UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA,
United States Department of Justice
Consumer Protection Branch
450 5th St. NW, Suite 6400
Washington, DC 20001

Plaintiff,

v.

NEXWAY SASU, a corporation, 1 Avenue du General de Gaulle 92074 Paris, La Defense, France;

NEXWAY GROUP AG, a corporation, Gerbergässlein 48 4051 Basel, Switzerland;

ASKNET SOLUTIONS AG, a corporation, (formerly ASKNET AG and NEXWAY AG) Vincenz-Prießnitz-Straße 3 76131 Karlsruhe, Germany;

NEXWAY, INC., a corporation, 235 West Lake Center, Number 30, Daly City, CA 94105;

ASKNET, INC., a corporation, 4804 Mission Street, Suite 208 San Francisco, CA 94112;

VICTOR IEZUITOV, also d/b/a VICTOR LEZUITOV, individually and as an officer of NEXWAY SAS, NEXWAY GROUP AG, ASKNET AG, and NEXWAY AG; and

CASEY POTENZONE, individually and as an officer of NEXWAY SAS, NEXWAY GROUP AG, ASKNET AG, and NEXWAY AG,

Defendants.

Case No. 1:23-cv-900

COMPLAINT FOR PERMANENT INJUNCTION, MONETARY RELIEF, CIVIL PENALTIES AND OTHER RELIEF

Plaintiff, the United States of America (Plaintiff), acting upon notification and authorization to the Attorney General by the Federal Trade Commission ("FTC"), for its Complaint alleges:

1. Plaintiff brings this action under Sections 5(m)(1)(A), 13(b) and 19 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. §§ 45(m)(1)(A), 53(b), 57b, and the Telemarketing Sales Rule, 16 C.F.R. Part 310.4 ("TSR"), to obtain a permanent injunction, civil penalties, and other relief for violations of the FTC Act and the TSR committed by the Defendants, Nexway SASU, Nexway Group AG, asknet Solutions AG, Nexway, Inc., asknet, Inc., Victor Iezuitov, and Casey Potenzone.

SUMMARY OF CASE

2. The Defendants are at the center of a technical support scam. Defendants worked with telemarketers who made misrepresentations to consumers about the performance and security of their computers in connection with the sale of bogus technical support services. Defendants violated the law either by assisting and facilitating those illegal sales and laundering the credit card charges through their own merchant accounts, or by engaging in the enterprise as the ultimate sellers liable for the transactions. The Defendants injured consumers in this District, throughout the United States and elsewhere in the world.

JURISDICTION AND VENUE

3. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331, 1337(a), and 1345.

4. Venue is proper in this District under 28 U.S.C. § 1391(b)(2), (b)(3), (c)(2), (c)(3), and (d), and 15 U.S.C. § 53(b).

PLAINTIFF

5. Plaintiff is the United States of America, acting upon notification and authorization to the Attorney General by the Federal Trade Commission, pursuant to Section 16(a)(1) of the FTC Act, 15 U.S.C. § 56(a)(1). The FTC is an independent agency of the United States Government created by the FTC Act. The FTC enforces Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), which prohibits unfair or deceptive acts or practices in or affecting commerce. The FTC also enforces the Telemarketing Sales Rule, which prohibits unlawful acts or practices in connection with telemarketing. 16 C.F.R. Part 310.

DEFENDANTS

6. Defendant Nexway SASU is a French corporation with its principal place of business at 1 Avenue du General de Gaulle 92074 Paris, La Defense, France. Nexway SAS became part of Nexway Group AG in 2018. Nexway SASU in connection with the matters alleged herein, transacts or has transacted business in this District and throughout the United States.

7. Defendant Nexway Group AG is a Swiss corporation with its principal place of business at 48 Gerbergässlein 484051 Basel, Switzerland. Nexway Group AG in connection with the matters alleged herein, transacts or has transacted business in this District and throughout the United States.

8. Defendant asknet Solutions AG is a German corporation with its principal place of business at Vincenz-Prießnitz-Straße 3, 76131 Karlsruhe, Germany and previously at 1 Avenue du General de Gaulle 92074 Paris, La Defense France. The company was previously named Nexway AG. Nexway AG was a combination of Nexway Group AG and asknet AG. askent AG purchased Nexway Group AG and Nexway SASU on or about December 2018, combined the companies to operate under the same officers and subsequently changed the name of the combined entity to Nexway AG. Nexway AG subsequently sold Nexway Group AG and Nexway SASU in

April 2020 after receiving a CID from the FTC. Nexway AG then changed its name to asknet Solutions AG which is publicly traded on the Frankfurt Germany stock exchange under the symbol ASKN. asknet Solutions AG in connection with the matters alleged herein, transacts or has transacted business in this District and throughout the United States.

9. asknet, Inc. is a Delaware Corporation, and its principal place of business is 4804 Mission Street, Suite 208, San Francisco, California. asknet, Inc. in connection with the matters alleged herein, transacts or has transacted business in this District and throughout the United States.

10. Nexway, Inc. is a Delaware corporation, and its principal place of business is 235 West Lake Center, Number 30, Daly City, California. Nexway, Inc. in connection with the matters alleged herein, transacts or has transacted business in this District and throughout the United States.

11. Defendant Victor Iezuitov is the Chief Executive Officer of Nexway SASU and Nexway Inc. and was formerly the CEO of Nexway AG from July 2019 to April 30, 2020. He resides in Switzerland. He was a member of the Executive Board and Leadership Committee of Nexway AG from July 2019 to April 30, 2020. He was the CEO of asknet, Inc. from September 13, 2019 to September 4, 2020. Defendant Iezuitov controlled and operated companies that did business in the United States, assisted and facilitated telemarketers who targeted consumers in the United States, engaged in credit card laundering in the United States, or claimed to be the merchant and took liability for telemarketing sales involving false statements about the performance and security of a computer to consumers in the United States. He also personally did business in the United States as the CEO of United States corporations. For example, he is the CEO of United States corporation asknet, Inc. and entered into an agreement with, and opened a merchant account

used to process credit card charges with Global Collect Services, USA, a United States corporation also doing business as Ingenico.

12. At times material to this Complaint, acting alone or in concert with others, he has formulated, directed, controlled, had the authority to control, or participated in the acts and practices of Nexway AG, Nexway SAS, Nexway, Inc., asknet, Inc. set forth in this Complaint. In connection with the matters alleged herein, he transacts or has transacted business in this District and throughout the United States.

13. Defendant Casey Potenzone was the Chief Strategic Officer of Nexway AG, Nexway SAS and Nexway Inc. from on or about October 2017 to December 2020. He is a United States citizen and resides in Holland. He was also the Senior Vice President of Sales and Marketing for Nexway AG, Nexway SASU and Nexway, Inc. from June 2016 to October 2017, and the United States Director of Sales for Nexway AG, Nexway SAS, and Nexway Inc. from October 2014 to May 2016. He was a member of the Executive Board and Leadership Committee of Nexway AG and Nexway SASU from on or about July 2019 to December 30, 2020. He was the Secretary of asknet, Inc. from September 13, 2019 to September 4, 2020 and was identified as the President of asknet, Inc., in a February 2020 loan agreement between asknet, Inc., and Nexway AG. Defendant Potenzone controlled and operated companies that did business in the United States, assisted and facilitated telemarketers who targeted consumers in the United States, engaged in credit card laundering in the United States, or claimed to be the merchant and took liability for telemarketing sales involving false statements about the performance and security of a computer to consumers in the United States. He also personally did business in the United States as the Secretary and President of a United States corporation, asknet, Inc. At all times material to this Complaint, acting alone or in concert with others, he has formulated, directed, controlled, had the

authority to control, or participated in the acts and practices of Nexway AG, Nexway SASU, Nexway Inc. and asknet, Inc. set forth in this Complaint. In connection with the matters alleged herein, he transacts or has transacted business in this District and throughout the United States.

COMMON ENTERPRISE

14. Defendants Nexway SASU, Nexway Group AG, asknet Solutions AG, Nexway, Inc., and asknet, Inc. (collectively "Nexway") have operated as a common enterprise while engaging in the deceptive and unfair acts and practices and violations of the TSR as alleged below. Nexway has conducted the business practices described below through an interrelated network of companies that have common ownership, officers, managers, business functions, employees, and office locations. Because these Corporate Defendants have operated a common enterprise, each of them is liable for the acts and practices alleged below.

COMMERCE

15. At all times material to this Complaint, Defendants have maintained a substantial course of trade in or affecting commerce, as "commerce" is defined in Section 4 of the FTC Act, 15 U.S.C. § 44.

DEFENDANTS' BUSINESS ACTIVITIES

16. Since at least August 2016, Nexway provided its foreign tech support scammer clients, including Tech Live Connect Pte Ltd, Saburi TLC, and Sensei Ventures, Inc., which collectively did business as Tech Live Connect and Premium Techie Support (collectively, "Tech Live Connect" or "TLC"), substantial assistance and surreptitious access to the United States credit card system, thus allowing the tech support scammers to charge and obtain money from duped consumers.

17. Defendants are located in the United States, do business with United States corporations to open and use a merchant account to submit credit card charges for processing,

submit charges involving United States consumers' credit cards and bank accounts, and receive money withdrawn from United States consumers' bank accounts. Defendants engaged in credit card laundering in the United States.

18. Defendants have processed credit card charges that were associated with one or more telemarketers located in the United States or whose principal is located in the United States, as well as additional telemarketers located elsewhere, through merchant accounts in Defendants' names. All of these telemarketers targeted and injured United States consumers through making false statements to consumers about the performance and security of their computers

19. The Defendants' acts or practices have caused reasonably foreseeable injury within the United States or involve material conduct occurring within the United States.

20. Tech Live Connect and other Nexway tech support telemarketing clients, made misrepresentations about the performance and security of consumers' computers to market and sell tech support services to consumers. Nexway caused the credit card information of consumers duped by Tech Live Connect and other tech support victims to be submitted into the credit card system through Nexway's own merchant account.

21. Ordinarily, sellers must obtain merchant accounts to process consumer credit card payments for the seller's good or services. By using its own merchant account to process consumer payments for third parties, Nexway made it possible for its clients engaged in tech support scams to obtain furtive access to the credit card system and evade detection by the card brands for a longer period of time. The charges Nexway surreptitiously placed in the credit card system and the collection of money consumers paid is the life-blood of tech support scams.

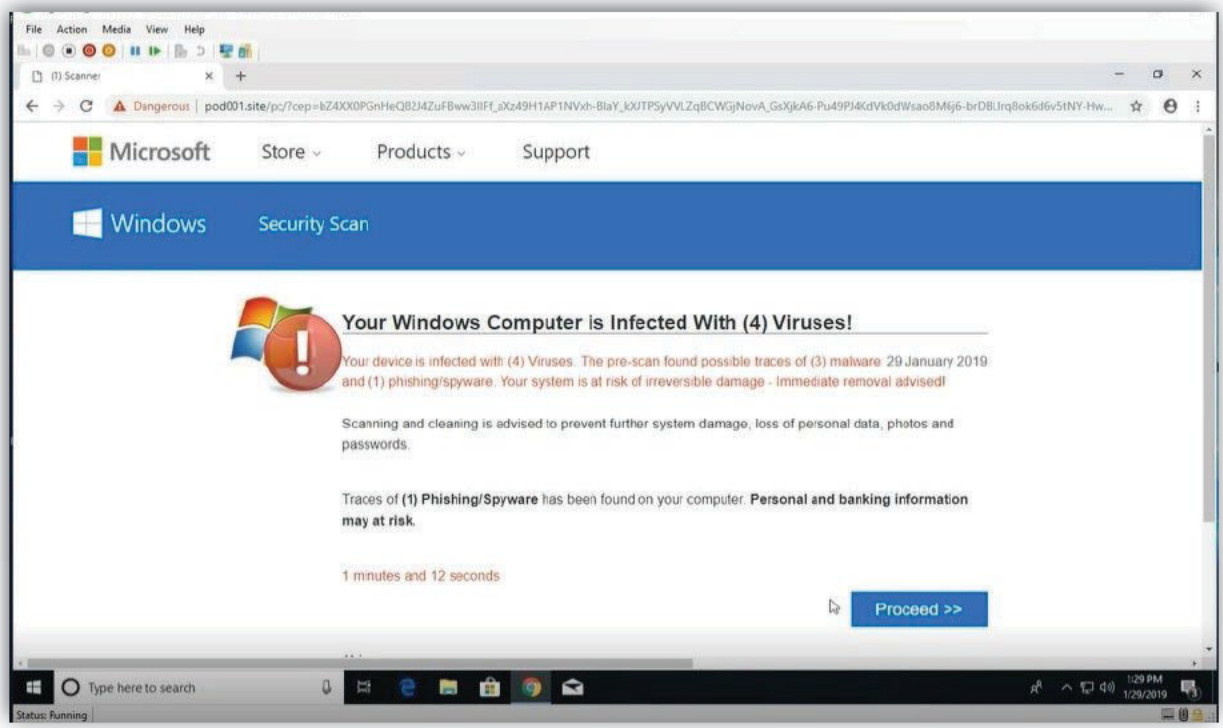
22. Nexway engaged in this activity even though it and its officers knew or consciously avoided knowing that its tech support clients were engaged in deceptive telemarketing practices.

23. Nexway claims to use a Merchant of Record ("MoR") business model. Under Nexway's MoR model, consumers or customers, after being subjected to deceptive pop ups and misrepresentations by the Tech Live Connect telemarketers, enter their credit card numbers into an online payment page that is supported by Nexway and includes the Premium Techie Support (the dba for Tech Live Connect) and Nexway name in order to pay for the bogus tech support services. Consumers receive emails from premiumtechiesupport-en.@nexway.com confirming the purchase. The charges on consumers' credit card statements include the name Nexway. Nexway admits that it is liable for the sales conducted when it undertakes to process transactions under the MorR business model. Nexway is a business that collects money from consumers under the Nexway name.

The Tech Live Connect Pop Up Scam

24. In numerous instances, Tech Live Connect used deceptive pop ups to ensnare consumers between August 2016 and February 2020.

25. The pop ups included the following:



26. Hitting the "Proceed >>" button downloaded software that, when run, indicated that the computer had hundreds of unwanted items, and provided a phone number to call.

27. In other instances, the pop ups appeared to freeze consumers' computers and directed them to call a toll-free number for assistance. One consumer described the following experience in their Better Business Bureau complaint against Nexway: "My computer locked up and a siren went off and an alert came up on the screen saying contact Microsoft about a virus along with a phone number."

28. Worried consumers subsequently called the number, which connected them to Tech Live Connect and its telemarketers.

29. Tech Live Connect and the telemarketers subsequently made additional misrepresentations including, (1) false representations about the performance and security of

consumer's computers; and (2) misrepresentations that Tech Live Connect's telemarketer was associated with legitimate companies, such as Microsoft.

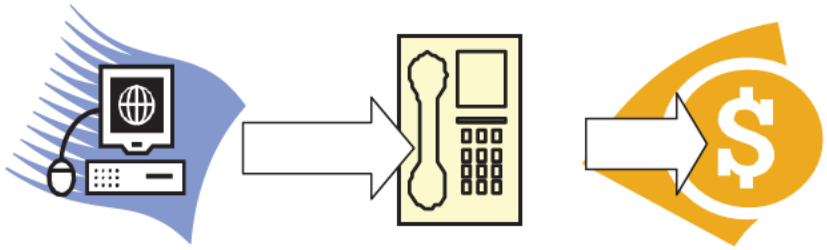
30. Tech Live Connect also injured consumers through another scheme. Consumers searching for software to enhance computer performance, sometimes would search, locate and download third-party software onto their computer. In order to activate the software, consumers needed to call a phone number, which was the number for Tech Live Connect. During those calls, Tech Live Connect would make false statements as part of upsell sales pitches to induce consumers to purchase their tech support services. These statements included the following: (1) your computer is "overwhelmed by thousands of bugs and issues," (2) "your computer lacks security, any foreign address can be connected to your computer and easily they can scam your details during an online transaction," and (3) "you have a virus due to which your drivers are not working."

31. As part of the transaction with Tech Live Connect, consumers provided their credit card information and were charged hundreds of dollars. Nexway submitted the credit card charges through its own merchant accounts with Adyen (a Dutch payment company), Deutsche Bank and other acquirers (an acquirer is a financial entity, or its agent, who is authorized to deposit charges into the credit card system).

32. Nexway subsequently received payment for the charges, which came from consumers, and after deducting its commission, which according to their signed agreement, was 7% for new charges and 8% percent for recurring charges, sent the money to Tech Live Connect.

33. Nexway provided substantial assistance through its processing services for Tech Live Connect and other tech support scam telemarketers, causing credit card charges to be

submitted into the credit card systems for payment, and distributing the funds to telemarketers as shown in the complaint graphic below:



Consumer (1) receives a deceptive pop up on his or her computer directing the consumer to call a number which leads to a telemarketer or (2) calls to activate software which leads to a telemarketer.

Telemarketer at call center deceptively pitches tech support services and charges consumers.

Nexway uses its merchant account to cause an acquirer to submit charges into the credit card system, collects money from consumers, and after taking a share, transfers the funds to companies scamming consumers.

34. In September 2020, Indian authorities raided the boiler rooms and offices of Tech Live Connect and other Nexway tech support telemarketing clients. According to the Indian authorities, the companies allegedly sent pop up messages to consumers' computers, giving bogus warnings about purported security issues and presence of malware. The pop ups displayed the phone number of a boiler room. If consumers called the phone number, telemarketers allegedly advised the consumers to install certain anti-malwares or anti-virus software. "The victims are allegedly given the option to activate the [software] by paying a fee online or by calling a support number advertised in the interface of the [program]. The victims are fraudulently influenced in this manner and allegedly fall in their trap to maintain their systems properly," an Indian Central Bureau of Investigation spokesperson told the press. *See* www.tribuneindia.com/news/nation/cbi-books-6-firms-for-installing-malware-on-peoples- computers-142533.

35. Less than one month later, the Department of Justice sued Brian Cotter doing business as Tech Live Connect and others. The court entered a Consent Decree in March 2021.

US v. Michael Brian Cotter, et al., Case No. 1:20-CV-24216-RNS (Complaint filed 10/15/20, Consent Decree entered 12/23/2020). The complaint alleged that Cotter worked with co-conspirators in India from at least 2011 to 2020 to operate a tech support fraud scheme. The scheme allegedly contacted consumers via internet pop-up messages that falsely appeared to be security alerts from Microsoft and another well-known company. The pop up messages fraudulently claimed that the consumer's computer was infected by a virus, purported to run a scan of the consumer's computer, falsely confirmed the presence of a virus and malware, and then provided a toll-free number to call for assistance. When victims called the toll-free number, they were connected to India-based call centers participating in the fraud scheme. Call center workers asked victims to give them remote access to their computers and told victims that they detected viruses and other malware on their computers. Eventually, the call center workers would falsely diagnose non-existent problems and ask victims to pay hundreds of dollars for unnecessary services and software.

Nexway Obtains Merchant Accounts in Its Name and Uses the Accounts For Charges Relating to TLC and Other Tech Support Scams

36. Since from around August 2016 to at least March 2020, Nexway used merchant accounts in its name to submit third-party tech support charges that arose from transactions between consumers and Tech Live Connect and other telemarketing tech support scams, which Nexway referred to collectively as their Premium Tech Support or PTS clients, into the credit card system.

37. In August 2016, Nexway executed a "Digital Partnership Agreement" with Tech Live Connect. Nexway's Digital Partnership Agreement with Tech Live Connect, and other telemarketing tech support clients, states, among other things, that "Nexway will be the seller and merchant of record for all Product sales to End Users [consumers];" Nexway has the right to set

the price at which each product is offered for sale; and that as "the seller and merchant of record, Nexway is responsible for setting the returns and cancellations policy applicable to the Products sold by Nexway." Moreover, Appendix 1 to the TLC Digital Partnership Agreement, includes a workflow diagram which shows what appears to be a telemarketer remotely accessing and controlling a consumer's computer as step 1, which is followed by the consumer providing their payment information.

38. In December 2017, Nexway executed a "Digital Distribution Agreement" with Saburi TLC. Like the Digital partnership Agreement, the Digital Distribution Agreement with Saburi TLC identified Nexway as the "seller and merchant of record" for all Saburi TLC products marketed and sold via Nexway.

39. Nexway entered into a merchant agreement with Adyen for processing servicesthrough Adyen and Deutsche Bank. Nexway represented that it sold goods or services through an online computer store. Nexway signed the contract on March 4, 2014. Adyen was the agent of Deutsche Bank. Nexway's merchant agreement with Adyen notes that:

> Adyen's acceptance of Merchant [Nexway] as user of the Services and the relevant Payment Methods is strictly personal and limited to the use by Merchant of the Services for payment of Merchant's own products and services. Merchant may not use the Services to facilitate the payment for products or services sold by third parties and therefor may not resell the Services to third parties.

40. Nexway processed Tech Live Connect charges through their processing accounts with Adyen in 2017, 2018, and 2019.

41. In September 2016, Nexway entered into an agreement with Ingenico ePayments ("Ingenico") for processing services. Iezuitov executed another agreement on behalf of asknet, Inc., a US company, with Ingenico in October 2019. The October 2019 agreement with Ingenico included language specifying that asknet agreed to comply with FTC regulations. Ingenico also

does business as Global Collect Services BV and Global Collect. The acquiring bank for these transactions was WorldPay. Ingenico was WorldPay's agent.

42. Nexway processed Tech Live Connect charges through their processing accounts with Ingenico and Global Collect (including the asknet account obtained in October 2019) from at least February 2018 until February 2020.

43. Furthermore, in 2007, Nexway entered into an agreement with PayPal for processing services. In March 2015, Nexway re-executed a merchant agreement with PayPal for processing services.

44. Nexway processed Tech Live Connect charges through their processing accounts with PayPal from at least February 2018 until the end of January 2020.

45. Nexway's unlawful practices resulted in substantial consumer injury.

Iezuitov and Potenzone
Controlled and Participated in Nexway's Unlawful Actions

46. Victor Iezuitov and Casey Potenzone controlled and participated in Nexway AG's, Nexway SASU's, Nexway, Inc.'s, and asknet, Inc.'s business activities, including providing payment processing services to clients that were telemarketing tech support services, such as Tech Live Connect and Econosoft. Additionally, they monitored the business activities of Tech Live Connect, Econosoft and other Nexway clients marketing tech support services, and made decisions on whether to take disciplinary action or terminate them for deceptive practices. Iezuitov and Potenzone knew or consciously avoided knowing that Nexway was submitting charges through its own merchant accounts for companies engaged in selling purported tech support services.

47. Nexway processed at least $1.7 million in Tech Live Connect tech support charges, and $2.2 million in Econosoft charges after Iezuitov became Nexway's CEO.

48. Potenzone participated in the laundering scheme. For example, in March 2017, Potenzone asked TLC to increase the number of sales it processed through Nexway so he could meet a sales target. TLC responded by sending more sales to Nexway to be processed during the last ten days of March 2017.

Defendants Knew or Consciously Avoided Knowing about Tech Live Connect and Other Tech Support Call Centers' Unlawful Practices and Nexway's Unlawful Credit Card Laundering

49. Since in or around August 2016, Nexway knew or consciously avoided knowing that its client, Tech Live Connect, and other foreign tech support call centers clients, made false or misleading statements to induce consumers to pay for purported tech support services. Yet, Nexway continued to illegally process Tech Live Connect's unlawful charges through its merchant accounts until at least February 2020.

50. Similarly, Iezuitov and Potenzone knew or consciously avoided knowing that companies marketing tech support services, including Tech Live Connect and Econosoft, were engaged in deceptive practices. However, both continued the processing of Tech Live Connect's charges under Nexway's name

51. Since on or about October 2017, Potenzone knew or consciously avoided knowing that its client, Tech Live Connect, and other clients operating foreign tech support call centers, made false or misleading statements to induce consumers to pay for purported tech support services.

52. Since around July 2019, Iezuitov knew or consciously avoided knowing that its client, Tech Live Connect, and other clients operating foreign tech support call centers, made false or misleading statements to induce consumers to pay for purported tech support services. Even prior to becoming the CEO of Nexway, Iezuitov received emails and other communications

containing obvious "red flags" about Nexway's tech support clients. For example, while he was on the Board of a company that had an ownership interest in Nexway, Iezuitov:

a. Received and responded to a June 4, 2019 email discussing one tech support client's use of prepaid cards to create bogus $3 micro transactions as a method to lower its chargeback rate to an acceptable level;

b. Received a June 5, 2019 email stating that Nexway's actions could be seen by the police as "assistance to fraud;" and

c. Received a June 24, 2019 email titled: "Plainte client au sujet de Vacillate" (Customer complaint about Vacillate), stating that Nexway was shielding PTS clients from the judiciary.

53. Nexway, Iezuitov and Potenzone also all knew that Nexway AG or Nexway SASU used its own merchant account to cause a payment processor or financial institution to submit charges into the credit card system that arose from transactions between consumers and companies offering telemarketed tech support services, including Tech Live Connect, to collect payment for those charges from consumers' bank accounts, and to transmit those funds, after deducting fees, back to such companies.

54. Nexway received many indications that Tech Live Connect and other foreign tech support call center clients of Nexway were engaged in unlawful practices, including the following: (1) numerous consumer complaints, including complaints that Nexway received directly from consumers by mail and phone, and complaints forwarded to Nexway by the Better Business Bureau ("BBB") and state attorneys general; (2) police reports and inquiries; (3); a complaint from another Nexway client, which is a software company specializing in virus detection, about Tech Live Connect making misrepresentations to consumers; (4) a newspaper article that detailed Tech

Live Connect's fraudulent telemarketing practices; (5) chargebacks and inquiries from Visa and Mastercard; (6) being placed in the VISA and Mastercard chargeback monitoring program; (7) being told by one or more payment processors to stop sending charges from Tech Live Connect; (8) a letter from the BBB noting that Nexway's clients used pop-up ads "claiming to be Microsoft" and asking Nexway to identify its procedures for handling scammers using its services; and (9) emails from their agent notifying them of a Nexway client tech support telemarketer's unlawful use of prepaid cards to create bogus $3 micro transactions as a method to lower its chargeback rate. Iezuitov and Potenzone received many of these warnings.

55. Despite these warnings, Nexway continued to process payments for Tech Live Connect and other foreign tech support call centers; ignoring advice from its own expert whom it hired to identify telemarketers engaged in fraud.

Timeline of Events

2016

56. Defendant Potenzone solicited Brian Cotter and Tech Live Connect to enter into a contract with Nexway. On August 3, 2016, Nexway entered into contract with Tech Live Connect. At the time Nexway entered into the contract with Tech Live Connect, Nexway and Potenzone knew that Tech Live Connect operated a call center in India marketing tech support services.

57. Nexway did not request or obtain copies of any scripts used by Tech Live Connect telemarketers prior to entering into a contract with Tech Live Connect, or afterward.

2017

58. Starting no later than January 2017, Nexway began receiving consumer complaints about TLC. Many of the complaints expressly referenced Tech Live Connect's use of deceptive pop ups.

a. For example, in a complaint received by Nexway that was filed with the BBB on June 1, 2017, the consumer stated, "[I] was on line running my computer when a message flashed across the screen that my computer was infected with a virus."

b. In addition, in a complaint received by Nexway that was filed with the BBB on March 20, 2018, the consumers stated, "I received a pop-up on my Mac computer saying my computer was seriously infected and that I needed to call a phone number immediately to rectify it. The pop-up appeared to be from Apple, and I thought I was calling Apple."

59. In February 2017, Nexway and Potenzone knew that a third party software company Nexway client had complained to them about Tech Live Connect making misrepresentations to consumers about the security of their computers. The misrepresentations included the following claim: "the security on your computer is missing, and you have a virus that is preventing your drivers from working." As part of that complaint, Nexway and Potenzone also knew that consumers who were interested in the software called a phone number to activate it, and were connected to Tech Live Connect. They further knew that telemarketers at Tech Live Connect then used misrepresentations to upsell separate purported consumer repair services.

60. In a March 20, 2017 email to Tech Live Connect president, Brian Cotter, Potenzone told Cotter "I have to do the sales guy thing. Can you give us a boost anywhere? I'm really really close to one of my quarterly goals … and am pulling a few strings to goose it." Cotter forwarded the email to his staff saying, "Let me know thoughts on below…and if we can wiggle any more sales onto Nexway in March," and Tech Live Connect diverted additional sales to Nexway for the last ten days of March 2017.

61. In early April 2017, the Hindustan Times published an investigative reporting article about TLCs deceptive practices with the headline "Scare and sell: Here's how an Indian

call centre cheated foreign computer owners," which was posted on the internet. It detailed TLC's/Premium Techie Supports' use of deceptive pop ups and deceptive telemarketing practices, including telemarketers misrepresenting their affiliation with Apple.

62. Potenzone and Nexway were aware of the Hindustan Times article by no later than April 11, 2017. Specifically, Brian Cotter admitted to Potenzone that the Tech Live Connect telemarketer had made a misrepresentation and that the telemarketer had not been fired.

63. Nexway's own documents show that Potenzone also went to the FTC Website in April 2017 and read a press release which detailed the deceptive practices of five tech support scams sued by the FTC, stated that the practices violated the Telemarketing Sales Rule, and contained links to the complaints which alleged violations of the Telemarketing Sales Rule and described the rule. The press release and link to the cases are located at https://www.ftc.gov/news-events/press-releases/2014/07/federal-court-orders-tech-support-scammers-pay-more-51-million.

64. Nexway continued to process Tech Live Connect's charges.

65. Nexway monitored Tech Live Connect's chargebacks. It also profited from the chargebacks since it charged Tech Live Connect and other companies a fee for each chargeback.

66. Consumers initiate "chargebacks" when they dispute credit card charges by contacting their "issuing bank," which is the bank that issued the credit card to the consumer. When a consumer successfully disputes a charge, the consumer's issuing bank credits the consumer's credit card for the disputed amount, and then recovers the chargeback amount from the "acquiring bank," the bank which provided Nexway with access to the credit card network. Here, the acquiring bank would, in turn, collect the chargeback amount from Nexway.

67. For example, on February 10, 2017, the Senior Key Account Manager at Nexway sent Potenzone an email titled "Nexway/TechLiveConnect: Chargeback & Cancellation rates."

The February 10, 2017 email included a table showing Tech Live Connect had (1) chargeback rates of 2.2% in November 2016, 2.6% in December 2016, and 1.5% in January 2017; and (2) cancelation rates of 23.2% in November 2016, 27% in December 2016, and 21.8% in January 2017.

68. In order to detect and prevent illegal, fraudulent or unauthorized merchant activity, the credit card networks operate various chargeback monitoring and fraud monitoring programs. For example, if a company generates excessive levels of chargebacks that trigger the one percent thresholds set under Visa's and Mastercard's Chargeback Monitoring Program, the company is subject to additional monitoring requirements and, in some cases, penalties and termination.

69. Nexway had such high chargebacks that Visa placed the company in its Chargeback Monitoring Program in December 2017.

2018

70. In January 2018, Nexway submitted a chargeback remediation plan to Adyen, Deutsche Bank, and Visa, which included numerous false representations. For example, Nexway represented its business as a computer software store. It also included the following statement describing its business model:

> "Nexway is a leader in digital distribution of software, games or services. Nexway is selling software/games/services on behalf of its merchants to consumers whereby Nexway takes full ownership."

Additionally, Nexway's remediation plan included a form that included boxes to check to describe the nature of Nexway's business. Nexway checked the box for retail sales. It did not check the box for telemarketing. Nexway also indicated that the transactions involved credit cards on file (rather than "card not present" transactions used for internet and telephone purchases, which are subject to additional scrutiny from card networks due to their higher propensity for fraudulent transactions).

71. In reality, Nexway was providing processing services to a number of telemarketers. The transactions were not computer store sales or retail sales. They involved telemarketing and card not present transactions, not credit cards on file, as Nexway indicated in its remediation plan. Moreover, Tech Live Connect's chargebacks were a primary reason for Nexway's inclusion in the Chargeback Monitoring Program, as Nexway was aware. Nexway also knew that Tech Live Connect engaged in the telemarketing of tech support services, not software, games or retail sales.

72. Also in January 2018, in an email with the subject line Adyen-Visa Monitoring and Remediation Plan, Nexway identified Tech Live Connect and Econosoft as having high levels of chargebacks.

73. The same month, January 2018, Potenzone and Nexway learned of a BBB report, which was (and still is) available at https://www.bbb.org/globalassets/article-library/tech-scam-study/bbb-computer-tech-support-study.pdf. The report detailed how tech support scams worked. For example, Potenzone sent an email to others at Nexway in January 2018 informing them of (1) a BBB report that explained how tech support scams worked, including through the use of pop ups, and which included a reference to the Telemarketing Sales Rule, and (2) FTC cases brought against tech support scammers as part of Operation Tech Trap, which included the following link to an FTC press release:https://www.ftc.gov/news-events/press-releases/2017/06/operators-tech-support-scam-settle-ftc-charges. Nexway also had a hard copy of the report in its business records.

74. The FTC press release described in detail one of the FTC complaints, which alleged a scheme in which Defendants worked with affiliate marketers to place pop-up ads falsely claiming that a consumer's computer was infected using ads that purported to originate from legitimate technology companies like Apple or Microsoft. The ads included dire warnings and

urged consumers to immediately call a toll-free number for help. When consumers called the number, they were connected to telemarketers based in India. The telemarketers claimed they needed remote access to consumers' computers in order to diagnose the problem. Once given access, the telemarketers showed consumers innocuous screens and directories on the computers, deceiving consumers into believing that these were evidence of problems that required immediate repair.

75. The BBB received so many complaints about Nexway that it started an investigation of the company and sent a letter to Nexway seeking more information about its business model. The February 2018 letter included the following statement and requests:

> Current complaints on file state that consumers receive a pop up ad claiming to be Microsoft which states that their computer is infected…Because consumers believe your company is responsible for the pop up ads and your responses state otherwise, BBB would like your company to provide clarification on the following:
>
> 1. What is your policy when your business becomes aware that a scam company is using your platform?
> 2. What requirements are needed to use your company's platform.
> 3. Please provide a list of company principals. Please provide contact name, title, email and direct dial number.

Nexway did not respond to the BBB's questions. The BBB received over a hundred complaints relating to Nexway and awarded Nexway an "F" rating. Nexway did respond to individual BBB complaints by stating that it manages billing for different companies.

76. In February 2018, Adyen required Nexway to stop sending credit card charges for TLC.

77. Subsequently, Nexway sent Tech Live Connect's credit card charges to Ingenico to be submitted into the credit card system. WorldPay was an acquiring bank for these charges.

78. In March 2018, Nexway received a letter from the Missouri State Attorney General's office forwarding a complaint from a consumer about Tech Live Connect. Between

March 2018 and January 2020, Nexway also received letters from Attorneys General in the states of Ohio, Michigan, Wisconsin, and Kansas forwarding complaints from consumers relating to charges from tech support companies for which Nexway provided credit card processing services.

79. In April 2018, Nexway received a complaint from a consumer about Tech Live Connect. In the complaint, the consumer noted that the Tech Live Connect telemarketer misrepresented that they were with Apple Inc. and charged the consumer $699.95 to "fix" the consumer's computer.

80. In May 2018, Visa again placed Nexway in its chargeback monitoring program. Mastercard also placed Nexway in its chargeback monitoring program the same month.

81. Subsequently, Nexway planned to engage in "load balancing" to hide Tech Live Connect's high chargeback rates. Load balancing involves combining charges from a company with low chargebacks with one with high chargebacks. Load balancing is used to dilute or reduce the overall chargeback number. For example, an email dated July 24, 2018, authored by Potenzone stated the following:

> "We need volume from other business to dilute the chargeback volume…How does adding PC Vark reduce the TLC chargeback levels? It won't say TLC and the PSP's won't know its TLC volume…" ["PSP" refers to payment service providers, including payment processors]

82. In October 2018, Ingenico told Nexway about numerous people who had complained about virus alerts on their computers relating to charges Nexway submitted to Ingenico. Nexway told Ingenico in a November 7, 2018 email that Nexway had stopped processing payments for the two Nexway "customers" causing the complaints – "Tech Live Connect and Sensei." Yet, in truth, Nexway continued to submit charges through Ingenico on behalf of Tech Live Connect. Nexway submitted these charges through its own merchant account.

83. In December 2018, Ingenico warned Nexway about its clients, including Saburi, engaging in a scam. Nexway also responded that they were aware that the clients were using telemarketing.

2019

84. In or about early February 2019, Nexway and Potenzone received emails related to a complaint about TLC from a newspaper reporter. In the complaint, the reporter noted that Premium Techie Support used pressure tactics on his elderly mother, claiming that her computer was hacked and that if she did not immediately arrange technical help her identity would be stolen. The reporter also noted in the complaint that Premium Techie Support had improperly used his mother's fear of cybercrime to charge more than £1600 on her credit card for repair services for an old computer worth only £200.

85. In April 2019, Nexway admitted that its clients knew that Nexway preferred to turn a blind eye to unlawful activity. For example, an April 1, 2019 email from Nexway's in- house counsel to Potenzone states that "Premium Tech Support" clients (which refers to a group of clients that include the TLC entities): "know that for the moment we prefer to cash in and turn a blind eye…"

86. Nexway discussed implementing a formal chargeback monitoring program. However, it decided to take action only with new clients. For example, the same April 1, 2019 email above states the following:

> [W]hen the chargeback rate exceeds > 0.9 we implement a Chargeback Monitoring Program (which involves firstly a step up in Chargeback fees for the client. If nothing changes after a few months a huge penalty will be invoiced to the Client and if that has no effect, then after a year it may end up wiht (sic) the termination of the contract). Of course these conditions only apply to new customers. For former customers, it would be necessary to sign addendums, but it's unlikely that they consent to such new pricing terms willingly.

87. On April 3, 2019, the asknet Vice President for eCommerce Solutions sent an email to a representative of Tech Live Connect stating:

> I have to inform you that we have to stop selling your service to german (sic) endcustomer because of too many police complaints. We had a very intensive conversation with the german (sic) police and they mad (sic) it very clear that there is a high risk for us if we continue handling your service to german (sic) endcustomers.

The Tech Live Connect representative called the asknet Vice President for eCommerce Solutions and reported in an April 4, 2019 email that the asknet VP told him that Defendants had:

> [B]een in regular touch with the local German cops on complaints received on tech support sales done on their platform and have been averting any major action on them (by using good contacts with the coos (sic)) such as a house search on their office premises (4 times they have managed to avoid), but it finally reached a stage where it was unavoidable and their cop liaison told them that anymore complaints, house search on their premises in inevitable. Thus, their CEO decided to STOP German tech support processing for all remaining active accounts with immediate effect. (emphasis in original).

88. Nexway knew that some of its tech support telemarketing clients were using prepaid cards and micro transactions to lower artificially their chargeback rate. For example, on June 3, 2019, Potenzone received an email from Nexway agent Nicholas Forcier confirming that a tech support telemarketer was using prepaid cards to lower chargeback levels. Potenzone shared this email with Iezuitov on June 4, 2019, and in July 2019, Nexway staff confirmed that the telemarketer was using prepaid cards to add "micro transactions at about $3 on our checkouts."

89. Nexway knew that: (1) the German police were investigating asknet and Nexway, (2) both companies had already attracted the attention of credit card associations because of high chargebacks, and (3) both companies had appeared in BBB complaints. For example, a June 5, 2019 email from a Management Board member of asknet AG states the following:

> Both companies already attracted the attention of PSPs [payment service providers] and credit card organizations, have to deal with police complaints and appeared in media, internet and BBB complaints. …Summary of Meeting

> 27.05.19 with german (sic) police. Asknet was informed of suspicions for 15! (sic) of asknets (sic) clients to be involved in fraudulent activities. In most researches it was reported that money was charged "unauthorized"….German "federal prosecution" issued a confiscation of Servers at asknet—our contact at German police could avert it. This may not be possible for future incidents and it was already the second time this could be avoided. We are (sic) now been informed about this and there is note about this in the file, if we do not react or change something, this can (and will) be seen as "Assistance to fraud".

Iezuitov and Potenzone received the email.

90. Also, in a June 24, 2019 email exchange that included Potenzone and Iezuitov about the latest complaint about Vacillate, a Nexway PTS client:

a. Nexway's legal advisor noted that the attached online discussion "below is the latest exchange concerning PTS fraud;"

b. Potenzone replied that, "[w]e know the nature of this business and all need to be extra diligent in our responsibilities to better the company. But we will be more doomed shutting down PTS today then we will be juggling their revenue;"

c. Nexway's legal advisor responded that, "PTS are well aware that we are trying to shield them from the judiciary" and "as we backed down from each attempt to reinforce the coercive nature of our contracts, there is not much we can do."

91. Moreover, a July 11, 2019 email with the subject "PTS Issues" that was sent from asknet's Business Operations Teamleader to both Potenzone and Iezuitov included an attachment of the same name. The attachment included the June 5, 2019 email with its discussion of the German police, and additionally which noted, among other things, that:

a. Microsoft Legal Department called and the told Nexway that they had collected hundreds of thousands of claims; 35 call centers in India had been closed; and 100s of persons in India had been arrested;

b. The tech support companies had a "Bad risk rating at PSPs [payment service providers]," with WorldPay telling them "openly when discussing new conditions, want to introduce much higher monthly minimum, showed bad fraud rates for both companies," and noted that PSPs were telling them [Nexway] that there were "[t]oo few „good (sic)" transactions to compensate the „bad (sic) ones;" and

c. Adyen requested that Nexway stop submitting Discover charges due to high fraud and chargeback figures.

92. Nexway intentionally shielded the telemarketers engaged in deceptive practices from law enforcement. For example, a June 24, 2019 email from in-house counsel states the following:

> I'm well aware of the financial situation we are facing… PTS [Premium Tech Support Clients] are well aware that we are trying to shield them from the judiciary…we will be more doomed shutting down PTS today…

Iezuitov and Potenzone received this email.

93. The minutes of a July 11, 2019 leadership meeting at Nexway, which included Iezuitov and Potenzone, show that Nexway was strongly dependent on its Premium Tech Support clients, which represented 25% of Nexway's revenue. The minutes also show that the meeting involved reviewing the "toxic traffic" for each client, and then it would be up to the leadership, including Victor Iezuitov and Casey Potenzone, to act.

94. Nexway hired Associate Professor Nick Nikiforakis on or around July 18, 2019, to provide advice on how to identify telemarketers engaged in fraud. On July 29, 2019, Professor Nikiforakis provided concrete options in a written document that Nexway could use, including mystery shopper or undercover calls by written submission. Iezuitov and Potenzone received the written document.

95. Nexway did not adopt any of Professor Nikiforakis' recommendations and continued to process credit card charges for Tech Live Connect.

96. In a September 23, 2019 email from Potenzone to Iezuitov titled PTS updates, Potenzone wrote that Econosoft, Assured Money and Vacillate were to be considered as one consolidated entity, and that Assured Money had engaged in fraud.

97. In an October 9, 2019 email exchange between Iezuitov and Potenzone, the two discussed steps that could be made to pay monies owed to Econosoft, another PTS client, who also operated under the dbas Assured Money and Vacillate, so that Econsoft would not stop sending tech support transactions to Nexway. Iezuitov and Potenzone continued to provide processing services even though they knew Econosoft was engaged in deceptive practices.

2020

98. The FTC served a Civil Investigative Demand ("CID") on Nexway on February 3, 2020. The CID stated that the FTC was investigating the company to determine, among other things, whether it was engaged in credit card laundering, and assisting and facilitating unlawful conduct in violation of the Telemarketing Sales Rule.

99. Only after receiving the CID, Victor Iezuitov sent Saburi TLC a letter, dated March 17, 2020, in which he recognized the red flags showing that Tech Live Connect was engaged in unlawful practices. The letter stated:

> Your company's risk profile doesn't match the industry standards imposed to us by our Payment Service Providers. Hence, due to your unusually high refund rates, we were asked to suspend all transactions on your accounts. In parallel, we were alerted by a huge amount of negative reviews and after investigation, have come to the conclusion that your activity bears a too high fraud potential. This obliges us to act urgently and make use of our right of rescission. …Moreover, should Nexway be held liable by consumers or any criminal authorities further to the fraudulent acts referred to herein, we will inform you without delay in order to trigger the warranty and indemnification process allowed by law.

100. Nexway's actions caused Deutsche Bank, WorldPay, and other acquirers, to deposit over $18 million of charges from Tech Live Connect's transactions with consumers into the credit card system for payment from approximately August 2016 to approximately February 2020. Nexway also deposited tens of millions of dollars in charges from other Premium Tech Support clients, including Econosoft, from approximately October 2018 until approximately March 2020. The charges included records of credit card transactions, also known as credit card sale drafts. These drafts were generated by a telemarketing transaction between Tech Live Connect or other Premium Tech Support clients and consumers that was not the result of a telemarketing credit card transaction between the cardholder and Nexway.

101. Based on the facts and violations of law alleged in this Complaint, the Plaintiff has reason to believe that Defendants are violating or are about to violate laws enforced by the Plaintiff and the FTC because, among other things: they had, for years, laundered charges, processed Tech Live Connect's and others telemarketers' unlawful charges through its merchant accounts, they engaged in their unlawful conduct knowingly, continued their unlawful practices despite consumer complaints, Visa placing them in the Merchant Chargeback Monitoring Program, and their processor telling them to stop doing business with Tech Live Connect, and issued a termination letter to Tech Live Connect only after receiving a CID from the FTC.

VIOLATIONS OF THE FTC ACT

102. Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), prohibits "unfair or deceptive acts or practices in or affecting commerce." Acts or practices are unfair under Section 5 of the FTC Act if they cause or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition. 15 U.S.C. § 45(n). Misrepresentations or deceptive omissions of material fact constitute deceptive acts or practices prohibited by Section 5(a) of the FTC Act.

Count I
Section 5 Unfairness Count

103. In numerous instances, Defendants have submitted credit card charges through Nexway's merchant account for an entity that made false statements to consumers.

104. Defendants' actions cause or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition.

105. Therefore, Defendants' acts or practices as set forth in Paragraph 103 constitute unfair acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(a), (n).

Count II
Misrepresentations to Consumers
(Pled in the Alternative)

106. Defendants submitted the credit card charges related to Tech Live Connect and others sale of tech support services through merchant accounts in Defendants' name, identifying themselves to payment processors, acquiring banks, consumers, or their telemarketers, as the seller and merchant of record and taking "full ownership" of the charges processed through Defendants' merchant accounts. Defendants also entered into agreements with Tech Live Connect and other entities, and admit to being the seller.

107. In numerous instances in connection with the offering for sale of tech support services, Defendants have represented, directly or indirectly through Tech Live Connect and other telemarketers, expressly or by implication, that, among other things, they have identified significant performance or security problems on consumers' computers, including that consumers' computers are infected with a virus; and that the telemarketer was associated with legitimate companies, such as Microsoft.

108. In truth and in fact, in numerous instances in which Defendants, directly or indirectly, have made the representations set forth in paragraph 107, they have not detected significant performance, security problems, or viruses on consumers' computers and were not associated with legitimate companies, such as Microsoft.

109. Therefore, Defendants' acts or practices as set forth in paragraphs 106 through 108 constitute deceptive practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(a).

VIOLATIONS OF THE TELEMARKETING SALES RULE

110. In 1994, Congress directed the FTC to prescribe rules prohibiting abusive and deceptive telemarketing acts or practices pursuant to the Telemarketing Act, 15 U.S.C. §§ 6101–6108. The FTC adopted the original TSR in 1995, extensively amended it in 2003, and amended certain sections thereafter.

111. Tech Live Connect is a seller or telemarketer under the TSR. A "seller" means any person who, in connection with a telemarketing transaction, provides, offers to provide, or arranges for others to provide goods or services to the customer in exchange for consideration. 16 C.F.R. § 310.2(dd). A "telemarketer" means any person who, in connection with telemarketing, initiates or receives telephone calls to or from a customer or donor. 16 C.F.R. § 310.2(ff).

112. Nexway is a seller and/or merchant under the TSR. A "merchant" means a person who is authorized under a written contract with an acquirer to honor or accept credit cards or to transmit or process for payment credit card payments, for the purchase of goods or services. 16 C.F.R. § 3102(u).

113. Deutsche Bank, WorldPay and its agents Adyen and Ingenico, are acquirers under the TSR. An "acquirer" means a business organization, or an agent of one, that has authority from an organization that operates or licenses a credit card system to authorize merchants to accept,

transmit, or process payment by credit card through the credit card system for money, goods or services, or anything of value. 16 C.F.R. § 310.2(a).

114. A "credit card sales draft" means any record or evidence of a credit card transaction. 16 C.F.R. § 310.2(l).

115. It is a deceptive telemarketing act or practice and a violation of this Rule for a person to provide substantial assistance or support to any seller or telemarketer when that person knows or consciously avoids knowing that the seller or telemarketer is engaged in any act or practice that violates Sections 310.3(a), (c) or (d) or Section 310.4 of the TSR. 16 C.F.R. § 310.3(c).

116. It is a violation of the TSR for a seller or telemarketer to make a false or misleading statement to induce any person to pay for goods or services. 16 C.F.R.§ 310.3(a)(4).

117. Except as expressly permitted by the applicable credit card system, it is a deceptive telemarketing act or practice and a violation of the TSR for a merchant to present to or deposit into, or cause another to present to or deposit into, the credit card system for payment, a credit card sale draft generated by a telemarketing transaction that is not the result of a telemarketing credit card transaction between the cardholder and merchant. 16 C.F.R. § 310.3(c)(1).

118. Pursuant to Section 3(c) of the Telemarketing Act, 15 U.S.C. § 6102(c) and Section 18(d)(3) of the FTC Act, 15 U.S.C. § 57a(d)(3), a violation of the TSR constitutes an unfair or deceptive act or practice in or affecting commerce, in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

Count III
Assisting and Facilitating

119. In numerous instances, Defendants provided substantial assistance and support to one or more sellers or telemarketers, whom they knew, or consciously avoided knowing, were violating § 310.3(a)(4) of the TSR.

120. Therefore, Defendants' acts or practices as set forth in Paragraph 119 violate the TSR, 16 C.F.R. § 310.3(b).

Count IV
Credit Card Laundering

121. In numerous instances, Defendants presented to or deposited into, or caused another to present to or deposit into, the credit card system for payment, a credit card sales draft generated by a telemarketing transaction that is not the result of a telemarketing credit card transaction between the cardholder and the merchant.

122. Therefore, Defendants' acts or practices as set forth in Paragraph 121 violate the TSR, 16 C.F.R. § 310.3(c)(1).

Count V
Misrepresentations to Consumers
(Pled in the Alternative)

123. Defendants were Sellers who made or caused to be made false or misleading statements about the performance or security of a computer to induce a person to pay for technical support services.

124. Therefore, Defendants' acts or practices as set forth in Paragraph 123 violate the TSR, 16 C.F.R § 310.3(a)(4).

CONSUMER INJURY

125. Consumers have suffered tens of millions of dollars of injury, and will continue to suffer, substantial injury as a result of Defendants' violations of the FTC Act and the

Telemarketing Sales Rule. In addition, Defendants have been unjustly enriched as a result of their unlawful acts or practices. Absent injunctive relief by this Court, Defendants are likely to continue to injure consumers, reap unjust enrichment, and harm the public interest.

CIVIL PENALTIES

126. The Defendants' violations of the TSR were committed with the knowledge required by Section 5(m)(1)(A) of the FTC Act, 15 U.S.C. § 45(m)(1)(A).

127. Section 5(m)(1)(A) of the FTC Act, 15 U.S.C. § 45(m)(1)(A), as modified by Section 4 of the Federal Civil Penalties Inflation Adjustment Act of 1990, 28 U.S.C. § 2641, as amended, and as implemented by 16 C.F.R. §1.98(d), authorizes this Court to award monetary civil penalties of up to $46,517 for each violation of the TSR. See 16 C.F.R. §1.98(d); 87 Fed. Reg. 1070 (Jan. 10, 2022).

PRAYER FOR RELIEF

Wherefore, Plaintiff requests that the Court:

A. Enter a permanent injunction to prevent future violations of the FTC Act and the Telemarketing Sales Rule by Defendants;

B. Award civil penalties;

C. Award other monetary relief and other relief within the Court's power to grant; and\

D. Award any additional relief as the Court may determine to be just and proper.

Dated: April 3, 2023

Respectfully submitted,

Of Counsel:

RUSSELL DEITCH
J. RONALD BROOKE, JR.
Attorneys
Federal Trade Commission
Washington, DC 20580
Tel: 202-326-2585 (Deitch)
Tel: 202-326-3484 (Brooke)
rdeitch@ftc.gov
jbrooke@ftc.gov

FOR THE UNITED STATES OF AMERICA:

BRIAN M. BOYNTON
(D.C. Bar No. 483187)
Principal Deputy Assistant Attorney General
Civil Division

ARUN G. RAO
Deputy Assistant Attorney General

AMANDA N. LISKAMM
Director
Consumer Protection Branch

LISA K. HSIAO
(D.C. Bar No. 444890)
Assistant Director
Consumer Protection Branch

/s/ Claude F. Scott
CLAUDE F. SCOTT
(D.C. Bar No. 414906)
Senior Litigation Counsel
Consumer Protection Branch
U.S. Department of Justice
450 5th Street, N.W.
Washington, D.C. 20530
Tel: 202-514-9471
Fax: 202-514-8742
Claude.F.Scott@usdoj.gov