HINSHAW

Policyholders Face Substantial Challenges in Obtaining Coverage for Cyber Claims Under First-Party Property Policies

Notwithstanding a Maryland District Court Ransomware Attack Decision

Insights for Insurers Alert | 5 min read
Jan 29, 2020

Notwithstanding the wide array of cyber specific insurance products available in the market, policyholders have and will continue to look for coverage for cyber, data breach, and privacy claims under commercial general liability and first-party property policies when confronted with a claim or suit. Policyholders face numerous hurdles in obtaining coverage under these policies, which often do not apply at all or provide only limited coverage for such claims. *See generally,* S. Seaman & J. Schulze *Allocation of Losses in Complex Insurance Coverage Claims* (Thomson Reuters 8th Ed. 2019-2020) at Chapter 17 "Cyber and Data Breach Claims."

On January 23, 2020, the U.S. District Court for the District of Maryland ruled on summary judgment that a businessowner's insurance policy covers the replacement of an embroidery and screen printing company's computer system resulting from a 2016 ransomware attack. *National Ink and Stitch, LLC v. State Auto Property and Cas. Ins. Co.*, No. SAG-18-2138 (D. Maryland) (applying Maryland law). Although the case finds coverage and will not serve to deter policyholders from turning to traditional first and third-party policies for coverage, the district court decision does not change the landscape materially and is not beyond challenge on various grounds.

Judge Stephanie Gallagher determined that the ransomware attack resulted in "direct physical loss of or damage to" the policyholder's computer hardware and software and, as such, is covered under the businessowner's ("BOP") policy. The policyholder, National Ink, claimed that it was prevented from accessing its art files and most of its software programs. National Ink agreed to pay the attacker in bitcoin to restore access to its data and software, but when the attacker demanded more bitcoin to remove the virus, the policyholder retained a security contractor to replace and reinstall all its software and install protective programs on its system. The security updates left National Ink's computers running more slowly, and the company later discovered that remnants of

the ransomware virus likely were still in its system, threatening to re-infect it. Rather than wiping the computer system clean, National Ink bought an entirely new server and computers.

State Auto paid the $5,000 "forensic information technology review" limit, but otherwise denied the claim. State Auto contended that, because National Ink only lost intangible data and could still use its systems to run its business, there was no direct physical loss as required by the policy. National Ink argued the policy language provides that computer files and software are property that can be subject to a direct physical loss and that its computers themselves sustained damage "in the form of impaired functioning."

Judge Gallagher determined that "loss of reliability, or impaired functionality demonstrate the required damage to a computer system, consistent with the 'physical loss or damage to' language in the policy." According to the court, National Ink sustained a loss of its data and software and was left with a slower system that appears to be harboring a dormant virus. The court cited to *American Guarantee & Liab. Ins. Co. v. Ingram Micro, Inc*., 2000 WL 726798, at *1 (D. Ariz. April 18, 2000) for the proposition that "physical damage" is not restricted to the physical destruction or harm of computer circuitry but includes loss of access, loss of use, and loss of functionality and to *Ashland Hospital Corp. v. Affiliated FM Ins. Co*., 2013 WL 4400516, at *1 (E.D. Ky. Aug. 14, 2013) (direct physical loss or damage includes a loss of reliability). The *Ingram Micro decision* relied upon statutes to interpret physical loss. The decision has been criticized because physical loss should be afforded its defined or plain meaning and not interpreted by reference to statute.

The court also ruled that the loss of data and software falls within the coverage of the Businessowners Special Form Computer Coverage endorsement that defined "Covered Property" to include "Electronic Media and Records (including software). "Electronic Media" was defined to include electronic data processing, recording or storage media such as films, tapes, discs and data stored on such media. According to the court:

> While the term "data" is qualified with the phrase "stored on such media," if the Policy intended to require physical loss or damage to the media itself, as opposed to just the data, it could have stopped at subsection (a), which describes the covered media. . . Instead the Policy includes "data stored on such media" as a separate subcategory of Covered Property in subsection (b). . . The Policy also contains the phrase "Including Software" in its heading describing covered property.

Some observations are worth making.

- It is unclear exactly what the consultant did to scrub the computer system, but it appears that it installed protective software/devices after which the computer system operated, but at a slower pace. Apparently, the computer system did not process the data as efficiently as it did before the implementation of the protective software or devices raising the issue as to whether the functionality resulted from the "repair" as opposed to the ransomware. Indeed, the policyholder's consultants stated that it was the protective software and/or devices impacting functionality.
- There does not appear to be any evidence that, after the consultant addressed the issue, any ransomware remnants impeded the computer's functionality. A speculative possibility that not all of the ransomware was

removed fails to meet the requirement of "direct physical loss." There was no evidence that, after the repairs, there remained a material change to the computer operating systems from ransomware remnants that degraded its functioning. Although the policyholder argued that certain data or files were inaccessible, no evidence was put forth to support what data or software was lost that could not be re-inputted with the repairs.

- The declination letter raised several bases, including that: (a) replacement of all the hardware and software was a preventative measure and not because direct physical damage or loss necessitated the replacement; and (b) no covered cause of loss. An argument can be made that there was no covered cause of loss as raised in its denial letter insofar as the software and hardware were not replaced because of a covered cause of loss but due to its slower computing with the addition of the protective software/devices.
- The subject policy was issued in 2016, however, the BOP form at issue was the 1999 ISO form. More recent forms, such as the 2012 ISO BOP form, exclude computer-related losses that, by definition, includes malicious code. The 2012 BOP form excludes loss caused by viruses or malware.
- Covered cause of loss was modified by endorsement to include computer fraud, which was specifically defined to mean "theft" by "use of any computer to fraudulently cause a transfer of that property inside the premises to a person (other than a messenger) outside the premises." Theft was defined as the act of stealing. The motion by State Auto addressed the single issue of whether the software (code) and electronic data sustained direct physical loss or damage.
- *March 2, 2020 addendum*: although we believe that State Auto had grounds for appeal of the district court's ruling, we understand that the case has been settled.

Related People

Peter E. Kanaris

Partner

312-704-3628

Scott M. Seaman

Partner

312-704-3699

Related Capabilities

Insurance

Insurance Coverage Litigation & Counseling