IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
NEWNAN DIVISION

SOUTHWIRE COMPANY, LLC, *Plaintiff*, v. **JOHN DOE**, In Possession of Stolen Southwire Confidential Information, Thereby Injuring Southwire and Its Customers, Clients, and Vendors, *Defendant*.	Civil Action No. JURY TRIAL DEMANDED

COMPLAINT

Plaintiff Southwire Company, LLC ("Southwire" or "Plaintiff") hereby complains and alleges against John Doe ("Defendant"), as follows:

NATURE OF THE ACTION

1. This is a civil action for injunctive relief and damages against Defendant arising under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, and the common law of trespass to chattels. As further alleged below, Defendant wrongfully accessed Southwire's computer systems and extracted Southwire's confidential business information and other sensitive information from the computer systems. Defendant then demanded several million dollars to keep the

information private, but after Southwire refused Defendant's extortion, Defendant wrongfully posted part of Southwire's confidential information on a publicly-accessible website that Defendant controls. Unless enjoined from further exposing this information to the public, Defendant likely will continue to post more of Southwire's confidential and sensitive information on Defendant's publicly-accessible website, causing substantial, imminent, and irreparable harm to Plaintiff.

THE PARTIES

2. Plaintiff Southwire Company, LLC is a prominent cable and wire manufacturer. Southwire is a Delaware corporation with its principal place of business at One Southwire Drive, Carrollton, Georgia 30119, USA.

3. On information and belief, Defendant controls the [redacted] domain that is being used to cause harm to Southwire, its customers, and the public. Southwire is informed and believes and thereupon alleges that John Doe can likely be contacted via web portal available at [redacted]. Southwire is unaware of the true name(s) of Defendant sued herein as John Doe and, therefore, sues this

Defendant under a fictitious name.[1] Plaintiff will amend this Complaint to allege the true name and capacity of Defendant when ascertained. Plaintiff has exercised due diligence and will continue to exercise due diligence to determine Defendant's true name(s), capacity, and contact information, and to effect service on that Defendant.

4. On information and belief, the fictitiously named Defendant is responsible for the occurrences herein alleged, and Southwire's injuries as herein alleged were proximately caused by such Defendant.

5. On information and belief, third-party [redacted], is a domain name registrar that provides domain-name registration and web-hosting services to individuals and companies. [redacted] is the administrator of the IP address [redacted]—connected to domain [redacted]—used by Defendant in this action. [redacted] has operated subdomain services through that domain directed at the United States and Georgia. Based on information and belief, Plaintiff asserts that [redacted] is located in [redacted].

[1] The gender-neutral "they" and "their" pronoun is used throughout this Complaint because Plaintiff is unaware of Defendant's identity (which could be an individual or a group).

6. On information and belief, the actions and omissions alleged herein to have been undertaken by Defendant and their agents were actions that Defendant authorized, controlled, directed, or had the ability to control, direct, and/or were actions and omissions Defendant assisted, participated in, or otherwise encouraged, and are actions for which Defendant is liable.

JURISDICTION AND VENUE

7. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1331, as the action arises under the federal Computer Fraud and Abuse Act (18 U.S.C. § 1030) ("CFAA"). This Court has subject-matter jurisdiction under 28 U.S.C. § 1367 over the claim for trespass to chattels, which forms part of the same case or controversy as the CFAA claim.

8. This Court has personal jurisdiction over Defendant as a result of the Defendant's unauthorized access into, and misappropriation of information from, a "protected computer" as defined in 18 U.S.C. § 1030(e)(2)(B) that is used for commerce and communication with persons and entities in Georgia, and also as a result of Defendant's wrongful conduct causing injurious effect in Georgia.

9. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(b). A substantial part of the events or omissions giving rise to Southwire's

claims occurred in this judicial district. Additionally, a substantial part of the property that is the subject of Southwire's claims is situated in this judicial district.

FACTS

10. Ransomware is a type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid. Ransomware typically spreads through phishing emails or by unknowingly visiting an infected website.

11. On or about [redacted], Southwire learned of the unauthorized access to and exfiltration of its data when a variant of ransomware software known as "Maze Ransomware" was executed on [redacted]. When Maze Ransomware was executed on Southwire's systems, it encrypted Southwire's files, causing Southwire to lose access to the data stored on these systems. (*See* **Exhibit A**).

12. The breached machines, or computers, are "protected computers" under 18 U.S.C. § 1030(e)(2)(B), which defines a "protected computer" as a computer "which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communications to the

United States." The breached computers are used for interstate and foreign commerce or communication.

13. Since discovering the incident, Southwire acted promptly to prevent the spread of the Maze Ransomware and undertook an investigation to try to determine the identity of the intruder, the precise scope of the intrusion, and the extent of the damages. This investigation is ongoing.

14. Based on this investigation to date, Southwire has determined that Defendant accessed Southwire's systems without authorization and [redacted]

15. After stealing Southwire's data and deploying the Maze Ransomware, Defendant demanded from Southwire a payment of [redacted] in exchange for decrypting Southwire's data and not releasing Southwire's confidential and sensitive information to the public. Southwire refused to pay Defendant.

16. Defendant erected a website on the public Internet — [redacted] — which, as of [redacted], listed the company names and corresponding websites for twenty-seven victims of its malware that have declined to pay a ransom demand, including Southwire. On information and belief, the information on the website includes [redacted].

17. From on or about [redacted], Plaintiff communicated with Defendant about recovering the stolen information, and Defendant continued to request a ransom payment in exchange for not releasing Plaintiff's confidential and sensitive information on the public Internet. During this time, Defendant threatened to release this information and pointed to its release of other companies' data as an indicator that it would follow through on its threats.

18. After Plaintiff did not pay the ransom demanded by Defendant, a portion of Plaintiff's stolen confidential and sensitive information was publicly posted to [redacted]. (*See* **Exhibit B**). Defendant has threatened to expose further confidential and sensitive information to the public if the ransom

payment is not made in the coming days. [redacted].

19. Plaintiff has already been irreparably harmed by Defendant's illegal misappropriation and public dissemination of Southwire's data. To date, Plaintiff has spent a substantial sum of money (far in excess of $5,000) to investigate the incident and to remediate the damage Defendant has caused and is in the position to further cause. Additionally, news of the incident and the Defendant's exploits has been spread to various media outlets by the Defendant in an effort to harm Southwire's reputation and alarm its customers, vendors, and employees.

FIRST COUNT – VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT (18 U.S.C. § 1030)

20. Southwire realleges and incorporates by reference the allegations contained in paragraphs 1 through 19 above.

21. Title 18, United States Code, Section 1030(g) provides that "any person who suffers damage or loss by reason of a violation of this security may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." Under 18 U.S.C. § 1030(g), (a)(2)(C), and (c)(4)(A)(i)(I), a civil action may be brought if the conduct involves a loss during any one-year period aggregating at least $5,000 in value.

22. Defendant violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2)(C), by knowingly and intentionally accessing Southwire's protected computers without authorization or in excess of any authorization and thereby obtaining information from the protected computers in a transaction involving an interstate or foreign communication.

23. Defendant violated the Computer Fraud and Abuse Act, 18 U.S.C. 1030(a)(5)(B), by intentionally accessing protected computers without authorization, and as a result of such conduct, recklessly causing damage to Plaintiff.

24. Defendant violated the Computer Fraud and Abuse Act, 18 U.S.C. 1030(a)(5)(C), by intentionally accessing protected computers without authorization, and as a result of such conduct, causing damage and loss to Plaintiff.

25. Defendant's conduct has caused a loss to Plaintiff during a one-year period aggregating at least $5,000 in value.

26. Plaintiff has suffered damages resulting from Defendant's conduct.

27. Plaintiff seeks compensatory and punitive damages under 18 U.S.C. § 1030(g) in an amount to be proven at trial.

28. As a direct result of Defendant's actions, Plaintiff has suffered and continues to suffer irreparable harm for which Plaintiff has no adequate remedy at

law. Plaintiff will continue to suffer irreparable harm until an injunction issues against Defendant.

SECOND COUNT – TRESPASS TO CHATTELS

29. Plaintiff realleges and incorporates by reference the allegations contained in paragraphs 1 through 19 above.

30. Defendant's actions in infiltrating Plaintiff's systems to execute Maze Ransomware resulted in Defendant's unauthorized access to Southwire's computers and servers.

31. Defendant intentionally caused this conduct, and this conduct was unauthorized.

32. Defendant's actions have caused injury to Southwire and imposed substantial costs on Southwire, including time, money, and a burden on Southwire's computers, as well as injury to Southwire's business goodwill. Also, Defendant's actions have diminished the value of Southwire's possessory interest in its computers and servers.

33. As a result of Defendant's unauthorized and intentional conduct, Southwire has been damaged in an amount to be proven at trial.

34. As a direct result of Defendant's actions, Southwire has suffered and continues to suffer irreparable harm for which Southwire has no adequate remedy

at law. Plaintiff will continue to suffer irreparable harm until an injunction issues against Defendant.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Southwire prays that the Court:

a. Enter judgment in favor of Southwire and against the Defendant;

b. Declare that Defendant's conduct has been willful and that Defendant has acted with fraud, malice, and oppression;

c. Enter a preliminary and permanent injunction enjoining Defendant and their officers, directors, principals, agents, servants, employees, successors, and assigns, and all persons and entities in active concert or participation with them, from engaging in any of the activity complained of herein or from causing any of the injury complained of herein and from assisting, aiding or abetting any other person or business entity in engaging in or performing any of the activity complained of herein or from causing any of the injury complained of herein;

d. Order that Defendant and their officers, directors, principals, agents, servants, employees, successors, and assigns, and all persons and entities in active concert or participation with them, immediately deliver to Plaintiff: (i) all copies of the data stole from Southwire's systems; and (ii)

all copies of any materials (in paper, electronic, or any other form) that contain or reflect any information derived from Southwire's data.

e. Award Plaintiff a money judgment that includes (a) disgorgement of the Defendant's profits; (b) compensatory damages; (c) enhanced, exemplary, special, and punitive damages; (d) attorney's fees, costs, and expenses; and (e) interest.

f. Award Plaintiff any and all other relief to which Plaintiff is entitled.

Respectfully submitted on December 31, 2019.

/s/ Jonathan S. Klein
Jonathan S. Klein (Georgia Bar No. 540895)
jklein@mayerbrown.com
MAYER BROWN LLP
1999 K Street N.W.
Washington, D.C. 20006
T: (202) 263-3327
F: (202) 403-3232

Marcus A. Christian (*pro hac vice* forthcoming)
mchristian@mayerbrown.com
MAYER BROWN LLP
1999 K Street N.W.
Washington, D.C. 20006
T: (202) 263-3731
F: (202) 263-5371

Counsel for Plaintiff Southwire Company, LLC