UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

MARITZ HOLDINGS INC.,	)	
	)	
Plaintiff,	)	
	)	
v.	)	Case No. 4:18-cv-00826
	)	
COGNIZANT TECHNOLOGY SOLUTIONS	)	
U.S. CORPORATION,	)	
	)	
Serve:	)	
The Corporation Company	)	
120 South Central Avenue	)	
Clayton, Missouri 63105	)	

COMPLAINT

Plaintiff Maritz Holdings Inc. states as follows for its Complaint against Defendant Cognizant Technology Solutions U.S. Corporation:

The Parties, Jurisdiction, and Venue

1.   Plaintiff Maritz Holdings Inc. ("Maritz") is, and at all relevant times has been, a corporation organized and existing under the laws of Missouri. Maritz's principal place of business is located at 135 North Highway Drive, Fenton, Missouri 63099. Maritz is therefore a citizen of Missouri. 28 U.S.C. § 1332(c)(1).

2.   Maritz, including through its subsidiary companies, is, and at all relevant times has been, in the business of, *inter alia*, providing market and customer research, incentive programs, learning solutions, event management services, and travel management services to companies throughout the United States.

3.   Defendant Cognizant Technology Solutions U.S. Corporation ("Cognizant") is, and at all relevant times has been, a corporation organized and existing under the laws of

Delaware. Cognizant's principal place of business is located at 211 Quality Circle, College Station, Texas 77845. Cognizant is therefore a citizen of Delaware and Texas. 28 U.S.C. § 1332(c)(1).

4.   Cognizant claims that it is one of the world's leading providers of information technology, consulting, and business process outsourcing services.

5.   This Court has personal jurisdiction over Cognizant because this action arises out of its contacts with the State of Missouri as described herein.

6.   This Court has subject matter jurisdiction under 20 U.S.C. § 1332(a)(1) because this civil action is between citizens of different states and the amount in controversy exceeds the jurisdictional amount. This Court also has federal question jurisdiction because Maritz asserts a claim under the federal Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030.

7.   Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events giving rise to this matter occurred in this judicial district. Venue is also proper based on the forum selection provision in the agreement at issue in this case.

Factual Background

A.   Maritz and Cognizant enter into an Offshore Contracting Master Services Agreement.

8.   On or about January 1, 2010, Maritz and Cognizant entered into an Offshore Contracting Master Services Agreement (the "Agreement").

9.   Because the Agreement contains a confidentiality provision, Maritz will seek leave to file under seal a true and accurate copy of the Agreement as **Exhibit 1** to this Complaint.

10.   According to the Agreement, Maritz "desire[ed] to outsource certain information technology ("IT") and application development and management services to an offshore IT

service vendor with a proven track record of experience, reputation and quality. . . ." **Ex. 1** at p. 1.

11.   The Agreement further states that Cognizant "is a leading IT solutions provider specializing in custom software development, integration and maintenance services," and that "in reliance on [Cognizant's] asserted credentials and experience, Maritz has requested [Cognizant] to provide outsourcing services described herein as an offshore operation based in their development centers in India. . . ." *Id*.

12.   Cognizant further represented that it "is willing to and desires to assume responsibility for such outsources services in accordance with the terms, conditions and provisions of this Agreement. . . ." *Id*. at pp. 1-2.

13.   Pursuant to Section 4.2, Cognizant agreed that it "will diligently perform the Outsourced Services in accordance with the highest industry standards of workmanship and professionalism." *Id*. at p. 6.

14.   Pursuant to Section 4.5.1, Cognizant agreed that it "shall assign Outsourced Services to those of its employees, representatives and permitted subcontractors who are qualified and experienced in the required subject matter." *Id*. at p. 8.

15.   Cognizant further agreed that "all Outsourced Services will be of professional quality and will be performed in compliance with applicable laws, rules and regulations and in a competent, timely and efficient manner . . . ." *Id*. at p. 27 (Section 13.2.4(i)).

16.   Under Section 6.2.2, Cognizant "shall be responsible for and shall immediately notify Maritz of, investigate and remedy any security breaches or potential security breaches at the Service location(s)."

17.   Pursuant to Section 9.2 of the Agreement, Cognizant agreed to various restrictions on the use and disclosure of Maritz' "Confidential Information," which includes "all information and proprietary materials, not generally known in the relevant trade or industry" received by Cognizant in connection with its work under the Agreement. *Id*. at pp. 3, 20. Cognizant further agreed to "keep all Confidential Information strictly confidential. . . ." *Id*. at p. 26.

B.   Maritz is subject to a massive cyber-attack in Spring 2016.

18.   As part of incentive programs or related services provided to its clients, Maritz manages and operates rewards programs for its clients.

19.   As part of these rewards programs, participants in the programs are awarded or rewarded with gift cards/certificates that they can redeem with designated vendors. By way of example, gift cards/certificates are purchased through vendors like Target, Amazon, Apple (iTunes), and other vendors.

20.   Once a participant selects and receives a gift card/certificate, the participant can redeem it with the issuing vendor through the use of a redemption code. Upon redemption, the participant is provided with a credit for the face amount of the gift card/certificate at the issuing vendor.

21.   The redemption codes are typically conveyed to the participant on a piece of plastic (similar in size to a credit card) or in an electronic format. Electronically conveyed gifts are referred to herein as "eGift Cards."

22.   Maritz maintains eGift Cards that it purchases for use by clients and participants in its clients' rewards programs.

23.   Maritz maintained at relevant times eGift Cards both before and after they had been issued to participants in the programs. In each instance, the eGift Card consisted of the

- 4 -

redemption code relating to an assigned face value (i.e., denomination) with a particular issuing vendor.

24.   During times relevant herein, Maritz maintained these eGift Cards in files on a shared network (the L-Drive) found on Maritz's computer systems.

25.   One of Maritz's clients (Client A) ran a campaign directed to 40,000 of its cardholders, which involved eGift Cards with various vendors purchased by Maritz and held by Maritz during the relevant time periods.

26.   On or about March 10, 2016, the account teams for Maritz and Customer A reported that a large number of participants in certain programs had received eGift Cards with no value, including, but not limited to, Amazon, iTunes, and Target eGift Cards.

27.   Maritz promptly retained a data security consulting firm, Charles River Associates ("CRA"), and other third parties to investigate.

28.   As a result of its investigation, Maritz discovered the following:

   a. On March 1, 2016, an unidentified perpetrator directed so-called "phishing emails" to 63 Maritz email addresses (63 Maritz employees and one generic email address).

   b. The phishing emails contained a malicious file in an attached Microsoft Word document.

   c. The malicious file provided a backdoor to each such computer and the systems that such computer could access within Maritz's computer system.

   d. Sixteen computers in the Maritz environment loaded the malicious Microsoft Word document, which downloaded a backdoor. Twelve Maritz computers

communicated with the command and control server associated with the backdoor.

e. In addition, 87 Maritz employees received similar phishing emails on March 14, 2016. These emails operated similarly to those received March 1, 2016. Twenty-three of these computers in the Maritz environment loaded the malicious Microsoft Word documents, which downloaded the backdoor. Five of these computers communicated with the command and control server associated with the backdoor.

f. In addition, 91 Maritz employees received similar emails on March 15, 2016, although there is no evidence of computers infected through the March 15, 2016 emails.

g. In total, 17 computers were infected with the backdoor in March 2016, two of which had credential harvesting malware installed. One infected computer had additional malware inserted on it to harvest active directory credentials.

h. The perpetrator(s) were in Maritz's computer systems between March 2, 2016 and March 26, 2016, during the period the perpetrator(s) accessed Maritz's L-Drive where Maritz held, among other confidential information, the eGift Cards at the relevant times.

i. The perpetrator(s) transferred 1.2 gigabytes of data from the Maritz server.

29. After temporarily ceasing its operations relating to eGift Cards on March 11, 2016, Maritz began contacting vendors for eGift Cards, providing related eGift Card inventory that had yet to issue to participants, requesting that the vendors identify redeemed eGift Cards and devalue any unredeemed eGift Cards to prevent future unauthorized redemptions.

30.   Of the 28 vendors involved, Maritz identified loss through unauthorized redemption of eGift Cards with a number of vendors.

31.   In total, Maritz's vendors confirmed the redemption of $11,094,077.39 in unissued eGift Cards. These eGift Cards had not been directed to participants for redemption purposes at the time of the computer fraud upon Maritz.

32.   Maritz cancelled all undirected eGift Cards on the system that had not been redeemed, for purposes of replacement.

33.   Maritz suffered loss with respect to the non-directed and improperly redeemed eGift Cards in the amount of at least $11,094,077.39.

34.   In addition, Maritz was required to issue certain Gift Cards involving two vendors that had previously been directed to participants in Client A's reward program, because of the volume of complaints received from participants that were provided eGift Cards with no value. Maritz paid approximately $323,000.00 to purchase the replacement cards.

35.   Separate and apart from the issued cards identified in the immediately preceding paragraph, Maritz received complaints from a number of participants in rewards programs concerning previously issued eGift Cards containing no value or incorrect value. Maritz reissued eGift Cards based on these complaints, totaling at least $107,120.00.

36.   In connection with its investigation, Maritz incurred out-of-pocket expenses totaling at least $1,207,859.26.

C.   Maritz is subject to additional cyber-attacks in Spring 2017 through accounts assigned to Cognizant.

37.   In February and March 2017, Maritz suffered additional cyber-attacks.

38.   As a result, Maritz declared a security incident and, in March 2017, hired Intersec Worldwide ("Intersec") to investigate the cyber-attack.

39.   That investigation revealed the following:

a. Spear phishing or targeted emails were directed to Maritz employees from February 17, 2017 through February 20, 2017;

b. When certain Maritz employees accessed a URL link in those emails, remote access tools were placed on Maritz's computer systems;

c. The installation of these remote access tools on Maritz's systems permitted the perpetrator(s) broad access to Maritz's computer systems;

d. The perpetrator(s) accessed Maritz's systems to obtain confidential information; and

e. The perpetrator(s) accessed, among other things, credentials to access Maritz's card fulfillment system, which held Gift Card information including redemption codes for Gift Cards.

40.   As a result of these attacks, Maritz suffered loss relating to Gift Cards in the amounts of at least $1,239,574.00 for non-issued Gift Cards and at least $620,150.00 relating to participant complaints for improperly redeemed cards.

41.   In connection with its investigation, Maritz incurred out-of-pocket expenses in excess of $5,000,000.

42.   Intersec uncovered numerous signs of unusual activity. For example, Intersec found that attackers had used a program called "Screen Connect" to access computers belonging to Maritz employees. This was the same tool that was used to effectuate the cyber-attack in Spring 2016. Intersec also determined that the attackers had run searches on the Maritz system for certain words and phrases connected to the Spring 2016 attack.

43.   Intersec also determined that the attackers were accessing the Maritz system using accounts registered to Cognizant. For example, in April 2017, someone using a Cognizant account utilized the "fiddler" hacking program to circumvent cyber protections that Maritz had installed several weeks earlier.

44.   Subsequent investigation also revealed that Cognizant employees violated industry standards and Maritz company policy by sharing credentials and usernames for Cognizant accounts.

45.   At least one of these accounts as to which Cognizant employees shared credentials and usernames was used to hack the Maritz system in 2017.

Count I – Computer Fraud and Abuse Act (18 U.S.C. § 1030)

46.   Maritz realleges Paragraphs 1 through 45 as if set forth fully herein.

47.   Maritz relies on a secure computer network to host and manage its confidential and proprietary information, including managed rewards programs for its clients.

48.   The computer network is used in interstate commerce.

49.   Maritz's computer network is "protected" within the meaning of 18 U.S.C. § 1030(e)(2).

50.   On information and belief, one or more of Cognizant's employees, while acting in the scope of their employment and under the control and supervision of Cognizant, intentionally accessed Maritz's network and removed or copied confidential information belonging to Maritz (including, but not limited to, codes and data for Gift Cards and/or eGift Cards) without authorization and/or by exceeding their authorization, all in violation of CFAA § 1030(a)(2).

51.   Cognizant was negligent or reckless in allowing one or more of its employees and/or third parties to intentionally access Maritz' network as described herein.

52.   Maritz has been damaged and has suffered losses as a result of Cognizant's actions in an amount greatly exceeding $5,000. 18 U.S.C. § 1030(e)(11).

53.   In addition to Maritz's direct financial loss, Cognizant's actions have caused and continue to cause Maritz irreparable harm.

Count II – Computer Tampering (Mo. Rev. Stat. §§ 537.525, 569.095)

54.   Maritz realleges Paragraphs 1 through 53 as if set forth fully herein.

55.   Section 537.525.1 of the Missouri Revised Statutes provides: "In addition to any other civil remedy available, the owner or lessee of [a] . . . computer program . . . may bring a civil action against any person who violates sections 569.095 to 569.099, RSMo, for compensatory damages."

56.   A person violates Section 569.095.1 of the Missouri Revised Statutes if he or she "knowingly and without authorization or without reasonable grounds to believe that he [or she] has such authorization: … (3) Discloses or takes data, programs, or supporting documentation, residing or existing internal or external to a computer, computer system, or computer network."

57.   Cognizant violated Section 569.095.1 and, therefore, is liable to Maritz under Section 537.525.1.

Count III - Conversion

58.   Maritz realleges Paragraphs 1 through 57 as if set forth fully herein.

59.   Maritz maintains confidential information on its secure computer network that includes, among other things, codes and data relating to Gift Cards and eGift Cards.

60.   On information and belief, one or more of Cognizant's employees, while acting in the scope of their employment and under the control and supervision of Cognizant, took

possession of Maritz's codes and data relating to Gift Cards and eGift Cards without authorization, thereby misappropriating them.

Count IV – Breach of Contract

61.   Maritz realleges Paragraphs 1 through 60 as if set forth fully herein.

62.   Under the Agreement, Cognizant agreed, *inter alia*, that it would assume responsibility for the services that it performed for Maritz, that it would perform the services "in accordance with the highest industry standards of workmanship and professionalism," and that it would safeguard Maritz's confidential and proprietary information.

63.   Cognizant also agreed that only "qualified and experienced" personnel would work on the Maritz account and that all work "will be of professional quality and will be performed in compliance with applicable laws, rules and regulations and in a competent, timely and efficient manner."

64.   Cognizant breached these and other contractual provisions by, *inter alia*, failing to prevent Cognizant employees or other unauthorized personnel from accessing Maritz's systems for improper purposes, failing to take responsibility for the above-referenced security breaches, and by failing to prevent its employees from sharing credentials and usernames for Cognizant accounts in violation of industry standards and Maritz's company policy.

65.   Cognizant's actions have caused Maritz to suffer damages.

66.   Additionally, Cognizant billed Maritz for service time provided by Cognizant employees involved in accessing Maritz's computer systems for improper and authorized purposes.

67.   On information and belief, Cognizant billed Maritz for service time by such employees improperly in that such employees were actually spending time billed to Maritz

engaging in attacking Maritz's systems rather than providing the services Cognizant contracted to provide to Maritz.

68.   On information and belief, Maritz paid amounts billed improperly by Cognizant, without knowledge that the Cognizant employees were billing time for providing services to Maritz when such employees were actually engaged in efforts to attack Maritz's systems rather than providing the services billed by Cognizant.

69.   Billings by Cognizant for such time were in breach of the Agreement.

70.   Maritz suffered damages as a result of Maritz's payment of amounts improperly billed by Cognizant in breach of the Agreement.

Count V - Negligence

71.   Maritz realleges Paragraphs 1 through 70 as if set forth fully herein.

72.   Cognizant owed Maritz a duty to act in accordance with reasonable industry standards and prevent foreseeable harm to Maritz, including taking reasonable safeguards to prevent its employees and/or third parties from using Cognizant accounts to hack Maritz's computer network

73.   Cognizant also owed Maritz a duty to safeguard the credentials and usernames issued to Cognizant employees with access to Maritz's system.

74.   Cognizant breached the applicable standard of care by, *inter alia*, failing to appropriately hire, train and/or supervise its employees, allowing its employees to share credentials and usernames, and allowing its employees and/or third parties to hack Maritz's computer network.

75.   Cognizant's failure to fulfil its duties owed to Maritz has caused Maritz to suffer damages.

Count VI – Unjust Enrichment & Accounting

76.   Maritz realleges paragraphs 1 through 75 as set forth fully herein in the alternative to Count VI.

77.   In paying amounts improperly invoiced by Cognizant, Maritz conferred a benefit on Cognizant in good faith.

78.   Cognizant accepted and retained the benefit of such payments.

79.   Acceptance and retention of this benefit by Cognizant under the circumstances is inequitable.

80.   To the extent that Maritz cannot recover said amounts under Count VI, it lacks an adequate remedy at law.

81.   Maritz additionally requires an accounting to ascertain the full extent of the unjust enrichment to Cognizant.

WHEREFORE, Plaintiff Maritz Holdings, Inc. respectfully requests the Court enter judgment in its favor and against Defendant Cognizant Technology Solutions U.S. Corporation for actual and punitive damages, attorneys' fees, expenses, and costs, and award Plaintiff any additional and further relief the Court deems just and proper.

- 14 -

Respectfully submitted,

THOMPSON COBURN LLP

By: /s/ Jan Paul Miller
    Jan Paul Miller, 58112MO
    Brian A. Lamping, 61054MO
    Elise N. Puma, 68336MO
    One US Bank Plaza
    St. Louis, Missouri 63101
    314-552-6000
    FAX 314-552-7000
    jmiller@thompsoncoburn.com
    blamping@thompsoncoburn.com
    epuma@thompsoncoburn.com

Attorneys for Plaintiff Maritz Holding, Inc.