UNITED STATES DISTRICT COURT
DISTRICT COURT OF MINNESOTA

SJ COMPUTERS, LLC, Plaintiff, v. TRAVELERS CASUALTY AND SURETY COMPANY OF AMERICA, Defendant.	Civil File No. _____ **COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff SJ Computers, LLC ("SJ Computers"), for its Complaint against Defendant Travelers Casualty and Surety Company of America ("Travelers"), alleges as follows:

NATURE OF THE ACTION

1. This is a civil action arising out of Travelers' bad faith refusal to acknowledge its obligation to provide insurance coverage for computer fraud and its failure to pay all amounts due under a crime policy issued to SJ Computers.

2. After discovering that it was the victim of computer fraud in which a bad actor infiltrated its computer systems, intercepted emails between SJ Computers and its vendors, and impersonated a company executive to cause fraudulent wire transfers, SJ Computers sought coverage for social engineering and computer fraud coverage under the Travelers' crime policy.

3. Travelers agreed to pay a portion of SJ Computers' loss under the policy's social engineering coverage, but refused to provide its insured with the computer fraud coverage the policy promised to pay, despite SJ Computers providing prompt notice of the computer fraud and cooperating fully and completely with Travelers' investigation of the computer fraud.

4. Travelers' refusal to pay SJ Computers' loss under the computer fraud coverage constitutes a breach of the policy and its duty of good faith and fair dealing, depriving SJ Computers of the computer fraud coverage it purchased, and forcing SJ Computers to commence this action.

THE PARTIES

5. SJ Computers is a limited liability company organized under the laws of Minnesota with its principal place of business in Eagan, Minnesota.

6. Travelers is an insurance company organized and domiciled under the laws of Connecticut with its principal place of business in Hartford, Connecticut.

JURISDICTION AND VENUE

7. This Court has original jurisdiction pursuant to 28 U.S.C. § 1332 based on complete diversity of citizenship between the parties and because the amount in controversy, exclusive of costs and interest, exceeds $75,000.

8. This Court has personal jurisdiction over Travelers because Travelers has conducted and continues to conduct substantial insurance business throughout Minnesota, including engaging in the business of selling insurance, investigating claims, and issuing policies that cover policyholders or activities in Minnesota.

9. Venue is proper under 28 U.S.C. § 1391, as this is a diversity action and a substantial part of the events leading to this Complaint occurred in this judicial district.

BACKGROUND

A. The Policy

10. In consideration of significant premiums paid to cover the exact type of loss here, Travelers sold SJ Computers Travelers Wrap+® crime insurance policy, number 107244011, for

the policy period February 11, 2021 to February 11, 2022 ("Policy"). A copy of the Policy is attached at **Exhibit 1**.

11. SJ Computers is the named insured under the Policy, and paid all premiums due.[1] The Policy was in full force and effect at all times during the relevant policy period.

12. Under the Policy, Travelers promised to provide coverage for, among other things, an attack on, or hacking of, SJ Computers' computer system in which a bad actor(s) gains unauthorized access of SJ Computers' computer system.

13. The Policy's insuring agreement for the crime coverage part provides that:

> The Company will pay the **Insured** for the **Insured's** direct loss of, or direct loss from damage to, **Money, Securities** and **Other Property** directly caused by **Computer Fraud.**

Id. at SJC-TravPolicy-65 (emphases in original).

14. The Policy defines "Computer Fraud" broadly to mean,

> an intentional, unauthorized, and fraudulent entry or change of data or computer instructions directly into a **Computer System**:
>
> 1. by a natural person or entity, other than an **Employee**, **Authorized Person**, independent contractor, or any individual under the direct supervision of the **Insured**, including any such entity or change made via the internet, provided that such entry or change causes **Money**, **Securities**, or **Other Property** to be transferred, paid, or delivered inside the **Premises** or from the **Insured's Financial Institution Premises**, to a place outside the **Premises** or the **Insured's Financial Institution Premises**; or
>
> 2. made by an **Employee** or **Authorized Person** acting in good faith upon an intentional, unauthorized, and fraudulent instruction received from a computer software contractor who has a written agreement with the **Insured** to design, implement, or service

1 The policy identifies the named insured as "SJ COMPUTER, LLC," but "SJ COMPUTERS, LLC" is the proper, legal name. See Ex. 1 at SJC-TravPolicy-6.

> **Computer Programs** for a **Computer System** covered under section **I. INSURING AGREEMENTS, F. COMPUTER CRIME**.
>
> For purposes of this definition, an intentional, unauthorized, and fraudulent entry or change of data or computer instructions does not include such entry or change made by an **Employee**, **Authorized Person**, independent contractor, or any individual under the direct supervision of the **Insured** made in reliance upon any fraudulent electronic, cable, teletype, telephonic voice, telefacsimile, or written instruction, except as defined in E.2. above. An intentional, unauthorized, and fraudulent entry or change of data or computer instructions also does not include such entry or change that involves the use, or purported use, of any **Credit**, **Debit**, or **Charge Card** or any access, convenience, identification, stored value, or other similar cards, including the information contained on such cards.
>
> Computer Fraud does not include Social Engineering Fraud or Funds Transfer Fraud.

Id. at SJC-TravPolicy-94 (emphases in original) (Computer Fraud definition as amended by the Social Engineering Fraud Insuring Agreement Endorsement); *see also id.* at SJC-TravPolicy-65 & SJC-TravPolicy-69.

15. The Policy defines "Computer System" to mean,

> 1. any computer; and
>
> 2. any input, output, processing, storage, or communication device, or any related network, cloud service, operating system, or application software, that is connected to, or used in connection with, such computer, that is rented by, owned by, leased by, licensed to, or under the direct operational control of, the **Insured**.

Id. at SJC-TravPolicy-93 (emphasis in original) (Computer System definition as amended by the Social Engineering Fraud Insuring Agreement Endorsement); *see also id.* at SJC-TravPolicy-69.

16. The Policy defines "Money" to mean,

> a medium of exchange in current use and authorized or adopted by a domestic or foreign government, including currency, coins, bank notes, bullion, travelers' checks, registered checks and money orders held for sale to the public.

Id. at SJC-TravPolicy-74.

17. "Premises" is defined in the Policy to mean,

> the interior of that portion of any building the **Insured** occupies in conducting the **Insured's** business.

Id. (emphases in original).

18. "Financial Institution Premises" means,

> the interior of that portion of any building occupied by a **Financial Institution** (including any night depository chute and any safe maintained by such **Financial Institution**), transfer agent or registrar or similarly recognized place of safe deposit.

Id. at SJC-TravPolicy-72.

19. The Policy is endorsed to also provide coverage for SJ Computers' direct loss from the transferring, paying or delivering of money, directly caused by social engineering.

B. The Computer Fraud

20. SJ Computers is a personal computer company that provides quality computer products, service, and support to residential and business customers for a low price with a quick turnaround time.

21. As part of its course of business, SJ Computers routinely sends wire transfers of money to vendors for the purchase of computer equipment.

22. As part of this process, SJ Computers' purchasing manager issues purchase orders to vendors for the purchase of certain computer equipment. Upon receipt of the purchase order, vendors issue invoices to SJ Computers for the cost of the computer equipment. The purchasing manager confirms the invoices are accurate, and forwards the invoices to the CEO for payment.

23. Upon receipt of invoices from the purchasing manager, the CEO initiates payment to the vendors via wire transfer from SJ Computers' bank to the designated bank account of the respective vendor. The CEO is the only person responsible for initiating wire transfers to vendors.

24. On or before March 23, 2021, SJ Computers' purchasing manager received an email purportedly from one of SJ Computers' vendors, Electronic Recyclers International Direct ("ERI Direct"), advising that there had been a change in the wire transfer information at its recipient bank used for wire transfers. An investigation later revealed that the email, purportedly from ERI Direct, was from a spoofed email address of "@eridlrect.com," with the word "direct" spelled with a lowercase letter "L," rather than "eridirect.com," with the word "direct" spelled with a lowercase letter "I." The email is attached as **Exhibit 2**.

25. SJ Computers had sent the wire transfer to ERI Direct for the March 23, 2021 invoice, before receiving the email about a change in wire transfer information and data, so no loss was sustained as a result of the bad actor's fraudulent attempt. *See id.* An investigation revealed, however, that the purchasing manager's email account had likely been compromised by that time, with the bad actor(s) having infiltrated SJ Computers' computer system and monitoring the purchasing manager's emails for an opportunity to intercept a wire transfer.

26. A few days later, on March 29, 2021, invoices for another purchase from ERI Direct were sent to the purchasing manager's email account. This time, the invoices had been altered to change the instructions for wire transfer payment. The emails were spoofed, again, and came from an account at "@feaircraft.com." The emails from @feaircraft.com are attached as **Exhibits 3-6**.

27. Subsequently, the bad actor(s)—who was monitoring the purchasing managers' emails—accessed the purchasing manager's email account and sent the fraudulent invoices from the purchasing manager's email account to the CEO's email account. The email was sent with the subject line "BANK ACCOUNT UPDATE," and provided fraudulent wire instructions to an account number belonging to the bad actor(s), instead of ERI Direct. The email and fraudulent wire instructions are attached as **Exhibits 7-8**.

28. Upon receipt of the fraudulent email from the purchasing manager's email account, as with all requests to change account information, the CEO called SJ Computers' contact at ERI Direct to confirm the requested change. The CEO was unable to reach anyone and left a voicemail message. The CEO did not receive a response from ERI Direct before the invoice payment deadline of March 31, 2021. Assuming the email from the purchasing manager and the request to update the wire transfer instructions from ERI Direct were legitimate; the CEO followed the payment instructions received in the fraudulent email and updated the recipient bank account. He sent the following wire transfers:

3/31/2021	Checking Account #xxxxxxx570	$450,555.00
3/31/2021	Checking Account #xxxxxxx334	$143,000.00
Total		***$593,555.00***

29. SJ Computers made two wire transfers because its bank has a $500,000 limit restriction for wire transfers.

30. SJ Computers discovered the fraud and unauthorized access to SJ Computers' computer system on April 5, 2021, when the CEO received several confusing emails, purportedly from the purchasing manager, to his SJ Computers' email account. The CEO called the purchasing manager to ask about the emails, and the purchasing manager advised that he had not sent them. The CEO and purchasing manager determined that the bad actor(s) had gained unauthorized access to the purchasing manager's email.

31. Not long after discovering the unauthorized access to the purchasing manager's email account, SJ Computers learned that ERI Direct had not received the two wire transfers from SJ Computers that had been initiated a few days earlier. Efforts to stop or reverse the wire transfers failed as the money had been moved from SJ Computers' bank account to the bad actor(s)' bank account.

32. An investigation confirmed that the bad actor(s) intentionally, without authorization from SJ Computers, infiltrated SJ Computers' computer system.

33. The bad actor(s) intercepted emails between SJ Computers and its vendor, ERI Direct, and sent emails from the purchasing manager's email account and viewed common payment practices between SJ Computers and ERI Direct.

34. The bad actor(s) spoofed ERI's email address and leveraged the unauthorized access to SJ Computers' computer system to send fraudulent invoices with modified data and instructions for the wire transfers to the CEO for payment to the bad actor(s)' bank account.

35. The two wire transfers cleared to the benefit of the bad actor(s). SJ Computers did not receive any goods or services from the bad actor(s) in exchange for the wire transfers. SJ Computers' vendor, ERI Direct, did not receive the wire transfers.

36. The hacking and infiltration of SJ Computers' computer system, interception of emails between SJ Computers and its vendors, and impersonation of a company executive to cause fraudulent wire transfers by the bad actor(s)—someone other than an employee, authorized person, independent contractor, or any other individual under the direct supervision of SJ Computers—constitutes an intentional, unauthorized, and fraudulent entry or change of data or computer instructions directly into a computer system, or Computer Fraud, under the Policy.

37. The Policy promises to pay for SJ Computers' loss of money caused by Computer Fraud.

C. Travelers Erroneously Denies SJ Computers' Computer Fraud Claim

38. SJ Computers promptly notified Travelers of the computer fraud incident and submitted a proof of loss statement on April 8, 2021 for coverage under the Policy. **Exhibit 9.**

39. The Policy provides coverage for an intentional, authorized, and fraudulent entry or change of data or computer instructions directly into any computer by someone other than an

employee, authorized person, independent contractor, or any other individual under the direct supervision of SJ Computers.

40. On June 9, 2021, Travelers accepted coverage for SJ Computers' loss under the Social Engineering Fraud Insuring Agreement Endorsement, subject to the sublimit of $100,000.00. Travelers, however, denied coverage under the Computer Fraud Insuring Agreement. Travelers' Coverage Letter is **Exhibit 10.**

41. In denying coverage under the Computer Fraud Insuring Agreement, Travelers refused to pay nearly 80% of SJ Computers' loss from the computer fraud incident.

D. Travelers' "Voluntary Payment" Defense is Legally Incorrect

42. Travelers contends that the Policy's Computer Fraud coverage was not triggered because the "fraudulent e-mails did not, by themselves, 'cause Money, Securities or Other Property to be transferred, paid, or delivered from inside the Premises or from the Insured's Financial Institution Premises, to a place outside the Premises or Insured's Financial Institution Premises.'" *Id.* at 7. Travelers contends, "the claimed loss occurred only after an Employee voluntarily used his authorized access to change banking information for the wire transfer intended for ERI." *Id*.

43. Travelers' position ignores recent case law, including one case to which Travelers was a party, holding that a fraudulent email that triggers a chain of events leading to the fraudulent transfer of funds is enough to constitute the use of a computer system to fraudulently cause a transfer of money.

44. Courts have also found that a fraudster's email posing and impersonating as someone else, such as a company executive, is a fraudulent instruction and that all later actions are the natural and probable cause of the initial fraudulent email.

45. Travelers has not met its burden of establishing that an exclusion or policy condition precludes coverage under the Computer Fraud Insuring Agreement.

E. Travelers' "Single Coverage" Defense Does Not Bar Coverage

46. Travelers further contends that coverage under the Computer Fraud Insuring Agreement is unavailable "for the separate and independently sufficient reason that the claimed loss falls within the definition of Social Engineering Fraud," and "Social Engineering Fraud does not include Computer Fraud . . . ." *See* **Exhibit 10** at 7.

47. Travelers' position that "Social Engineering Fraud does not include Computer Fraud or Funds Transfer Fraud" is not supported by the plain language of the Policy.

48. The plain language of the Policy does not include an express provision that says "Social Engineering does not include Computer Fraud."

49. The plain language of the Policy also contemplates trigger and payment of coverage under more than the liability coverage part.

50. The Limits of Liability subsection of the Policy's Conditions states,

> 1. Liability Coverage Limit of Liability
>
> Regardless of the number of persons or entities bringing **Claims** or the number of persons or entities who are **Insureds,** and regardless of when payment is made by the Company or when an **Insured's** legal obligation with regard thereto arises or is established, and further subject to any applicable **Liability Coverage Shared Limit of Liability or Annual Reinstatement of the Liability Coverage Limit of Liability:**
>
> a. the Company's maximum limit of liability for all **Loss,** including **Defense Expenses,** for all **Claims** under each applicable **Liability Coverage** will not exceed the remaining **Liability Coverage Limit of Liability** stated in ITEM 5 of the **Declarations** for each applicable **Liability Coverage;** and
>
> b. *in the event that a **Claim** triggers more than one **Liability Coverage,** the Company's maximum limit of liability for all **Loss**, including **Defense Expenses**, for any such **Claim** will not exceed the sum of the remaining **Liability Coverage Limits of Liability** of the applicable **Liability Coverages.***

Exhibit 1 at SJC-TravPolicy-18 (emphases in original and added).

51. Travelers has not met its burden to establish that an exclusion or policy provision precludes payment under more than one coverage section.

F. Travelers' Denial Breached the Policy and Was Done in Bad Faith

52. No terms, provisions, conditions, or exclusions in the Policy preclude coverage for SJ Computers' claim under the Computer Fraud Insuring Agreement.

53. Travelers denied coverage under the Computer Fraud Insuring Agreement based on its flawed interpretation of the Policy.

54. In denying coverage, Travelers ignored recent case law and critical parts of its own Policy.

55. Travelers wrongfully denied SJ Computers' claim for coverage under the Computer Fraud Insuring Agreement.

56. The positions described above constitute bad faith towards SJ Computers.

57. On June 22, 2021, SJ Computers, through counsel, responded to Travelers outlining in detail Travelers' erroneous coverage positions and requesting that Travelers withdraw its denial for coverage under the Computer Fraud Insuring Agreement. *See* **Exhibit 11**.

58. Travelers responded on August 2, 2021, and maintained its erroneous positions contrary to case law, the plain language of the Policy, and its obligations to handle claims in good faith. *See* **Exhibit 12**.

COUNT I (BREACH OF CONTRACT)

59. SJ Computers repeats and realleges the allegations in the preceding paragraphs.

60. All applicable terms, conditions, and other requirements under the Policy have been satisfied and, alternatively, compliance with the applicable terms, conditions, and other requirements, in whole or in part, have been waived or compliance is unnecessary for other reasons, including Travelers' actions and inactions related to its handling of the claim.

61. Under the Policy, Travelers was obligated to pay SJ Computers' claim under the Computer Fraud Insuring Agreement and failed to make such payment.

62. Travelers breached the Policy by failing to pay SJ Computers' losses incurred as a result of the computer fraud incident.

63. Because of Travelers' breach, SJ Computers sustained damages.

64. SJ Computers demands judgment against Travelers in an amount of $493,555.00, demands prejudgment and post-judgment interests, and seeks attorneys' fees and costs as well as all other damages resulting from Travelers' breach.

COUNT II (BREACH OF DUTY OF GOOD FAITH AND FAIR DEALING)

65. SJ Computers repeats and realleges the allegations in the preceding paragraphs.

66. Travelers owed SJ Computers a duty of good faith and fair dealing.

67. Travelers lacked an arguable basis for denying coverage and maintaining its denial.

68. No reasonable insurer would, under the given facts and recent court rulings, be expected to deny SJ Computers' claim and maintain its denial.

69. Travelers exhibited gross disregard for its obligations under the Policy in denying coverage.

70. For example, Travelers ignored information SJ Computers' counsel provided in support of its claim that directly conflicted with Travelers' positions and was inconsistent with the Policy that Travelers issued to SJ Computers.

71. Travelers also misrepresented the scope of the Policy's conditions, and relied on conclusory statements or inferences in its favor to decline coverage, despite having the burden to establish that a Policy exclusion or condition precludes coverage under the Computer Fraud Insuring Agreement. When presented with these reasons why Travelers had no arguable basis to deny SJ Computers' claim, Travelers refused to reconsider its erroneous positions.

72. Travelers breached its duty of good faith in handling SJ Computers' claim and delaying payment of SJ Computers' covered loss.

73. Because of Travelers' bad faith conduct and refusal to pay, SJ Computers has suffered damages, including, but not limited to, attorneys' fees.

74. Travelers' breach of its duty of good faith and fair dealing has deprived SJ Computers of its bargained-for benefits under the Policy.

75. SJ Computers is entitled to judgment against Travelers for the breach of its good faith obligations and Travelers is liable for all resulting damages, including attorneys' fees and interest.

PRAYER FOR RELIEF

SJ Computers requests that the Court enter judgment as follows:

(a) In favor of SJ Computers against Travelers;

(b) Determining that Travelers breached the Policy;

(c) Determining that Travelers breached its duty of good faith and fair dealing; and

(d) Awarding damages, including consequential damages, prejudgment and post-judgment interest, attorneys' fees, costs, and other and further relief as the Court deems proper.

JURY DEMAND

SJ Computers demands a jury trial on all triable issues within this Complaint.

Dated: November 11, 2021

HUNTON ANDREWS KURTH LLP

By: s/ Kelly R. Oeltjenbruns
Kelly R. Oeltjenbruns (# 0400395)
Syed S. Ahmad (to be admitted *pro hac vice*)
Latosha M. Ellis (to be admitted *pro hac vice*)
2200 Pennsylvania Avenue, NW
Washington, DC 20037
Telephone: (202) 955-1500
Facsimile: (202) 778-2201
koeltjenbruns@HuntonAK.com
sahmad@HuntonAK.com
lellis@HuntonAK.com

Attorneys for Plaintiff SJ Computers, LLC