UNITED STATES DISTRICT COURT
DISTRICT OF COLUMBIA

FEDERAL TRADE COMMISSION
600 Pennsylvania, Ave., N.W.
Washington, DC 20580

Plaintiff,

v.

REVENUEWIRE, INC., also dba SafeCart, a corporation,
Suite 102, 3962 Borden St.
Victoria, BC
V8P 3H8, Canada;

and

ROBERTA LEACH, individually and as an officer of RevenueWire, Inc.,
4989 Georgia Park Terrace
Victoria BC
V8Y 2B8, Canada,

Defendants.

Case No. _____

COMPLAINT FOR PERMANENT INJUNCTION AND OTHER EQUITABLE RELIEF

Plaintiff, the Federal Trade Commission ("FTC"), for its Complaint alleges:

1. The FTC brings this action under Sections 13(b) and 19 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. §§ 53(b), 57b, and the Telemarketing and Consumer Fraud and Abuse Prevention Act, (the "Telemarketing Act"), 15 U.S.C. §§ 6101-6108, to obtain permanent injunctive relief, rescission or reformation of contracts, restitution, the refund of monies paid, disgorgement of ill-gotten monies and other equitable relief for Defendants' acts or

practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a) and the Telemarketing Sales Rule ("TSR"), 16 C.F.R. Part 310.

JURISDICTION AND VENUE

2. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331, 1337(a), and 1345, and 15 U.S.C. §§ 45(a), 53(b), 6102(c), and 6105(b).

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

OVERVIEW

4. Consumers throughout the country have been injured by tech support scams in which fraudsters deceptively market services to "fix" purported problems on consumers' computers. The FTC and state law enforcers have brought cases against the software sellers and call centers involved in these scams, including call centers operated by Vast Tech Support, LLC ("Vast") and Inbound Call Experts, LLC ("ICE"). *FTC v. Boost Software, Inc.*, No. 14-81397 (S.D. Fla. filed Nov. 10, 2014); *FTC v. Inbound Call Experts, LLC*, No. 14-81395 (S.D. Fla. filed Nov. 10, 2014). RevenueWire, Inc. and its Chief Executive Officer (collectively, "Defendants") have played a key role in many of these scams, including the Vast and ICE scams. Using a business model named "Call Stream," the Defendants have provided lead generation, business development, payment processing, and money distribution services to numerous tech support fraudsters, leading to hundreds of millions of dollars of consumer injury.

PLAINTIFF

5. The FTC is an independent agency of the United States Government created by statute. 15 U.S.C. §§ 41-58. 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 is also charged with enforcement of the Telemarketing Act, 15 U.S.C. §§ 6101-6108, as amended, under which the FTC promulgated and enforces the TSR, 16 C.F.R. Part 310, which prohibits deceptive or abusive telemarketing practices.

6. The FTC is authorized to initiate federal district court proceedings, by its own attorneys, to enjoin violations of the FTC Act and the TSR and to secure such equitable relief as may be appropriate in each case, including rescission or reformation of contracts, restitution, the refund of monies paid, and the disgorgement of ill-gotten monies. 15 U.S.C. §§ 53(b), 56(a)(2)(A), 6102(c) and 6105(b).

DEFENDANTS

7. Defendant RevenueWire, Inc., also doing business as "SafeCart" ("RevenueWire") is a Canadian corporation with its principal place of business at 26 Bastion Square, Third Floor – Burnes House, Victoria BC V8W1H9, Canada. RevenueWire is a closely-held company. RevenueWire entered into contracts with other companies, including call centers in the United States, to provide payment processing services. RevenueWire entered into contracts with banks and payment processors in the United States and abroad to open and maintain merchant accounts. RevenueWire transacts or has transacted business in this district and throughout the United States. RevenueWire is registered in the state of Nebraska as a foreign corporation with a Nebraska-based registered agent, and RevenueWire holds numerous federal trademark registrations.

8. Defendant Roberta Leach is the CEO of RevenueWire. Leach has executed documents on behalf of RevenueWire, including agreements with ICE and Vast and WorldPay. Leach

claims to have invented the "Call Stream" Business Model, and she is the senior officer of a small closely held company, and is responsible for its operations. At all times material to this Complaint, acting alone or in concert with others, Leach has formulated, directed, controlled, had the authority to control or participated in the acts or practices of RevenueWire, including the acts or practices set forth in the Complaint. Defendant Roberta Leach, in connection with the matter alleged herein, transacts business in this district and throughout the United States.

COMMERCE

9. 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

Overview of Tech Support Scams

10. Tech support scams, including scams involving ICE, Vast, and other clients of the Defendants, often involve an initial online hook in the form of a software company that markets a registry cleaner to improve computer performance. The software company typically offers consumers a "free scan" to check their computer's "health." After consumers obtain the results of the scan, a web page tells them they need to purchase the full software to fix the purported errors identified in the scan, and to call a phone number to activate the software.

11. Consumers who call the identified telephone numbers, reach tech support call centers in the U.S. and abroad. The telemarketers at these call centers then reel in consumers by activating the software and diving into a deceptive diagnostic followed by a deceptive sales pitch for costly computer repairs. The telemarketers make misrepresentations to consumers about "necessary"

repairs to their computers and often fail to run meaningful diagnostics to determine the cause of any purported problems. The telemarketers charge consumers hundreds of dollars for their purported tech support services.

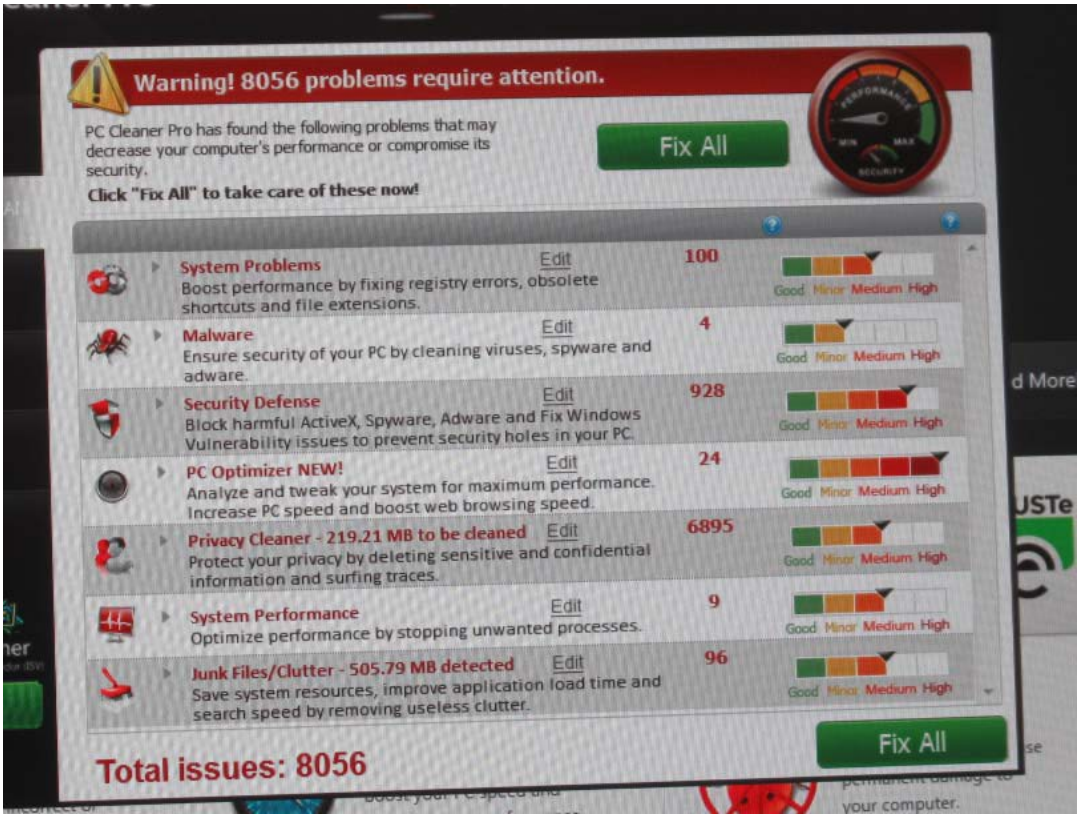
12. Tech support telemarketers often use the Event Viewer program to perpetuate their deception. Event Viewer is a pre-installed utility program on Windows computers. As part of its normal operation, it often lists innocuous system activity as "errors" and "warnings." For example, it may show an error or warning if there is a temporary loss of connection to the internet or if a keyboard is disconnected from the computer.

13. The telemarketers of tech support scams often use Event Viewer as a scare tactic to convince consumers to pay hundreds of dollars for computer repairs. Using a remote connection, the telemarketers run Event Viewer on the consumers' computers, often referring to the program as "Windows Log," rather than Event Viewer, and inform consumers that the program has found numerous errors and warnings, each of which is a "red flag" that needs to be repaired.

ICE and Vast Cases

14. In November 2014, the FTC and the State Attorney General of Florida brought two lawsuits alleging that two Florida-based tech support call centers, ICE and Vast, made false or misleading statements, directly or by implication, including misrepresenting that they had identified performance or security problems on consumers' computers. *FTC v. Inbound Call Experts, LLC*, No. 14-81395 (S.D. Fla. filed Nov. 10, 2014; Stipulated Order for Permanent Injunction and Monetary Judgment entered December 19, 2016) and *FTC v. Boost Software, Inc.*, No. 14-81397 (S.D. Fla. filed Nov. 10, 2014; Stipulated Order for Permanent Injunction and Monetary Judgment entered June 20, 2016).

15. The deception alleged in both ICE and Vast started with lead generators that advertised "free" registry scans on the internet. The free diagnostic scans purported to show numerous "problems," even on new, uninfected, properly operating computers. For example, the FTC ran a scan using one of the lead generator programs, PC Cleaner Pro, on a clean computer that did not have any viruses or performance issues. The PC Cleaner Pro scan showed 8056 errors, as shown in the screenshot below.

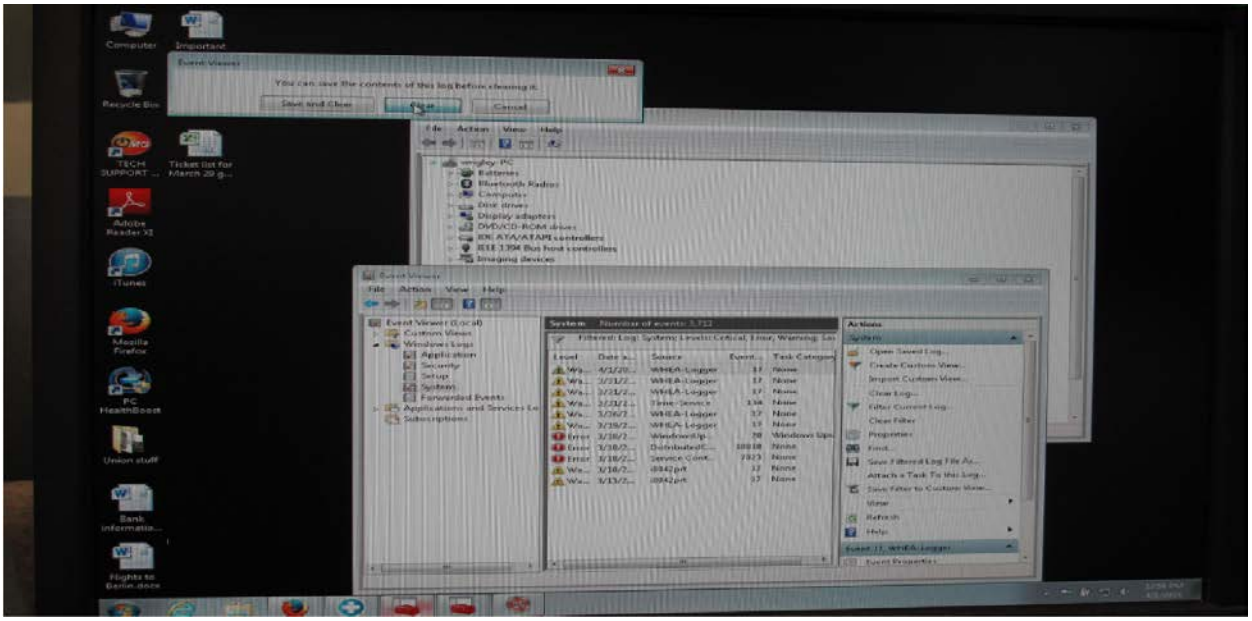


To fix the purported problems identified by the free scan, consumers were prompted to pay for registry cleaner software. Consumers who paid were then given toll-free phone numbers to "activate" their software.

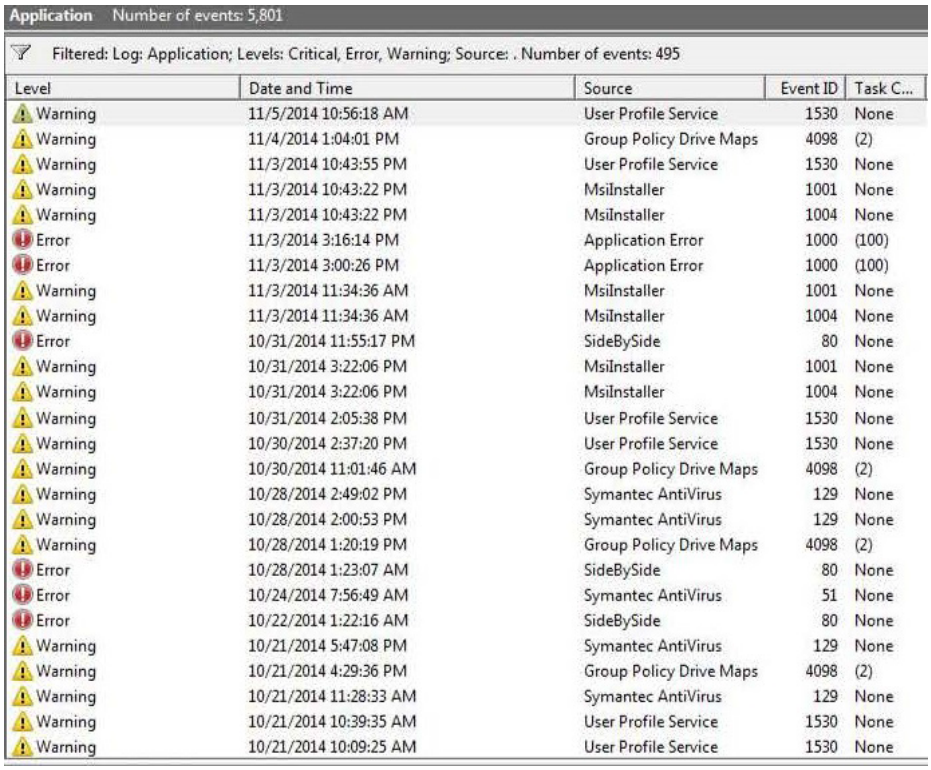
16. Consumers who called the toll-free numbers were connected to telemarketers from Vast and ICE, who, after gaining remote access to consumers' computers, subjected consumers to

further misrepresentations and scare tactics designed to convince consumers to purchase computer repair services. The misrepresentations included statements about "errors" and "warnings" on Event Viewer, the number of processes running, and the existence of "trace damage."

17. For example, a telemarketer at Vast pulled up the Event Viewer report displayed in the screenshot below in an attempt to convince an undercover FTC investigator to purchase unnecessary technical support services:



18. A telemarketer at ICE similarly used misstatements about the errors and warnings noted in Event Viewer in an attempt to sell unnecessary tech support services to an undercover FTC investigator, as shown in the following screenshot:



Application Number of events: 5,801

Filtered: Log: Application; Levels: Critical, Error, Warning; Source: . Number of events: 495

Level	Date and Time	Source	Event ID	Task C...
Warning	11/5/2014 10:56:18 AM	User Profile Service	1530	None
Warning	11/4/2014 1:04:01 PM	Group Policy Drive Maps	4098	(2)
Warning	11/3/2014 10:43:55 PM	User Profile Service	1530	None
Warning	11/3/2014 10:43:22 PM	MsiInstaller	1001	None
Warning	11/3/2014 10:43:22 PM	MsiInstaller	1004	None
Error	11/3/2014 3:16:14 PM	Application Error	1000	(100)
Error	11/3/2014 3:00:26 PM	Application Error	1000	(100)
Warning	11/3/2014 11:34:36 AM	MsiInstaller	1001	None
Warning	11/3/2014 11:34:36 AM	MsiInstaller	1004	None
Error	10/31/2014 11:55:17 PM	SideBySide	80	None
Warning	10/31/2014 3:22:06 PM	MsiInstaller	1001	None
Warning	10/31/2014 3:22:06 PM	MsiInstaller	1004	None
Warning	10/31/2014 2:05:38 PM	User Profile Service	1530	None
Warning	10/30/2014 2:37:20 PM	User Profile Service	1530	None
Warning	10/30/2014 11:01:46 AM	Group Policy Drive Maps	4098	(2)
Warning	10/28/2014 2:49:02 PM	Symantec AntiVirus	129	None
Warning	10/28/2014 2:00:53 PM	Symantec AntiVirus	129	None
Warning	10/28/2014 1:20:19 PM	Group Policy Drive Maps	4098	(2)
Error	10/28/2014 1:23:07 AM	SideBySide	80	None
Error	10/24/2014 7:56:49 AM	Symantec AntiVirus	51	None
Error	10/22/2014 1:22:16 AM	SideBySide	80	None
Warning	10/21/2014 5:47:08 PM	Symantec AntiVirus	129	None
Warning	10/21/2014 4:29:36 PM	Group Policy Drive Maps	4098	(2)
Warning	10/21/2014 11:28:33 AM	Symantec AntiVirus	129	None
Warning	10/21/2014 10:39:35 AM	User Profile Service	1530	None
Warning	10/21/2014 10:09:25 AM	User Profile Service	1530	None

Defendants' Role and Participation in Multiple Tech Support Scams

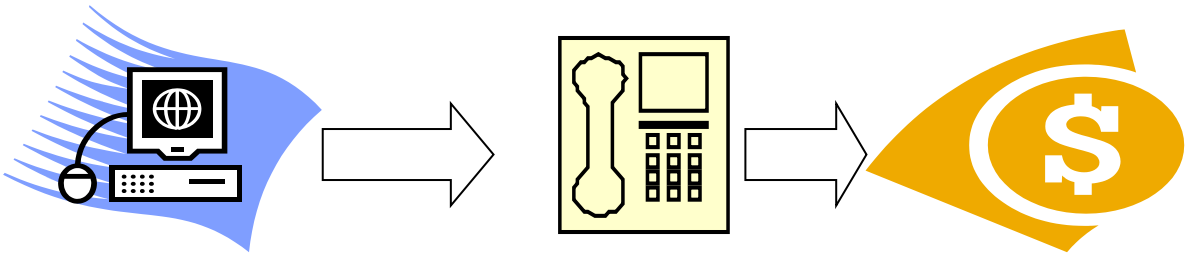
19. The Defendants assisted and benefited from numerous tech support scams, including those perpetrated by ICE and Vast by, among other things, providing payment processing services and consumer leads.

Defendants' Call Stream Business Model

20. Starting from at least 2011, Leach and RevenueWire operated a business model they called "Call Stream."

21. The Call Stream model involves three interrelated entities: (1) a software company (such as PC Cleaner Pro) that acts as a lead generator; (2) a call center whose telemarketers deceptively upsell consumers tech support services (e.g., ICE and Vast); and (3) a company (RevenueWire) that uses its credit card merchant account to submit consumers' payments for processing and

divides the ill-gotten funds among itself, the call center and the software seller. The following is a visual depiction of the Call Stream business model:



Consumer Purchases Downloadable Software & is Directed to Call Center for Activation

Call Center Deceptively Pitches Upsells or Tech Support Services

RevenueWire Uses Its Merchant Account to Process Charges and Transfers Funds to the Software Company and Call Center

22. As the central hub of the Call Stream model, RevenueWire: (1) contracts with the software sellers to funnel consumers to Defendants' tech support call center partners; (2) oversees the distribution of calls to the tech support call centers; (3) uses merchant accounts in its name to process the charges of the third-party tech support call centers; (4) receives and handles consumers' refund and chargeback requests related to the tech support call center charges; (5) handles tech support call centers' recurring charges to consumers who have been billed on an annual basis; and (6) divides the proceeds between itself, the tech support call centers and the software companies.

Defendants' Partnership with ICE

23. RevenueWire and ICE entered into a contract on December 14, 2011 under which RevenueWire would provide ICE with payment processing service.

24. On or about January, 2012, RevenueWire began providing processing services to ICE, charging a processing fee of 6.9% plus $1 on every ICE sales transaction.

Defendants' Partnership with Vast and Other Call Centers

25. On June 15, 2012, RevenueWire entered into a contract with call center Vast to provide payment processing and other services.

26. Around the same time, RevenueWire brokered deals with third-party software companies, including PC Cleaner, Inc. and Boost Software, Inc. These companies agreed to direct purchasers of their registry cleaner and "PC optimizer" software to RevenueWire's call center partners, including Vast and ICE, to "activate" the software and be pitched tech support services by telemarketers.

27. In addition to ICE and Vast, RevenueWire entered into payment processing and lead generation contracts with other tech support call centers that subsequently were subject to law enforcement actions for deceptive marketing practices, including ASAP Tech Help, LLC ("ASAP"), Fast Fix 123, LLC ("Fast Fix"), and iYogi, Inc. ("iYogi"). *See State of Florida v. ASAP Tech Help*, LLC, No. L14-3-1102 (Fla. Cir. Ct. filed Mar. 5, 2015); *State of Florida v. Fast Fix 123, LLC*, No. 52642779 (Fla Cir. Ct. filed Feb. 17, 2017); and *State of Washington v. iYogi, Inc.*, No. 15-2-3047-1 (Wash. Super. Ct. filed Dec. 15, 2015; Summary Judgment granted against iYogi on April 6, 2018).

28. Furthermore, in or about April 2014, RevenueWire added bogus warning "pop-ups" (i.e., pop-up dialog boxes on computer screens) to Call Stream. The pop-ups windows—referred to generically as 844Desktop—did not sell software, but instead deceptively claimed to have detected computer infections, froze consumers' computer screens, and directed consumers to call toll free numbers to fix the supposed problems. The toll free phone numbers would connect the consumer with RevenueWire Call Stream partner tech support call centers including Vast,

ASAP, and Fast Fix, as well as offshore call centers in India, such as Technicion. The RevenueWire Call Stream tech support call centers that received such calls would address the pop-up as a legitimate warning and attempt to sell the consumers their tech support packages. RevenueWire processed sales made to consumers duped by the pop-up through its merchant account. RevenueWire's pop-up campaigns generated thousands of calls a day for their Call Stream partner call centers.

Defendants' Interest in Helping Call Centers Generate High Sales Volume

29. RevenueWire's payment processing services involved two credit card sales drafts. One generated by the transaction between the software companies and consumers when the consumers pay for the software online, and a second generated by the telemarketing transaction between the Call Stream partner call centers and consumers for purported tech support services.

30. With either type of transaction, the name "SafeCart," a dba for RevenueWire, would appear on consumers' card statements. For the Call Stream partner call center transactions (telemarketing upsells), RevenueWire would: (1) cause an acquirer (a bank, payment processor, or financial institution that processes credit or debit card payments on behalf of merchants and enables them to accept card payments) to deposit credit card sales drafts into the credit card system; (2) collect payments through the Visa and MasterCard systems via a payment processor; (3) collect its fee (6.95% plus $1 on every transaction); (4) transmit 25% to 40% of existing funds to the software company that provided the telemarketing lead; and (5) transmit the remaining funds to the Call Stream partner call centers, such as ICE and Vast.

31. RevenueWire and Leach had a financial interest in keeping the sales volume of the call centers high because they earned processing fees and shares of revenue based upon sales volume.

For example, in November 2013, ICE was closed on Thanksgiving. RevenueWire contacted Vast and had calls temporarily routed to Vast instead of ICE.

RevenueWire Impermissibly and Deceptively Caused Consumer Credit Card Payments Generated by Call Center Sales to be Submitted Into the Credit Card Networks

32. In or around June 2009, RevenueWire entered into a merchant account agreement with payment processor and merchant acquiring business Chase Paymentech and JP Morgan Chase Bank ("Chase") for payment processing services for eBooks and software. Under the contract, RevenueWire was the merchant of record – i.e., the seller of the products and services for which Chase would process consumer payments. The contract prohibited RevenueWire from submitting payments generated by third-party sellers to Chase.

33. Despite the prohibition in its agreement with Chase, RevenueWire submitted to Chase for processing consumer payments totaling millions of dollars that were generated by the sales of third party call centers, including ICE and Vast. By doing so, RevenueWire caused Chase to present or deposit into the credit card system, for payment, numerous telemarketing credit card sales drafts that were not the result of transactions between the cardholders (consumers) and the merchant of record (RevenueWire).

34. Moreover, by 2012, Leach and RevenueWire knew that they were improperly presenting to or depositing credit card sales drafts into the credit card systems, or were causing another person to present to or deposit credit card sales drafts into the credit card system that were the result of transactions between call centers and consumers.

35. RevenueWire attempted to hide from Chase the fact that it was submitting to Chase payments generated by call centers by coding these sales as software store sales. For example, RevenueWire submitted to Chase numerous call center charges under Visa code 5734 ("Software

stores"), instead of the applicable 5967 Visa code ("Teleservices Merchants"). RevenueWire never told Chase that it was submitting payments from call centers, such as ICE and Vast. On May 9, 2012, RevenueWire's Vice President of Finance , sent an email to Roberta Leach, titled "Definition of Inbound Teleservices merchants (MCC 5967)," which stated:

> Under Visa Excessive CB monitoring program, merchants with the following service (MCC code 5967) is [sic] considered to be in the High-Risk CB Monitoring Program. It means no warning period and fees may be assessed if there are more than 100 CB per month. The risk for us is that Chase hasn't figured out that we provide these services, which they [sic] will need to put us under a separate MCC code as opposed to MCC 5734 (Software stores) we are under.

36. RevenueWire entered into a merchant account agreement with payment processor WorldPay in or around June 2007, and into a second agreement with WorldPay in or around June 2015. The contracts allowed RevenueWire to submit to WorldPay, for processing, credit card payments generated by sales of RevenueWire's goods or services. Under both contracts, RevenueWire was the merchant of record and was prohibited from submitting to WorldPay payments generated by sales of third parties.

37. Despite the prohibition in its agreements with WorldPay, RevenueWire submitted to WorldPay, for processing, numerous consumer payments totaling millions of dollars that were generated by the sales of third party call centers, including ICE and Vast. By doing so, RevenueWire caused WorldPay to present or deposit into the credit card system, for payment, numerous telemarketing credit card sales drafts that were not the result of transactions between the cardholders (consumers) and the merchant of record (RevenueWire).

38. RevenueWire hid from WorldPay that it was submitting renewal or rebill charges to consumers' credit cards on behalf of ICE that involved tech support services. For example, on

April 13, 2016, Roberta Leach received an email asking whether "we could move ICE's new sales and renewal charges to one provider (like WorldPay) and then close down PayPal…" Roberta Leach responded as follows:

> The reason we didn't put ATS (the dba for ICE) on the WorldPay gateway is because we were very concerned about having a high volume call center on WorldPay that is being investigated by the FTC. **As you know, we're only suppose [sic] to be selling software on the WorldPay account. WorldPay doesn't know that the old [ICE] rebills we migrated from Chase to WorldPay are for tech support – it's a low enough price point that rebills look like software.** If we move everything from PayPal to WorldPay we'll have two issues. First, as mentioned above, we're not supposed to be processing payment for premium tech support centers and this may jeopardize our account with WorldPay….Second, **if we move everything off PayPal, we'll send the PayPal account into severe chargeback state which will get reported to Visa**. This may have a number of repercussions including losing our Visa merchant account. (Emphasis added).

Defendants Knew or Consciously Avoided Knowing about the Deceptive Practices That Call Stream Call Centers, Including Vast and ICE, Used to Generate Sales

39. Since in or around January 2012, RevenueWire and Leach knew or consciously avoided knowing that the Call Stream partner call centers, including ICE and Vast, made false or misleading statements to induce consumers to pay for their purported tech support services.

40. RevenueWire and Leach received warning signs that ICE and Vast were engaged in deceptive practices from, among other things: (1) complaints from business partners; (2) RevenueWire's undercover shops of ICE and Vast; (3) complaints from consumers that ICE was billing them without their authorization or did not have the technical capability to perform the services it purported to offer; and (4) RevenueWire's fraud analyst's description of Vast's owners and managers as "a bunch of crooks." Yet, RevenueWire continued to process payments and provide leads to ICE, Vast and other Call Stream partner call centers.

41. Since on or about January 1, 2012, RevenueWire presented to or caused another to present to or deposit into the credit card system credit card sales drafts between consumers and entities, including ICE or Vast. Since that time, RevenueWire has earned millions from processing fees that it charged ICE and Vast.

Timeline of Events Demonstrating Defendants' Knowledge of Call Center Deception

2012

42. By October 2012, the FTC had brought cases against Pecon Software and others for engaging in tech support scams similar to ICE and Vast. *See FTC v. Pecon Software Ltd*, No. 12-7186 (S.D.N.Y. filed Sept. 24, 2012); *FTC v. PCCare 247 Inc.*, No. 12-7189 (S.D.N.Y. filed Sept. 24, 2012); *FTC v. Michael Marczak*, No. 12-7192 (filed S.D.N.Y. Sept. 24, 2012); *FTC v. Finmaestros, LLC*, No. 12-7186 (S.D.N.Y. filed Sept. 24, 2012); and *FTC v. Lakshmi Infosoul Services Pvt. Ltd.*, No. 12-7191 (S.D.N.Y. filed Sept. 24, 2012). On October 3, 2012, Leach shared a copy of a media report about the cases with officers of ICE, in an email with the subject line: "Phone tech support calls scammed tens of thousands in six countries".

43. In October 2012, via an email from a representative of Boost, Leach learned about a television news story where an ICE customer complained that she was charged for tech support services she never agreed to buy.

44. On November 9, 2012, Leach and RevenueWire managers received an email from RevenueWire's fraud analyst, that noted the improper use of Event Viewer by tech support telemarketers and why it was deceptive. Relating his experiences during a test purchase involving an unidentified call center partner, the fraud analyst noted:

> I told him [the telemarketer], from the off, that my computer was not running slowly, but he seemed to ignore me quite a bit, every time saying it needed a tune-up, regular repairs etc. He then did what I knew he'd do, **and ran the Windows**

> **Event Viewer (again without asking permission), which MAKES it look like there are hundreds of issues on your computer (he 'found' over 2,000), but is actually an app in Windows which merely records events that occur (google "windows event viewer scam" to see what I mean). It is not a tool that shows 'critical errors' of the type he was purporting it was.** At this point, I powered down the PC and hung up. I really didn't want him to do anything else on the computer. (Emphasis added.)

45. The Vice President of Finance at RevenueWire wrote in an email on December 21, 2012, that he told Leach that "we never screened Vastech" (Vast). He further stated that Vast "came on" before they had RevenueWire's fraud analyst screening potential merchant applications.

2013

46. One month later, in January 2013, the fraud analyst at RevenueWire warned RevenueWire's Vice President of Finance against having Vast as a client. On January 8, 2013, the Vice President of Finance at RevenueWire forwarded a series of emails from the fraud analyst to Leach. Among other things, the analyst wrote:

> we're dealing with a bunch of crooks here…and we are intrinsically associated with anything they do… I don't particularly fancy RW [RevenueWire] being caught up in a money laundering/RICO investigation because of these clowns, but if things continue on as they are, it's eminently possible that we will be.

The fraud analyst also highlighted that Vast 's owner and officer, Loewenstern, was involved in a criminal enterprise called Biltmore Securities, which was an "organization that is so debaucherous [sic] it's being made into a film where families were robbed of their savings by …Lowenstern's [sic] boilerrooms."

47. RevenueWire made undercover calls to ICE and Vast in 2013. During these calls, ICE and Vast telemarketers made misrepresentations like those described above. For example:

- In a report about an August, 2013 undercover call to ICE, the RevenueWire representative noted that the ICE telemarketer used the "Event manager" during the

diagnostic and informed him that there were "many things wrong with my computer and I need to get them fixed."

- In a September 2013 test call to Vast, the Vast telemarketer deceptively used Event Viewer.

Even after reviewing these undercover calls, RevenueWire continued to provide payment processing and lead generation services to ICE and Vast.

2014

48. A RevenueWire manager received an email in January 2014 from Bob Bryant with the software company Slimware, a Call Stream software seller that directed activation calls to ICE via RevenueWire, warning RevenueWire that ICE was making misrepresentations about Event Viewer. Later that month, during a business dinner in Las Vegas, Slimware managers discussed ICE's deceptive use of the Event Viewer with RevenueWire employees, including Leach.

49. RevenueWire's fraud analyst, wrote the following in an August 25, 2014 email forwarded to Leach by the Vice President of Finance at RevenueWire:

> I think the fact is is [sic] this type of …remote tech support which (as much as we may not like to admit it) preys on largely on the end-user's lack of technical knowledge and social engineering tactics is absolutely bound to attract the type of deceptive advertising that we desperately want to avoid. This is not helped in the slightest by the tech support companies themselves and their own deceptive techniques, which I've experienced before in test calls.

50. RevenueWire used its merchant account to process payments for Vast from June 15, 2012 until at least November 24, 2014, when the FTC sued Vast and the Court placed the company in receivership. Even after the FTC filed cases against Vast and ICE, RevenueWire continued to use its merchant account to process payments for other Call Stream partner call centers,

including ASAP and Fast Fix, that used similar deceptive sales tactics.

51. Based on the facts and violations of law alleged in this Complaint, the FTC has reason to believe that Defendants are violating or are about to violate laws enforced by the Commission because, among other things: Defendants remain in the payment processing business, continue to market and provide processing services to third-party merchants, including through their website RevenueWire.com, and maintain the means, ability, and incentive to resume their unlawful conduct; Defendants engaged in their unlawful acts or practices over a number of years; Defendants knowingly engaged in their unlawful acts or practices; and Defendants continued their unlawful acts or practices despite knowledge of unlawful activity

VIOLATIONS OF THE FTC ACT

52. Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), prohibits "unfair or deceptive acts or practices in or affection commerce."

53. 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 conterveiling benefits to consumers or competition. 15 U.S.C. § 45(n).

COUNT I

SECTION 5 UNFAIRNESS COUNT

54. In numerous instances, Defendants have submitted charges through RevenueWire's merchant account for companies that made false statements to consumers.

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

56. Therefore, Defendants' acts or practices as set forth in paragraph 54 constitute unfair acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(a), (n).

VIOLATIONS OF THE TELEMARKETING SALES RULE

57. 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, in 1994. The FTC adopted the original TSR in 1995, extensively amended it in 2003, and amended certain sections thereafter.

58. Vast and ICE are sellers or telemarketers 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).

59. RevenueWire is a 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).

60. Chase Paymentech is an acquirer 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).

61. 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 this Rule. 16 C.F.R. § 310.3(c).

62. The TSR's prohibition against making false or misleading statements applies to all statements regarding upsells, whether the statements were made during an outbound call initiated by the telemarketer or an inbound call initiated by the consumer. 16 C.F.R. § 310.6.

63. Except as expressly permitted by the applicable credit card system, it is a deceptive telemarketing act or practice and a violation of this rule 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). 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 II

CREDIT CARD LAUNDERING UNDER THE TSR

64. In numerous instances, RevenueWire and Leach 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.

65. RevenueWire's and Leach's acts or practices, as described in Paragraph 64 above, constitute violations of the TSR, 16 C.F.R. § 310.3(c)(1).

COUNT III

ASSISTING AND FACILITATING

66. Defendants RevenueWire and Leach 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.

67. Defendants RevenueWire'sand Leach's acts or practices, as described in Paragraph 66 above, violate the TSR, 16 C.F.R. § 310.3(b).

CONSUMER INJURY

68. Consumers have suffered and will continue to suffer substantial injury as a result of Defendants' violations of the FTC Act and the TSR. Defendants' violations of the law have caused millions in unreimbursed consumer injury. 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.

THIS COURT'S POWER TO GRANT RELIEF

69. Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), empowers this Court to grant injunctive and such other relief as the Court may deem appropriate to halt and redress violations of any provision of law enforced by the FTC. The Court, in the exercise of its equitable jurisdiction, may award ancillary relief, including rescission or reformation of contracts, restitution, the

refund of monies paid, and the disgorgement of ill-gotten monies, to prevent and remedy any violation of any provision of law enforced by the FTC.

70. Section 19 of the FTC Act, 15 U.S.C. § 57b and Section 6(b) of the Telemarketing Act, 15 U.S.C. § 6105(b) authorize this Court to grant such relief as the Court finds necessary to redress injury to consumers resulting from Defendants' violations of the TSR, including the rescission or reformation of contracts and the refund of money.

PRAYER FOR RELIEF

Wherefore, Plaintiff FTC, pursuant to Section 13(b) and 19 of the FTC Act, 15 U.S.C. §§ 53(b), 57b, the TSR, and the Court's own equitable powers, requests that the Court:

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

B. Award such relief as the Court finds necessary to redress injury to consumers resulting from Defendants' violations of the FTC Act and the TSR, including but not limited to, rescission or reformation of contracts, restitution, the refund of monies paid, and the disgorgement of ill-gotten monies; and

C. Award Plaintiff the costs of bringing this action, as well as such other and additional relief as the Court may determine to be just and proper.

Respectfully submitted,

ALDEN F. ABBOTT
GENERAL COUNSEL

Dated: April 21, 2020

s/Russell Deitch
Russell Deitch
J. Ronald Brooke, Jr.
Federal Trade Commission
600 Pennsylvania Ave., N.W.
Washington D.C. 20580
(202) 326-2585 rdeitch@ftc.gov
(202) 326-3484 jbrooke@ftc.gov

Attorneys for Plaintiff
FEDERAL TRADE COMMISSION