E-FILED
Wednesday, 06 July, 2022 05:03:49 PM
Clerk, U.S. District Court, ILCD

IN THE UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF ILLINOIS
URBANA DIVISION

TRAVELERS PROPERTY CASUALTY COMPANY OF AMERICA, Plaintiff, v. INTERNATIONAL CONTROL SERVICES, INC., Defendant.	Case No.

COMPLAINT FOR RESCISSION
AND DECLARATORY JUDGMENT

Travelers Property Casualty Company of America ("Travelers"), for its Complaint for Rescission and Declaratory Judgment against defendant International Control Services, Inc. ("ICS") alleges as follows:

NATURE OF THIS ACTION

1. Travelers brings this lawsuit to (1) rescind a CyberRisk Tech insurance policy Travelers issued to ICS (the "Policy") and (2) obtain a judicial determination and declaration, pursuant to 28 U.S.C. §§ 2201 and 2202, with respect to the rights and obligations of the parties concerning a ransomware event that targeted ICS computer systems.

2. Specifically, Travelers seeks to rescind the Policy because of material misrepresentations, omissions, concealment of facts and incorrect statements in connection with ICS's application for the Policy.

PARTIES

3. Travelers is an insurance company incorporated under the laws of the State of Connecticut and maintains its principal place of business in Hartford, Connecticut. Travelers is, therefore, a citizen of Connecticut.

4. ICS is a corporation organized and existing under the laws of the State of Delaware, and maintains its principal place of business in Illinois. ICS is, therefore, a citizen of Delaware and Illinois.

JURISDICTION AND VENUE

5. Federal subject matter jurisdiction exists in this action, pursuant to 28 U.S.C. § 1332, because it is an action between citizens of different states, and the amount in controversy exceeds $75,000, exclusive of interest and costs.

6. Pursuant to 28 U.S.C. § 1391(b)(2), venue is proper in this district because a substantial part of the events giving rise to Travelers' claim for rescission and declaratory relief occurred in this district.

THE INSURANCE APPLICATION

7. ICS submitted to Travelers a CyberRisk Tech Application, dated March 31, 2022, and signed by ICS's Chief Executive Officer, Dennis Espinoza ("Espinoza"), seeking a Travelers insurance policy to insure ICS against certain cybersecurity risks (the "Application"). A true and correct copy of the Application is attached to this Complaint as **Exhibit 1**.

8. In response to Question 41 of the Application, ICS listed Espinoza, along with "Bill Zimmerman," as "the person responsible for the Applicant's network and information security."

9. In the Application, ICS answered "Yes" to the following question:

> 60. Indicate whether the Applicant requires multi-factor authentication for:
> a. Administrative or privileged access

10. Above Espinoza's signature, the Application states, in relevant part, as follows:

> The undersigned Authorized Representative represents that to the best of his or her knowledge and belief, and after reasonable inquiry, the statements provided in response to this Application are true and complete, and, except in NC, may be relied upon by Travelers as the basis for providing

> insurance. The Applicant will notify Travelers of any material changes to the information provided.

11. In connection with the Application, and at Travelers' request, ICS provided Travelers with a Multi-Factor Authentication Attestation, dated March 10, 2022 and bearing Espinoza's signature (the "MFA Attestation"). The Application and the MFA Attestation are collectively referred to as the "Application Documents". A true and correct copy of the MFA Attestation is attached to this Complaint as **Exhibit 2**.

12. As explained in the MFA Attestation, multi-factor authentication refers to the use of two or more means of identification and access control in order to successfully verify a user's identity when accessing systems.

13. The MFA Attestation identified the importance of requiring multi-factor authentication for various systems, specifically explaining that:

a. Requiring multi-factor authentication for remote access is an important security control that can help reduce the potential for a network compromise caused by lost or stolen passwords;

b. Requiring multi-factor authentication for both remote and internal access to administrative accounts helps to prevent intruders that have compromised an internal system from elevating privileges and obtaining broader access to a compromised network, and can prevent an intruder from gaining the level of access necessary to successfully deploy ransomware across the network; and

c. Requiring multi-factor authentication for remote access to email can help reduce the potential for compromise to corporate email accounts caused by lost or stolen passwords, and that without this control an intruder can easily gain access to a user's corporate email account.

14. The MFA Attestation further provided as follows with respect to the importance of multi-factor authentication and the minimum controls required in order for an applicant to be eligible for a policy:

> The controls described above and listed below are the minimum controls that must be in place in order to be eligible for a Cyber

policy. Because of the importance of the controls in preventing ransomware attacks the following attestation should be completed with the assistance of the person(s) in charge of IT security.

15. ICS stated "Yes" to each of the following affirmations listed on the MFA Attestation:

1. Multi-Factor authentication is required for all employees when accessing email through a website or cloud based service.

2. Multi-Factor authentication is required for all remote access to the network provided to employees, contractors, and 3rd party service providers.

3. In addition to remote access, multi-factor authentication is required for the following, including such access provided to 3rd party service providers:
   a. All internal & remote admin access to directory services (active directory, LDAP, etc.).
   b. All internal & remote admin access to network backup environments.
   c. All internal & remote admin access to network infrastructure (firewalls, routers, switches, etc.).
   d. All internal & remote admin access to organization's endpoints/servers.

THE INSURANCE POLICY

16. After receiving the Application Documents, and in reliance on the statements and information contained in them, Travelers issued the Policy, which is a claims-made Travelers CyberRisk Tech Policy, No. ZPL-71N49757-22-I3, originally to be effective April 4, 2022 to April 4, 2023. A true and correct copy of the Policy is attached to and incorporated in this Complaint as **Exhibit 3**.

17. The Declarations included in the Policy lists ICS as the Named Insured.

18. The Policy's aggregate limit of liability for all *Loss* is $1,000,000, subject to applicable Retentions.

MISREPRESENTATIONS REGARDING MULTI-FACTOR AUTHENTICATION

19. In December 2020, ICS was the victim of a ransomware attack (the "2020 Ransomware Event"), during which intruders gained access to an ICS server by using the username and password of an ICS administrator's account (the "Compromised Username/Password").

20. During the Policy application process, ICS disclosed the 2020 Ransomware Event to Travelers and represented to Travelers that ICS had instituted cybersecurity improvements following the 2020 Ransomware Event, including changing the Compromised Username/Password.

21. Beginning on or about May 25, 2022, ICS was once again targeted in another ransomware attack (the "2022 Ransomware Event"), during which intruders gained access to an ICS server (the "Server") and infected it with virus software known as "ZEON."

22. On or about May 31, 2022, ICS notified Travelers of the 2022 Ransomware Event.

23. In the course of Travelers' investigation of the 2022 Ransomware Event, Travelers first learned that at the time ICS completed and submitted the Application Documents, (1) MFA was not being utilized to protect the Server and (2) ICS only utilized MFA to protect its firewall, and did not use MFA to protect any other digital assets.

24. Because MFA was not being utilized to protect the Server and various other digital assets of ICS at the time ICS applied for the Policy, statements ICS made in the Application Documents, set forth in paragraphs 9 and 15 of this Complaint, were misrepresentations, omissions, concealment of facts, and incorrect statements made in applying for the Policy.

COUNT I
(Policy Rescission and Declaratory Judgment)

25. Travelers realleges paragraphs 1-24 above as if set forth fully as this paragraph 25.

26. The Application Documents contained misrepresentations, omissions, concealment of facts, and incorrect statements regarding the extent to which ICS utilized MFA to protect its systems.

27. Each of the above misrepresentations, omissions and incorrect statements materially affected the acceptance of the risk and/or the hazard assumed by Travelers.

28. Had Travelers been made aware that ICS was not using MFA to the extent represented in the Application Documents, Travelers would not have issued the Policy.

29. As a result of the material misrepresentations, omissions, concealment of facts, and incorrect statements in the Application Documents, the Court should rescind the Policy and declare that there is no coverage for any losses, costs or claims submitted by ICS to Travelers for coverage under the Policy, including without limitation, losses, costs or claims relating to the 2022 Ransomware Event.

30. Travelers is tendering to ICS all amounts paid as premium for the Policy.

WHEREFORE, Travelers respectfully requests that the Court enter a judgment:

a. Declaring the Policy null and void;
b. Rescinding the Policy;
c. Declaring that Travelers has no duty to indemnify or defend ICS for any losses, costs or claims under the Policy, including without limitation, any losses, costs or claims resulting from the 2022 Ransomware Event; and
d. Granting such other relief as the Court may deem just and proper.

TRAVELERS PROPERTY CASUALTY COMPANY OF AMERICA

By: */s/ Christopher J. Bannon*
Christopher J. Bannon (ARDC# 6196298)
Samuel R. Leist (ARDC# 6330017)
Aronberg Goldgehn Davis & Garmisa
330 N. Wabash Avenue, Suite 1700
Chicago, IL 60611
(ph.) (312) 755-3175
(fax) (312) 222-6375
cbannon@agdglaw.com
sleist@agdglaw.com
Attorney for Travelers Property Casualty Company of America

4853-4860-1381, v. 2