# JOURNAL OF EMERGING ISSUES IN LITIGATION

Tom Hagy
Editor-in-Chief

Volume 2, Number 1
Winter 2022



fastcase FULL COURT PRESS

# Journal of Emerging Issues in Litigation

Volume 2, No. 1 Winter 2022

JOURNAL OF EMERGING ISSUES IN LITIGATION at $395.00 annually is published four times per year by Full Court Press, a Fastcase, Inc., imprint.  For customer support, please contact Fastcase, Inc., 711 D St. NW, Suite 200, Washington, D.C. 20004, 202.999.4777 (phone), 202.521.3462 (fax), or email customer service at support@fastcase.com.

Publishing Staff
Publisher: Morgan Morrissette Wright
Production Editor: Sharon D. Ray
Cover Art Design: Morgan Morrissette Wright and Sharon D. Ray

Cite this publication as:

Journal of Emerging Issues in Litigation (Fastcase)



A Full Court Press, Fastcase, Inc., Publication

Editorial Office

711 D St. NW, Suite 200, Washington, D.C. 20004
https://www.fastcase.com/

POSTMASTER: Send address changes to JOURNAL OF EMERGING ISSUES IN LITIGATION, 711 D St. NW, Suite 200, Washington, D.C. 20004.

**Articles and Submissions**

Direct editorial inquiries and send material for publication to:

Tom Hagy, Editor-in-Chief, tom.hagy@litigationconferences.com

Material for publication is welcomed—articles, decisions, or other items of interest to attorneys and law firms, in-house counsel, corporate compliance officers, government agencies and their counsel, senior business executives, scientists, engineers, and anyone interested in the law governing artificial intelligence and robotics. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the Editorial Content appearing in these volumes or reprint permission, please contact:

Morgan Morrissette Wright, Publisher, Full Court Press at mwright@fastcase.com or at 202.999.4878

For questions or Sales and Customer Service:

Customer Service
Available 8am–8pm Eastern Time
866.773.2782 (phone)
support@fastcase.com (email)

Sales
202.999.4777 (phone)
sales@fastcase.com (email)

# To Pay or Not to Pay: Does Your Insurance Policy Cover Ransomware Losses?

Pamela D. Hans*

*Abstract:* *Ransomware attacks are a rapidly growing threat against organizations. Paying ransom demands is a risky proposition and may even lead to sanctions against the targeted company. Either way, the damage to a company's operation and integrity can be cripplingly severe. Should a company suffer losses from cyber extortion, its insurance company will be one of the resources it turns to for relief. But with cyber coverage increasingly out of reach for some, policyholders may find coverage in more traditional coverages. In this article, the author evaluates the potential for coverage under several policy types, and underscores the importance of understanding policy language, the relevant law, and the potential regulatory ramifications of meeting ransom demands.*

While the COVID-19 pandemic brought some industries to a near or complete halt, it's as if it had the opposite effect on busy cybercriminals who continued to wreak havoc around the world. The *Wall Street Journal* has reported that ransomware attacks have increased by 300 percent in the past year.[1] Due to desired secrecy among both targets and perpetrators, precise data on ransomware attacks is not readily available. However, one study estimated that companies paid at least $350 million in online extortions during 2020 alone,[2] and cybersecurity officials have estimated that the damage to the U.S. economy was in the billions of dollars.[3] Relatedly, cyber insurance policy premiums continue to rise, with higher policy limits becoming increasingly difficult to procure. Many companies, however, do not realize that they may recover losses under more "traditional" insurance policies.

*Journal of Emerging Issues in Litigation* / Winter 2022, Vol. 2, No. 1, pp. 37–45.

In the typical ransomware attack, a hacker invades a network, encrypts files, and seeks payment (usually in the form of cryptocurrency) to decrypt them. Some cybercriminals also threaten to release sensitive or confidential information they have exfiltrated from the policyholder's network and demand additional ransom. As the use of preventive measures to avert ransomware attacks becomes increasingly important, companies should likewise be fully prepared for the aftermath of an attack. No matter how sophisticated a company's network may be, the likelihood it will be the target of a ransomware attack is high.[4] While often overlooked, insurance can play a pivotal role in a company's preparation plan.

A thorough understanding of a company's insurance policies is essential to mitigate the costs associated with ransomware attacks.

This article provides a brief overview of the primary policies available to recover losses from cyber incidents and examines potential legal ramifications of ransomware payments.

## Coverage Under CGLs Versus Crime Policies Versus Under Cyber Liability Network Security Policies

Companies that want to protect themselves against first- and third-party losses incurred as potential victims of cyber attacks may seek to purchase an insurance policy. There are different types of policies, both traditional and those that address cyber exposure directly. Notably, policyholders may seek to recoup their losses under a Commercial General Liability (CGL) policy, a Commercial Crime policy, or a Cyber Liability and Network Security policy.

## Commercial General Liability Policies

Companies usually purchase CGLs to protect themselves against potential liability to third parties. A type of standard-form policy provision, known as "Coverage A," provides insurance for "property damage" caused by an "occurrence" as defined in the policy.[5] When it comes to ransomware, the issue with this kind of policy is whether the terms "property damage" and "occurrence" apply

to loss of electronic or software programs by cyber attacks.[6] Additionally, Coverage A policies could expressly exclude insurance for ransomware payments and cyber-related losses in general. Coverage for cyber risks under CGLs is rare but depends on the specific circumstances surrounding the claim, as well as on the terms and exclusions of each policy, and the applicable law. If coverage is found under the CGL policy, it may not contain first-party coverage.

## Commercial Crime Policies

Commercial crime policies predate the insurgence of cybercrime. They were created decades ago primarily to insure the policyholder against theft, fraud, and forgery of company assets by both an employee and other third parties.[7] The classic example is an individual or entity posing as the policyholder (or one of its employees) or its bank to embezzle money.

Nowadays, crime policies can also include fraudulent instruction, funds transfer, and telephone fraud insurance, which covers the loss of company assets transferred by unauthorized use of a computer. These provisions, however, typically require the transfer to be "direct" and "fraudulently caused."[8] Issues arise as to whether policyholders are entitled to recover ransom payments under commercial crime policies. Most policyholders do not realize that should coverage be afforded under the crime policy for the ransom payment, tangential costs (such as legal, incident response, public relations, business interruption, etc.) would not be covered.[9] Insurance companies resist application of these policies to ransomware losses on the grounds that the losses were not caused directly by unauthorized use of a computer, or that they were not fraudulently caused.

## Cyber Liability and Data Security Policies

Cyber policies are a relatively recent type of insurance contract, specifically created to protect an organization's intangible assets from a data breach or other cyber attacks. They may contain both first-party and third-party provisions, which insure loss of

data or network interruption (first party), and liability to third parties arising from data loss or theft (third party).[10] In addition, cyber liability policies can insure incidental costs associated with ransomware attacks, such as payment of brokering fees associated with the procurement of cryptocurrency, legal costs, computer-forensic expertise and expenses, and dependent business interruption losses.[11]

The main difference between a crime policy and a cyber liability policy is that crime policies insure against the *direct* loss of funds, whereas cyber policies insure against *indirect* losses, usually economic losses due to a system failure or privacy controls. Another difference between crime and cyber policies is that the first generally cover losses of *tangible* property (usually money or securities), while the latter cover losses of *intangible* property (e.g., sensitive or confidential information).[12] However, because of the evolving laws surrounding cyber risks there is a lot of overlap between crime- and cyber-related losses. Thus, the line between the two types of policies has become blurred, and many cyber attacks can trigger both cyber and criminal policies.

## G&G Oil Co. v. Continental Western Ins. Co.

In March 2021, the Indiana Supreme Court opened the possibility of insurance coverage for payment of ransom to cybercriminals under commercial criminal policies. In *G&G Oil Co. v. Continental Western Ins. Co.*, a company was locked out of its computer systems by a ransomware attack.[13] After negotiations with the attackers and consultations with the FBI, G&G had to pay $35,000 ransom in bitcoin to obtain a decryption key from the cybercriminals. Later, G&G filed a claim with its insurance company to recover the ransom under a commercial criminal policy.[14] The insurance company denied the claim on the grounds that the policyholder's loss was not fraudulently conveyed as required by the policy and that the loss was not directly caused by unauthorized use of a computer, as the transfer of money was made voluntarily by the policyholder.[15]

The Indiana Supreme Court held that "fraudulently cause a transfer" means "to obtain by trick."[16] Thus, the Court concluded, if G&G could show that the hackers had gained control of its computer

system by trick, the crime policy was triggered. Additionally, the Court interpreted the word "directly" to mean "immediately or proximately without significant deviation from use of a computer," and found the payment was not truly voluntary but was made under duress.[17] As such, the Court found G&G's ransom payment was sufficiently close to the alleged unauthorized use of a computer. This case is significant because it has recognized that policyholders are not limited to cyber policies but may recover losses related to cyber attacks under "traditional" policies as well.

## Should Ransom Be Paid?

Policyholders must consider regulatory and legal ramifications of paying ransom. While they may be able to recover payments to cyber attackers through their insurance policies, paying ransom may lead to sanctions or even criminal charges.[18] The Office of Foreign Asset Control (OFAC) is a federal agency within the Treasury Department in charge of implementing economic and trade sanctions against countries and individuals (e.g., terrorists and hackers) that are imposed by the U.S. government based on foreign policy and national security considerations.[19] In the field of cybercrimes, OFAC maintains a list of perpetrators and facilitators of ransomware attacks and transactions designated as "malicious cyber actors."[20] Those actors and anyone assisting them is sanctioned under relevant agency guidance and federal law. Specifically, pursuant to a number of federal anti-corruption regulations and sanctions laws,[21] it is illegal to make ransom payments to foreign terrorist organizations, or global terrorists specially designated by OFAC. It does not matter whether these payments are made directly or indirectly through an intermediary (such as an insurance company), or whether the policyholder knows that a payment is being made to a prohibited organization or person. The rationale behind these sanctions is based not only on an attempt to prevent future attacks by recurrent bad faith actors, but to protect against funding of terrorist or criminal activities "adverse to the national security and foreign policy objectives of the United States."[22] OFAC has recently strengthened its guidance to discourage payment of

ransomware by policyholders, forensics investigators, and insurance companies.[23]

These regulations present several problems for incident response firms and insurance companies alike. First, it can be very difficult for policyholders to unmask the identity of anonymous attackers.[24] As such, policyholders who are victims of ransom attacks may not always know whether the attacker is part of OFAC's list of malicious cyber actors. Second, because the attacked network generally cannot be independently decrypted, critical data will be inaccessible until satisfaction of the ransom. By discouraging payment of ransomware, OFAC guidance has the effect of exponentially increasing business interruption costs as companies remain locked out of essential data.[25] Third, because it may be more cost-effective to pay ransom, insurance companies are incentivized to raise premiums and limit insurance coverage.[26] It is a common practice in the cyber insurance marketplace for insurance companies to introduce co-insurance on extortion (ransom) coverage, sublimate the coverage, or remove it altogether. Because of the rising number of extortion claims both in frequency and severity, insurance companies have changed their underwriting guidelines. Many now require separate supplemental applications regarding controls the policyholder has in place to mitigate the threat of ransomware claims. For example, many insurance companies require policyholders to implement multifactor authentication before providing terms.[27]

On the other hand, ransom payments may do more harm than good. As evidenced by the Colonial Pipeline attack in April 2021, ransom payments embolden hackers to expand their criminal enterprise to more high-profile targets (like critical infrastructure),[28] re-target previously attacked companies, and increase their ransom demands.[29] Moreover, paying ransom does not guarantee a company will regain access to the encrypted data. Companies cannot be sure that the hacker will give a working decryption key once payment is made. Additionally, more sophisticated ransomware attacks can hide a second layer of malware. After a company pays a first ransom, the first layer of encryption is removed, but data remains inaccessible, and the company will have to pay additional ransom for a new decryption key.[30] According to experts, there are

also a number of hackers posing as legitimate companies offering (non-working) decryption tools for a fee.[31]

## What Should Companies Do?

Unfortunately, maintaining proper cyber hygiene to prevent cyber attacks is not always sufficient. Hackers are getting more and more sophisticated, and the chances of being the target of a ransomware attack are very high. A company that does not have a standalone cyber insurance policy is not necessarily left to hang dry. Many policyholders do not realize their CGLs and commercial crime policies cover losses relating to ransomware attacks. Companies should also beware of potential sanctions and criminal liability arising out of ransom payments. A thorough understanding of the policy language, the relevant law, and potential regulatory ramifications is fundamental to ensure maximum protection against cyber attacks.

## Notes

* Pamela D. Hans (phans@andersonkill.com) is the managing shareholder of Anderson Kill's Philadelphia office. Her practice concentrates on insurance coverage exclusively on behalf of policyholders. Pam is also a member of the firm's COVID Task Group and Cyber Recovery Group.

1. James Rundle & David Uberti, *How Can Companies Cope With Ransomware?* Wall St. J. (May 9, 2021), https://www.wsj.com/articles/how-can-companies-cope-with-ransomware-11620570907.

2. Chainalysis Team, *Ransomware Skyrocketed in 2020, But There May Be Fewer Culprits Than You Think*, Chainalysis Insights (Jan. 26, 2021), https://blog.chainalysis.com/reports/ransomware-ecosystem-crypto-crime-2021.

3. Robert McMillan et al., *Beyond Colonial Pipeline, Ransomware Cyberattacks Are a Growing Treat*, Wall St. J. (May 11, 2021), https://www.wsj.com/articles/colonial-pipeline-hack-shows-ransomware-emergence-as-industrial-scale-threat-11620749675#:~:text=While%20

precise%20data%20on%20attacks,to%20the%20blockchain%20analysis%20firm.

4. Scott Calvert & Jon Kamp, *More U.S. Cities Brace for "Inevitable" Hackers*, Wall St. J. (Sept. 4, 2018, 5:20 PM), https://www.wsj.com/articles/more-cities-brace-for-inevitable-cyberattack-1536053401?mod=article_inline.

5. Paul E.B. Glad et al., *Types of Liability Coverage*, 3 New Appleman L. Liab. Ins. § 16.02 (2014).

6. Toni Scott Reed, *Cybercrime and Technology Losses: Claims and Potential Insurance Coverage for Modern Cyber Risks*, 54 Tort Trial & Ins. Prac. L.J. 153, 168 (2019).

7. Robert Persons & Ken Brownlee, *Commercial Crime Insurance*, in Excess Liability Rights & Duties of Commercial Risk Insured & Insurers § 14:16 (4th ed. 2021).

8. *See* Amy S. Malish, *Navigating Cyber Coverages for Modern Day Cybercrimes*, 54 Tort & Ins. L.J. 911 (2019).

9. *See* Jeffrey S. Price & Justing D. Wear, *Claims Made and Insurance Coverage Available for Losses Arising Out of or Related to Electronic Data*, 51 Tort & Ins. L.J. 51 (2015).

10. Roberta D. Anderson, *Viruses, Trojans, and Spyware, Oh My! The Yellow Brick Road to Coverage in the Land of Internet Oz*, 49 Tort & Ins. L.J. 529, 592-93 (2014).

11. Scott Calvert, *Baltimore to Buy $20 Million in Insurance in Case of Another Cyber Attack*, Wall St. J. (Oct. 16, 2019), https://www.wsj.com/articles/baltimore-to-buy-20-million-in-insurance-in-case-of-another-cyber-attack-11571246605; Reed, *supra* n. 7, at 170.

12. Anderson, *supra* n. 11, at 590-93.

13. 165 N.E.3d 82 (Ind. 2021).

14. *See id.* at 85-86.

15. *See id.* at 86.

16. *Id.* at 89.

17. *Id.* at 90.

18. Department of the Treasury, *Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments* (Oct. 1, 2020) [hereinafter OFAC Advisory], https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf.

19. *OFAC Consolidated Frequently Asked Questions*, U.S. Dep't of the Treasury, https://home.treasury.gov/policy-issues/financial-

sanctions/frequently-asked-questions/ofac-consolidated-frequently-asked-questions (last visited Aug. 2, 2021).

20. *Id.*

21. *See, e.g.*, Trading With the Enemy Act, 50 U.S.C. § 4301 et seq.; International Emergency Economic Power Act (IIEPA), 50 U.S.C. § 1701 et seq.

22. OFAC Advisory, *supra* n. 15, at 3.

23. *Id.*

24. John Reed Stark, *An OFAC Compliance Checklist for Ransomware Payments*, Law360 (Feb. 2, 2021), https://www.law360.com/articles/1349647/an-ofac-compliance-checklist-for-ransomware-payments.

25. James Rundle et al., *As Ransomware Proliferates Insuring for It Becomes Costly and Questioned*, Wall St. J. (May 12, 2021), https://www.wsj.com/articles/as-ransomware-proliferates-insuring-for-it-becomes-costly-and-questioned-11620811802.

26. Frank Bjak, *Insurer AXA to Stop Paying for Ransomware Crime Payments in France*, Ins. J. (May 9, 2021), https://www.insurancejournal.com/news/international/2021/05/09/613255.htm#.

27. Rachel Lerman & Gerrit De Vynck, *Ransomware Claims Are Roiling an Entire Segment of the Insurance Industry*, Wash. Post (June 17, 2021), https://www.washingtonpost.com/technology/2021/06/17/ransomware-axa-insurance-attacks/.

28. *The Ruthless Hackers Behind Ransomware Attacks on U.S. Hospitals: "They Do Not Care"*, Wall St. J. (June 10, 2021), https://www.wsj.com/articles/the-ruthless-cyber-gang-behind-the-hospital-ransomware-crisis-11623340215.

29. Andrew Ross Sorkin et al., *The Debate Over Hacking Ransomware Hackers*, N.Y. Times (June 8, 2021), https://www.nytimes.com/2021/06/08/business/dealbook/fbi-ransomware-crypto.html?searchResultPosition=9.

30. Lily Hay Newman, *Ransomware's Dangerous New Trick Is Double-Encrypting Your Data*, Wired (May 17, 2021), https://www.wired.com/story/ransomware-double-encryption/.

31. Rundle & Uberti, *supra* n. 1.