FROM THE DESK OF

ANDERSON KILL
PHILADELPHIA

February 2021

Who Pays? Cybercrime in the Courts in 2020

By Pamela Hans and Bruce Strong

In our pandemic year, the mass exodus from office to home office gave a fresh spur to the relentless increase in cyberattacks. Increased harm brings increased liability — and litigation. Here, we'd like to call your attention to two decisions in U.S. District Courts in 2020 that address "who pays" for damage caused by cyberattacks. One concerns the liability of the breached party; the other, the extent to which a business property insurance policy may cover damage to a policyholder's computer system.

Liability in the Wake of a Data Breach

Bank of Louisiana v. Marriott Int'l, Inc.,[1] concerns the ability of one business harmed by another business's data breach to hold the breached company liable. In this case, cyber criminals infiltrated Marriott's computer system and stole sensitive payment information, such as credit card numbers, many of which were not encrypted.

Bank of Louisiana, on behalf of itself and a putative class, sued Marriot alleging that it suffered damages including costs to "cancel or reissue credit and debit cards," "refund or credit any cardholder to cover the cost of any unauthorized transaction relating to the Marriott Data Breach," and "increase fraud monitoring efforts." Marriot responded that these damages were not cognizable injury (that is, injury capable of being adjudicated).

The court first noted that while "increased risk" of identity theft is "too speculative" of an injury to be cognizable, injury resulting from *actual* identity theft, or an "imminent threat" of identity theft, is cognizable. Critically, the court concluded that when cyber criminals target and extract payment data, whether encrypted or unencrypted, "[t]he only reasonable inference to draw from this is that they did not do so out of idle curiosity, but rather to access the payment card information and commit fraud."

Bank of Louisiana, and presumably other victims of malicious cyberattacks, can use that inference to assert claims in court due to the imminent threat of identity theft, and potentially recover costs and expenses from the entity that caused the injury and their insurance companies. Thus a company that suffers a breach that exposes other parties' data may be held liable for the expense those parties undertake to mitigate damage from the breach, whether or not the stolen data is ever used for harm.

ANDERSON KILL
1251 Avenue of the Americas
New York, NY 10020
(212) 278-1000

ANDERSON KILL
1760 Market Street, Suite 600
Philadelphia, PA 19103
(267) 216-2700

ANDERSON KILL
1055 Washington Boulevard, Suite 510
Stamford, CT 06901
(203) 388-7950

ANDERSON KILL
1717 Pennsylvania Avenue, NW, Suite 200
Washington, DC 20006
(202) 416-6500

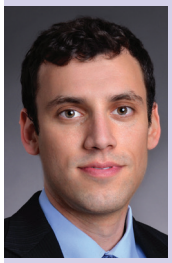
ANDERSON KILL
One Gateway Center, Suite 1510
Newark, NJ 07102
(973) 642-5858

ANDERSON KILL
Wells Fargo Building
355 South Grand Avenue, Suite 2450
Los Angeles, CA 90071
(213) 943-1444

www.andersonkill.com

who's who

Pamela D. Hans is the managing shareholder of Anderson Kill's Philadelphia office. Her practice concentrates in the area of insurance coverage exclusively on behalf of policyholders. Her clients include utilities, mining companies, home builders, non-profit organizations, ethanol producers, commercial lenders, and hog processors, whom she has represented in disputes with their insurance companies.
phans@andersonkill.com
(267) 216-2720



Bruce Strong is an attorney in Anderson Kill's New York and Philadelphia offices. Mr. Strong's practice concentrates in insurance recovery exclusively on behalf of policyholders and in corporate and commercial litigation.
bstrong@andersonkill.com
(212) 278-1034

One significant wrinkle in this case was that Marriot argued that Bank of Louisiana could not trace its injury to *this specific* cyberattack because Bank of Louisiana was also a victim of the Equifax cyberattack, and would not be able to distinguish any injury specifically caused by the Marriot attack. The court rejected this argument at the motion to dismiss stage, but the fact that Marriot even raised this issue shows how prevalent cyberattacks are becoming. No longer are businesses isolated random victims of attacks — they are constantly attacked. Robust legal mechanisms must be in place to help cyberattack victims recover.

Ransomware Attack: Damage Beyond the Ransom

In *Nat'l Ink & Stitch, LLC v. State Auto Prop. & Cas. Ins. Co.*,[2] a hacker perpetrated a ransomware attack on a U.S. business, National Ink & Stitch, locking out the business from its own computer system. In exchange for bitcoin, the hacker agreed to release the computer system back to the control of the owner. After Ink & Stitch paid the ransom, the hacker eventually restored modest control of the computer system, but issues remained. Ink & Stitch still could not access all its files, the computer system ran much slower, and tech experts confirmed that dormant remnants of ransomware virus could re-infect the entire system at any time. The only solution was to wipe the system or get a brand new one.

Unfortunately, these attacks have become the new normal for U.S. businesses. One day a business has a profitable enterprise, the next day, they can't even turn on their computers. While this development could devastate a business in any context, in the new COVID-19 pandemic world, where businesses rely primarily, if not exclusively, on computer or cloud platforms, these attacks can force a company out of business. That raises the stakes on an insurance claim.

Various lines of insurance coverage — including but not limited to specialty cyber insurance policies — may provide coverage for damage and liability caused by cyberattacks. In this case, Ink & Stitch filed a claim under a businessowners policy with a computer coverage endorsement that expressly covered damage to electronic media and records and data stored on such media. Nonetheless, the insurance company, State Auto Property and Casualty Insurance, denied coverage, arguing that the damage to Ink & Stitch's computer system — the lost files, the slower processing speeds, and the dormant virus that could disable the computer system at any time — were not "direct physical loss of or damage to" the computer system under the insurance company's standard "businessowner's insurance policy."

The court disagreed, finding that "the more persuasive cases are those suggesting that loss of use, loss of reliability, or impaired functionality demonstrate the required damage to a computer system" to trigger this type of policy, requiring the insurance company to cover such losses and damage.

This case underscores that cyber-specific coverage may come in many forms; and many policy types, including property, general

liability, D&O, and crime policies, may offer coverage for different aspects of the loss and liability stemming from an attack. Businesses need to assess their prevalent risks and consider which types of policies provide the coverage they need.

The case also illustrates, however, that purchase of policies that expressly cover the salient risks does not guarantee coverage. Policyholders should not take a coverage denial at face value without close analysis of the policy language.

ENDNOTES

1 438 F. Supp. 3d 433 (D. Md. 2020)

2 435 F. Supp. 3d 679 (D. Md. 2020),

We invite you to contact the newsletter's editor, Pamela Hans, at phans@andersonkill.com or (267) 216-2720, with your questions and/or concerns.