured's computer system, was enough like a pure hack to satisfy the courts, which refused to honor the use of the term "direct" as any form of restriction on coverage.

Likewise, the courts had no problem finding the alteration and insertion of code to be the "proximate cause" of the loss, even though the employees had to be tricked into performing multiple additional steps before the transfers could take place.

This case has emboldened insureds and their counsel to argue that fraudulent schemes employing a computer must be covered under any fairly-construed computer fraud endorsement or rider.

However, *Medidata* should be limited to address only policies with similar language, if any. "Direct loss" was given no effect, but the common phrase "loss resulting directly from" more clearly states the required close link between the covered cause and the transfer of money. Also, the loss could be "resulting from" a "fraudulently induced transfer" that itself was "resulting from" the change or entry of data into the insured's system. Two uses of "resulting from," especially without the restrictive modifier "directly," invited the courts to broaden their causation analysis. Finally, because the hacking-type activity could result in a "fraudulently induced transfer," the language necessarily implied that the insured's employees would be tricked into acting, so that those actions could not be considered a break in the causal chain for coverage purposes.

Other courts have recognized the restricted scope of computer fraud insuring agreements. *Apache Corp. v. Great American Ins. Co.*, 662 Fed. Appx. 252, 258 (5th Cir. 2016); *see also Aqua Star (USA) Corp. v. Travelers Casualty & Surety Co. of America*, 719 Fed. Appx. 701 (9th Cir. 2018) (holding turned on an exclusion, but court also held the loss resulted from tricking of employees, not a hack).