IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF FLORIDA
ORLANDO DIVISION

DATA PROTECTION SERVICES, LLC
D/B/A TORGUARD,

Plaintiff,

vs.

COLLECTIVE 7, INC., and TEFINCOM S.A.
D/B/A NORDVPN,

Defendants.

_____/

CASE NO: 6:19-cv-978

JURY TRIAL DEMANDED

PLAINTIFF'S AMENDED COMPLAINT

Plaintiff, Data Protection Services, LLC d/b/a TorGuard, ("TorGuard") hereby files this Amended Complaint against the Defendants, Collective 7, Inc., ("Collective 7"), and Tefincom S.A. d/b/a NordVPN ("NordVPN") (collectively the "Defendants"), and states as follows:

SUMMARY OF THE ACTION

1. TorGuard and NordVPN are competing providers of virtual private networks. Virtual private networks, known as "VPNs," employ encryption to provide secure access to a remote computer over the Internet.

2. TorGuard is a United States-based VPN provider headquartered in Orlando, Florida. NordVPN is a subsidiary of a Panama-based holding company, recently made notorious for providing "misleading" advertisements to consumers according a regulatory ruling,[1] and for (by NordVPN's own admissions) leasing Internet Protocol addresses as part of NordVPN's

[1] *See* ASA RULING ON TEFINCOM SA T/A NORDVPN (May 1, 2019), *available at* https://www.asa.org.uk/rulings/tefincom-sa-a19-547668.html (last visited May 22, 2019).

services that were acquired "dishonestly" by registering "more than 735,000 IP addresses from ARIN (the American Registry for Internet Numbers)" in a scheme where the United States Attorney for the District of South Carolina recently brought an indictment for twenty counts of wire fraud.[2]

3. Collective 7 is a Canadian hosting company formerly utilized by TorGuard as a service provider that, on information and belief, is now owned or controlled by NordVPN. Working together, Collective 7 and NordVPN wrongfully obtained and used TorGuard's confidential and trade secret business information to blackmail TorGuard.

4. NordVPN threatened to release TorGuard's confidential and trade secret information that was obtained by NordVPN from Collective 7— who, in turn, obtained this information during the time TorGuard utilized Collective 7 as a service provider. NordVPN threatened to release this information unless TorGuard forced or coerced a third party into silence, as this third party was publishing legitimate criticisms of issues associated with NordVPN's business practices.

5. This is not NordVPN's first foray into wrongful activity against TorGuard. As discussed below, NordVPN previously threatened TorGuard through the nom de guerre of "General Counsel Legal Affairs Tefincom S.A." NordVPN further orchestrated strategically timed distributed denial of service attacks (frequently referred to as "DDoS" attacks) against TorGuard

[2] WILL THE MICFO CASE IMPACT NORDVPN'S SERVICE?, *available at* https://nordvpn.com/blog/micfo-ip-service-update/ (last visited May 23, 2019); *see also,* Indictment, *U.S.A. v. Golestan et. al.,* 2:19CR00441 (D.S.C. May 14, 2019).

designed to prevent TorGuard from doing business— such as a major DDoS attack that occurred on Black Friday and caused TorGuard to suffer significant economic and reputational damages.[3]

6. TorGuard seeks injunctive and other equitable relief, as well as compensatory damages in excess of $75,000.00, associated with Defendants' violations of Florida's Uniform Trade Secrets Act ("FUTSA"), Fla. Stat. § 668.001 *et seq*., Florida's Computer Abuse and Data Recovery Act ("CADRA"), Fla. Stat. § 668.801 *et seq.*, and Defendants' tortious interference with TorGuard's contractual and prospective business relationships.

PARTIES

7. TorGuard is a Florida Limited Liability Company organized under the laws of the State of Florida, with its principal place of business in Orange County, Florida.

8. Defendant, Collective 7, is an Ontario Business Corporation, organized under the laws of Canada, with a principal place of business in Ontario, Canada. Collective 7 was previously a service provider to TorGuard. On information and belief, Collective 7 is affiliated with or controlled by NordVPN. Collective 7's Chief Technology Officer previously represented to TorGuard that he had a "direct relationship" with the owners of NordVPN, as well as soliciting TorGuard with a potential purchase offer of TorGuard.

9. NordVPN is a Panamanian corporation, organized under the laws of the Republic of Panama.

[3] Black Friday is "the highest-volume shopping day in the United States[,]" and courts have recognized that activities directed against a business will often have maximum impact on sales when timed congruent with Black Friday. *See e.g.*, *Romag Fasteners, Inc. v. Fossil, Inc*., 817 F.3d 782, 784 (Fed. Cir. 2016), *vacated in part on other grounds*, No. 3:10cv1827 (JBA), 2018 U.S. Dist. LEXIS 139637 (D. Conn. Aug. 16, 2018).

JURISDICTION AND VENUE

10. This Court has diversity jurisdiction pursuant to 28 U.S.C. § 1332(a), as Plaintiff is a Florida corporation, Defendant NordVPN is a Panamanian corporation, and Defendant Collective 7 is a Canadian Corporation.

11. This Court has personal jurisdiction over Collective 7 and NordVPN under Florida's long arm statute because *inter alia*, as set forth herein, Defendants conspired to commit a tort in Florida, resulting in harm in Florida, and one or more overt acts in furtherance of the conspiracy were committed within this judicial district in Florida.

12. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claims set forth in this Complaint occurred in this judicial district.

13. At all times herein material, TorGuard, NordVPN, and Collective 7 engaged in interstate and foreign commerce.

FACTUAL BACKGROUND

14. TorGuard is a technology company. Its primary offering is a virtual private network service that provides encrypted and secure access to a remote computer over the Internet. Virtual private networks (VPNs) are routinely used worldwide to keep Internet use and traffic secure from unauthorized and surreptitious access.[4]

15. VPNs routinely contract with hosts worldwide to provide routing and other services for the VPN network.

[4] *See, VirnetX Inc. v. Mitel Networks Corp*., No. 6:11-CV-18, 2012 U.S. Dist. LEXIS 107280, at *13 (E.D. Tex. Aug. 1, 2012) (Defining a VPN as "a network of computers which privately and directly communicate with each other by encrypting traffic on insecure paths between the computers where the communication is both secure and anonymous.")

16. In 2018, TorGuard contracted with Collective 7, a company that offers hosting services among other services. As part of this business relationship, Collective 7 gained access to certain confidential and trade secret information owned by TorGuard and employed by TorGuard in providing its services. At the time, TorGuard was not made aware that Collective 7 was affiliated with its competitor, NordVPN.

17. NordVPN is a competing VPN provider that has routinely, and systematically, targeted and threatened TorGuard.

18. As just one example, in late 2018, an unspecified and apparently nameless individual writing from the email address "legal@nordvpn.com" and titled only "General Counsel Legal Affairs Tefincom S.A." wrote TorGuard and stated: "I am writing on behalf of Tefincom S.A., the owner of NordVPN product and NordVPN registered trademark . . ." This nameless "General Counsel" demanded that TorGuard take certain actions— threatening that, if TorGuard did not, then "[a] refusal to take actions mentioned above will constitute grounds to refer the matter to the national competition authorities, arbitration institutions or courts in order to defend against false advertising, unfair competition, intellectual property infringement, and other claims, as well as to resort to all other available civil, administrative and criminal remedies, which we are ready to employ. Not authorized business activities related to extortion of NordVPN trademark are taken very seriously and will result in immediate legal action if such illegal activities remain."

19. Upon information and belief, NordVPN obtained certain of TorGuard's confidential and trade secret information from Collective 7. As TorGuard has learned, Collective 7's Chief Technology Officer has a "direct relationship" with the owners of NordVPN.

20. NordVPN confronted and threatened TorGuard with public disclosure of this information unless TorGuard took certain actions to silence criticism of NordVPN. NordVPN's presentation of this threat was brazen and involved in-person intimidation tactics by foreign actors.

21. On or about May 17, 2019 an unknown individual appeared unannounced at the personal residence of a TorGuard contractor, asking to speak with him about his relationship with TorGuard and the VPN industry.

22. Within an hour of this in-person and unannounced visit, the same TorGuard contractor received unsolicited correspondence from an employee at NordVPN. This correspondence stated that NordVPN had received certain of TorGuard's confidential and trade secret information and requested to set up an instant message chat to discuss this with TorGuard.

23. During the conversation, the representative of NordVPN stated that NordVPN's customers had dwindled, due to customer mistrust of NordVPN.

24. The NordVPN representative accused TorGuard of causing this mistrust and stated that an individual friendly to TorGuard had posted negative content about NordVPN on YouTube which had caused NordVPN to suffer business losses.

25. The representative of NordVPN then told TorGuard's representative that it wanted a "gentleman's agreement" whereby NordVPN would not publish TorGuard's confidential and trade secret information obtained by NordVPN regarding TorGuard's systems if TorGuard persuaded (through whatever means) this individual to remove negative YouTube postings.

26. NordVPN stated that if TorGuard did not comply, NordVPN would publish TorGuard's confidential and trade secret information.

27. The NordVPN representative proceeded to provide TorGuard with examples of TorGuard's confidential and trade secret information (hereinafter the "Information").

28. Based on the nature and content of the Information, the Information was obtained by NordVPN from Collective 7.

29. TorGuard earlier terminated its contract with Collective 7.

30. On information and belief, several members of Collective 7 were also employed by NordVPN— and Collective 7 may be owned or controlled by NordVPN.

31. At minimum, Collective 7's Chief Technology Officer, who had access to the Information, had a direct business relationship with the owners of NordVPN.

32. Moreover, after TorGuard's business relationship with Collective 7 concluded, TorGuard began to suffer service outages on its website, due to distributed denial of service attacks (frequently referred to as "DDoS" attacks).

33. DDoS attacks are Internet-based attacks where the attacker attempts to make a website unavailable by temporarily disrupting service by flooding a website or service with illegitimate traffic in a manner analogous to multiple individuals attempting to walk through a doorway at the same time— as multiple individuals attempting to enter a doorway would prevent all of the individuals from passing through the door, the flood of Internet traffic thereby prevents any users from accessing the website or service.

34. In a DDoS attack, the legitimate users or potential users of the Internet-based service are prevented from accessing the service due to the flood of illegitimate traffic.

35. The DDoS attacks directed against TorGuard were based upon the Information— the nature and way they occurred and were timed made it patently obvious that the attacker had obtained the Information from Collective 7 and was utilizing it as a roadmap for DDoS attacks.

36. These DDoS attacks against TorGuard occurred on multiple occasions since January 2018.

37. As a result of the website outages caused by the DDoS attack, TorGuard's business relationships with its clients and potential clients have been negatively affected and TorGuard has suffered significant losses. Many of TorGuard's potential customers were unable to sign up for TorGuard's services because of these coordinated DDoS attacks that were only possible due to Defendants' access to and sharing of the Information.

38. As just one example, as a result of one DDoS attack on November 23, 2018— otherwise known as Black Friday— TorGuard suffered outages that resulted in hundreds of cancellations of orders, causing TorGuard to suffer enormous losses in a single day.

39. These activities are made all the more egregious by apparent attempts by NordVPN— through its intermediaries at Collective 7— to purchase or otherwise acquire TorGuard, with the obvious inference through coordinated actions that NordVPN would continue to unlawfully attack TorGuard in order to prevent TorGuard from lawfully conducting its business; unless, of course, TorGuard were to sell its business.

COUNT I
VIOLATION OF FLORIDA COMPUTER ABUSE AND DATA RECOVERY ACT ("CADRA")
Against NordVPN and Collective 7

40. Plaintiff realleges and incorporates the allegations contained in paragraphs 1 through 39 above as if herein fully set forth.

41. At all times herein material, TorGuard's Information was stored on computer systems that constituted a "protected computer" as defined under CADRA, Florida Statutes § 668.802(6), because these systems were used in connection with the operation of TorGuard's business and they stored information, programs or code in connection with the operation of TorGuard's business that could be accessed only through a technological access barrier, as defined under CADRA, Florida Statutes § 668.802(7).

42. On or about January 16, 2018, Defendants knowingly, with intent to cause harm or loss, and without authorization, accessed the protected computer systems on which TorGuard had installed its Information, thereby obtained TorGuard's Information from a protected computer without authorization, and as a result caused harm or loss, all in violation of CADRA, Florida Statutes § 668.803.

43. Defendants further trafficked technological access barriers through which access to a protected computer may be obtained without authorization, in violation of CADRA, Florida Statutes § 668.803.

44. Defendants committed the acts set forth herein knowingly and with intent to cause loss as defined under CADRA, Florida Statutes § 668.802(5), including intending to profit as a result of their CADRA violations.

45. TorGuard has been damaged by Defendants' violations of CADRA, and is entitled under CADRA, Florida Statutes § 668.804(1), to recover such damages, to recover Defendant's profits gained as a result of their CADRA violations, to injunctive relief to prevent any future violations of CADRA, and to recovery of the Information.

46. TorGuard has incurred reasonable attorneys' fees and costs incident to bringing this action. Pursuant to Fla. Stat. § 668.04(2), Defendants are required to reimburse Plaintiff for all reasonable attorney's fees incurred due to Defendants' violation of CADRA.

WHEREFORE, TorGuard asks the Court to enter a judgment against Defendants awarding it (a) TorGuard's actual damages pursuant to Fla. Stat. § 668.804(1)(a); (b) Defendants' profits from violating CADRA that are not included in TorGuard's actual damages, pursuant to Fla. Stat. § 668.804(1)(b); (c) injunctive and other equitable relief from the Court to prevent a future violation of § 668.803, including without limitation, an order prohibiting Defendants from further

disclosing TorGuard's confidential information, pursuant to Fla. Stat. § 668.804(1)(c); (d) an order requiring Defendants to return TorGuard's confidential information and all copies thereof, pursuant to Fla. Stat. § 668.04(1)(d); (e) TorGuard's reasonable attorney's fees and other litigation costs, pursuant to Fla. Stat. § 668.04(2), as the prevailing party; and (e) such additional relief that this Court deems fair and equitable.

COUNT II
VIOLATION OF FLORIDA UNIFORM TRADE SECRETS ACT ("FUTSA")
Against NordVPN and Collective 7

47. Plaintiff realleges and incorporates the allegations contained in paragraphs 1 through 39 above as if herein fully set forth.

48. TorGuard's Information constitutes trade secret information, pursuant to Fla. Stat. § 688.002(4), as the Information derives economic value for TorGuard by not being generally known to or readily ascertainable to, other persons – especially to its competitors, such as NordVPN.

49. TorGuard developed the Information and uses the Information, and derivative works thereof, to provide its VPN services to its clients and to develop and market other technological solutions. TorGuard has at all times relevant to this action taken reasonable efforts to protect the secrecy of the Information.

50. Defendants misappropriated the Information as defined in Fla. Stat. § 688.002(2). Collective 7 obtained and disclosed to NordVPN the Information without consent of TorGuard and did so through improper means – specifically, by exceeding their authorization to access such Information, pursuant to Fla. Stat. § 688.002(2)(b)(1.). NordVPN knew or had reason to know that Collective 7 obtained the Information by improper means pursuant to Fla. Stat. § 688.002(2)(a). Thus, Collective 7 and NordVPN violated FUTSA.

51. TorGuard has been damaged by Defendants' violations of FUTSA, and is entitled under FUTSA, Fla. Stat. § 688.003 to injunctive relief, enjoining further misappropriation by Defendants. Further, per Fla. Stat. §688.004(1), TorGuard is entitled to recover monetary damages, including Defendant's profits gained as a result of their FUTSA violations, as well as for TorGuard's actual losses.

52. TorGuard further requests exemplary damages pursuant to Fla. Stat. §688.004(2), in the amount of twice the amount of actual damages awarded, as Defendants' conduct amounts to malicious and wilful appropriation of the Information.

53. TorGuard has incurred reasonable attorneys' fees and costs incident to bringing this action. Pursuant to Fla. Stat. §688.005, Defendants should be required to reimburse Plaintiff for all reasonable attorney's fees incurred due to Defendants' malicious and wilful misappropriation of the Information.

WHEREFORE, TorGuard asks the Court to enter a judgment against Defendants awarding it (a) TorGuard's actual losses pursuant to Fla. Stat. § 668.004(1); (b) Defendants' profits from violating FUTSA that are not included in TorGuard's actual damages, pursuant to Fla. Stat. § 668.004(1); (c) exemplary damages in the amount of twice the actual losses incurred by Defendants pursuant to § 668.004(2); (d) injunctive and other equitable relief from the Court to prevent a future violation of FUTSA pursuant to § 668.003, including without limitation, an order prohibiting Defendants from further disclosing TorGuard's Information; (e) TorGuard's reasonable attorneys' fees and other litigation costs, pursuant to Fla. Stat. § 668.005, as the prevailing party; and (f) such additional relief that this Court deems fair and equitable.

COUNT III
TORTIOUS INTERFERENCE WITH TORGUARD'S BUSINESS RELATIONSHIPS
Against NordVPN and Collective 7

54. Plaintiff realleges and incorporates the allegations contained in paragraphs 1 through 39 above as if herein fully set forth.

55. TorGuard maintains advantageous business relationships with its potential customers and current customers by providing website-based services that require TorGuard to have an active, fully functional website at all times.

56. The functionality of TorGuard's website is integral to the provision of web-based services to its current customers, as well as to providing a mechanism for prospective customers to enter into business relationships with TorGuard.

57. Defendants knew of TorGuard's business relationships with its current and potential customers.

58. Defendant NordVPN is a direct competitor and operates the same type of business, and Defendant Collective 7 was engaged in a business relationship with TorGuard in January of 2018 which required Collective 7 to gain familiarity with TorGuard's business model.

59. Defendants actions constituted intentional and unjustified interference with TorGuard's business relationships with its potential and current customers.

60. TorGuard has suffered damage including but not limited to, damages to TorGuard's reputation, loss of profit, and other financial amounts, the specific amount of which will be determined at trial.

WHEREFORE, TorGuard asks the Court to enter a judgment against Defendants awarding TorGuard its actual losses and such additional relief that this Court deems fair and equitable.

JURY TRIAL DEMANDED

Plaintiff hereby demands a jury trial on all issues so triable.

Dated: May 30, 2019

Respectfully Submitted,

ADAM C. LOSEY, ESQ. (FBN 69658)
Primary Email: alosey@losey.law
Secondary Email: docketing@losey.law
KAREN L. MIDDLEKAUFF, ESQ. (FBN 99884)
Primary Email: kmiddlekauff@losey.law
Secondary Email: docketing@losey.law
LOSEY PLLC
1420 Edgewater Drive
Orlando, Florida 32804
Phone: 407.906.1605
Lead Trial Counsel
Counsel for Plaintiff