Reach Of Ohio Ransomware Ruling Limited To Policy At Hand

By **Jane Warring** (January 19, 2022, 3:38 PM EST)

Jane Warring

We are still in the relatively early stages of jurisprudence addressing the insurability of loss stemming from data breaches.

Compared to the more developed body of case law interpreting coverage provisions and exclusions contained in more traditional property insurance policies, case law exploring coverage issues under so-called silent cyber or stand-alone cyber policies is sparse.

As such, when any new decision does come down in this arena, it sparks commentary.

This was true for the recent Ohio appellate court decision in EMOI Services Inc. v. Owners Insurance Co.,[1] in which the Ohio Court of Appeals' Second Appellate District **reversed** the common pleas court's summary judgment ruling in favor of the insurer and allowed the insured's silent cyber claim to proceed.

The majority's decision in EMOI has come under fire by the insurance bar for being results-oriented and ignoring precedent. Conversely, policyholder attorneys have lauded the decision, going so far as to claim that EMOI stands for the proposition that a policy insuring physical loss or damage does not require physical alteration of property.

But are these criticisms and characterizations fair? And what lessons can we take from this rare and candid discussion by a court grappling with the bounds of insurance coverage for data loss?

EMOI's holding was dependent on very specific policy language.

In EMOI, a medical billing company sustained a ransomware attack, paid the ransom, decrypted most of its data and then sued its property insurer for claimed business interruption losses and alleged damage to computer software.

Careful review of the appellate court's decision in EMOI indicates that its holding was entirely dependent on the unique language of the Owners' electronic equipment endorsement contained in the policy at issue.

That endorsement covered "direct physical loss of or damage to 'media,'" where media was defined as "materials on which information is recorded such as film, magnetic tape, paper tape, disks, drums, and cards."

Importantly, the definition section goes on to state that "media" includes "computer software and reproduction of data contained on covered media." In short, the policy insured damage to media and defined media as software and as materials on which software is recorded, i.e., servers.

The trial and appellate court's disagreement over the facts may explain the different results.

The trial court concluded from the record before it that, after decryption, EMOI's computer systems were "fully-functional with all the data it had before the ransomware attack."[2] This was the critical fact supporting its finding in favor of the insurer.

The trial court explained that even assuming the software was damaged while it was encrypted, it was no longer damaged because "EMOI has all the data it did before the ransomware attack" and "its software is now fully-functional."[3]

The appellate court disagreed with the trial court's finding that EMOI's software was no longer damaged after decryption. Specifically, there was unrefuted testimony from EMOI witnesses that certain portions of the system could no longer communicate with each other and a program that generated remittances no longer functioned, among other issues.

EMOI does not upend any "physical loss or damage" jurisprudence.

After two years of the property insurance industry being abuzz over the meaning of "physical loss or damage," it is tempting to want to put EMOI on the insurer versus insured scoreboard on this issue. But EMOI does not belong on the scoreboard. Yet again, the specific policy language at issue in EMOI compelled the appellate court's decision on this issue.

The insurer in EMOI argued that even if the software was damaged, it was not physical damage as required by the policy. The insurer responded that (1) the policy covered only tangible items, (2) loss of use is not physical damage, and (3) physical damage does not occur when an item can be restored by cleaning.

The appellate court refused to consider any cases where the policy at issue required physical loss to tangible property as EMOI's policy did not include the term "tangible."

The court also refused to consider any COVID-19 cases on the grounds that businesses unable to operate due to government mandates are not analogous to an intrusion into EMOI's computer system.

The court appeared to find cases discussing physical alteration of property that could be removed by cleaning somewhat analogous.

After grappling with what exactly happens when data is encrypted, and noting that neither side provided the court with an expert to assist, the court concluded that the encryption caused damage to software that was more than merely aesthetic and did more than simply block access.

Ultimately, the court agreed with EMOI. The policy insured damage to software, and if software was tangible enough to insure, it was tangible enough to be damaged. The court suggested that if EMOI's policy had not insured damage to media and then gone on to define media to include software, it would have to come to a different conclusion.

No helpful physical loss or damage case law was made with this decision. The entire order reads like a foregone conclusion on this point. Damage to software was specifically insured.

Perhaps unsurprisingly, the court cited favorably the U.S. District Court for the District of Maryland's 2020 decision in National Ink and Stitch LLC v. State Auto Property and Casualty Insurance Co.[4] That decision was also driven by very specific policy language.

The policy at issue in National Ink specially insured data. That court reasoned that if the policy had intended to require physical loss or damage to the media device it could have stopped at the "covered media" subsection. Instead, the policy went on to include a "data stored on such media" subsection in the definition of covered property.

The EMOI court wanted to hear from a computer expert.

One of the more interesting lessons to come out of EMOI is the need for computer experts. These are relatively complicated issues for a layperson to understand. When applying policy terms to facts, it is important to truly understand the technology. Courts want experts to help them navigate these waters. Indeed, the appellate court in EMOI was begging for one.

At several points in the decision, the court notes that there was no opinion offered by any computer experts and that it could have benefitted from that type of direction:

- "Owners did not provide evidence from an IT specialist to address what constitutes media."[5]
- "The record contains minimal information about how encryption occurs and its effects on computer data."[6]
- "[EMOI's IT manager] did not describe, in technical terms, how encryption and decryption occurs and the effects on the item being encrypted. No other evidence regarding encryption was offered by the parties."[7]

The court cited to testimony from EMOI's IT manager as some of the critical information it used to understand what happens during encryption and decryption. This individual himself struggled for the right words:

I'm trying to think about the best way to explain this. It's a mathematical function that's been designed so it's hard to find a solution for it, but if you know the answer to the problem, you would be able to basically undo the encryption.[8]

Computer experts can help courts and parties understand the facts affecting coverage. They are also helpful in analyzing the insured's invoices and costs and commenting on the purpose of each expense. This may prove even more important in the next phase of EMOI where the trial court or jury will be asked to determine which of EMOI's costs were directed at repairing damage to software versus recreating data or upgrading its systems to avoid future cyber threats.

Like most policies insuring data breach, this policy excludes "the cost endured by EMOI to upgrade its systems to cure the deficiency that left it vulnerable to attack" in the first place.[9]

In the end, EMOI is not as good or bad as it has been made out to be, and it should not have implications beyond policies specifically insuring damage to software. Certainly, it may be cited to support broader propositions regarding damage to intangible property but its limitations are clear.

Jane Warring is a partner at Zelle LLP.

[1] EMOI Services Inc. v. Owners Insurance Co., 2021-Ohio-3942, 2021 WL 5144828 (Ohio Ct. App. Nov. 5, 2021).

[2] EMOI Services LLC, Owners Ins. Co., Montgomery C.P. No. 2019 CV 05979, p. 6 (May 4, 2021).

[3] Id.

[4] National Ink and Stitch LLC v. State Auto Property and Casualty Insurance Co., 435 F.Supp.3d 679 (D. Md. 2020).

[5] EMOI, supra, at 17.

[6] EMOI at 25.

[7] Id.

[8] 2021-Ohio-3942, ¶ 49, 2021 WL 5144828, *9.

[9] 2019 CV 05979, p. 6.