Russell Deitch (CA Bar No. 138713)
Sung W. Kim (DC Bar No. 1048330)
Federal Trade Commission
600 Pennsylvania Ave., NW
Washington, DC 20580
(202) 326-2585 / rdeitch@ftc.gov
(202) 326-2211 / skim6@ftc.gov
(202) 326-3395 (fax)

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT
DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. Nuvei Corporation, a Canada corporation; Nuvei International Group Limited, formerly known as SafeCharge International Group Limited, a private Guernsey company; Nuvei Limited, formerly known as SafeCharge Limited, a private Cyprus company; SafeCharge Digital Limited, a private Cyprus company; and Nuvei Technologies Inc., a Delaware corporation. Defendants.	No. CV- **COMPLAINT FOR PERMANENT INJUNCTION, MONETARY JUDGMENT, AND OTHER RELIEF**

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

1. Plaintiff brings this action for Defendants' violations of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), and the FTC's Telemarketing Sales Rule ("TSR"), 16 C.F.R. Part 310. For these violations, the FTC seeks relief, including a permanent injunction, monetary relief, and other relief, pursuant to Sections 13(b) and 19 of the FTC Act, 15 U.S.C. § 53(b) and 57(b), and the TSR, 16 C.F.R. Part 310.

SUMMARY OF CASE

2. Defendants operate a global payment processing business that enables merchants to accept debit and credit card payments from consumers.

3. Since at least 2011, Defendants have assisted and facilitated a tech support scheme operating under the name Reimage, among others, that substantially harmed consumers through its deceptive online marketing and telemarketing.

4. Defendants opened numerous merchant accounts for Reimage and spread Reimage's transactions, including chargebacks initiated by deceived consumers, among those accounts. By doing so, Defendants helped Reimage mask its excessive chargeback rates from the card networks' fraud monitoring programs.

5. In early 2020, Defendants received a warning from Visa that Reimage was impersonating Microsoft with fake virus alerts and luring consumers to offshore call centers under the guise of offering remote tech support services. Despite the fraud warning, which was accompanied by a fine, Defendants ramped up its payment processing for Reimage and its call centers and began processing recurring charges on Reimage's tech support services and software.

6. Defendants also submitted merchant applications for Reimage containing false information. By opening and maintaining merchant accounts for Reimage using nominee directors, fake business locations in Europe, and a misleading description of Reimage's business, Defendants helped Reimage conceal its offshore telemarketing activities from the card networks and circumvent the card network rules and transaction monitoring designed to prevent fraud.

7. Defendants also processed payments for Reimage by opening and using merchant accounts under the names of so-called "Merchant of Record" processors ("MoRs") to process Reimage charges. In reality, those MoRs were not the actual merchants—Reimage was—as the MoRs did not sell Reimage's goods or services to consumers.

8. Between 2017 and 2023, Defendants' illegal payment processing practices have allowed Reimage to unlawfully obtain over $30 million from consumers. Defendants' processing for Reimage ended only when Reimage stopped submitting charges to Defendants after Reimage learned of the FTC's investigation into its marketing practices.

9. In addition to Reimage, Defendants have also opened and maintained merchant accounts for other deceptive tech support merchants and for merchants deceptively selling business opportunities with false or baseless earnings claims, merchants impersonating government tax authorities, and merchants that were previously terminated for cause by other payment processors or acquiring banks.

JURISDICTION AND VENUE

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

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

PLAINTIFF

12. The FTC is an agency of the United States Government created by the FTC Act, which authorizes the FTC to commence this district court civil action by its own attorneys. 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 also enforces the Telemarketing and Consumer Fraud and Abuse Prevention Act ("Telemarketing Act"), 15 U.S.C. §§ 6101-6108. Pursuant to the Telemarketing Act, the FTC promulgated and enforces the TSR, 16 C.F.R. Part 310, which prohibits deceptive and abusive telemarketing acts or practices.

DEFENDANTS

13. Defendant **Nuvei Corporation ("Nuvei Canada")** is a private company incorporated in Canada on or about November 28, 2024 (Canada Corp. No. 1655609-4). Nuvei Canada's registered business address is 1100 Rene-Levesque Blvd. West, Suite

900, Montreal, Canada. Nuvei Canada is the legal successor to various corporate entities under which Defendants previously conducted business, including 10390461 Canada Inc. a/k/a Pivotal Development Corporation Inc. (Corp. No. 1039046-1), Nuvei Technologies Corp. (Canada Corp. No. 1059017-7), Pivotal Payments Corporation (Canada Corp. No. 1034052-9), and Pivotal Payments Direct Corp. (Canada Corp. No. 430561-1). Through a series of amalgamations with its various Canadian subsidiaries in recent years, Nuvei Canada has assumed the rights, assets and liabilities of the aforementioned entities. Since 2019, Nuvei Canada and its predecessors have registered six different trademarks with the United States Patent and Trademark Office (USPTO) for the provision of payment processing services in the United States. In 2019, Defendants registered a shell company in Canada—11411802 Canada Inc.—to facilitate Nuvei's acquisition of the SafeCharge family of companies. 11411802 Canada Inc. is a wholly-owned subsidiary of Nuvei Canada and the corporate parent of Nuvei Limited, Nuvei International Group Limited, and SafeCharge Digital Limited. At all times material to this Complaint, Nuvei Canada has processed credit card and other electronic transactions with consumers in the United States for tech support and other services. Nuvei Canada transacts or has transacted business in this District and throughout the United States.

14. Defendant **Nuvei International Group Limited ("Nuvei Guernsey")** is a private company incorporated in the British Virgin Islands in 2006 and re-domiciled in the British Crown dependency of Guernsey in 2015. Until 2021, Nuvei Guernsey conducted business under its former name, SafeCharge International Group Limited, and promoted itself as a "global provider of payment services, technologies and risk management solutions for online and mobile businesses." Nuvei Guernsey was co-founded by the former majority owner of Crossrider Israel Ltd. (now known as Kape Technologies PLC), which took ownership of and control over Reimage's tech support operations in or around 2014. Nuvei Guernsey was acquired by Nuvei Canada as part of Nuvei's acquisition of the SafeCharge group of entities in or around August 2019. Nuvei Guernsey is an indirect subsidiary of Nuvei Canada and is the parent company of various

Nuvei corporate entities, including Defendant Nuvei Limited and Defendant SafeCharge Digital Limited. Through its corporate parent, subsidiaries and affiliates, Nuvei Guernsey transacts or has transacted business in this District and throughout the United States.

15. Defendant **Nuvei Limited** is a private company registered in Cyprus in or around 2002. Until 2021, Nuvei Limited conducted business under its former name SafeCharge Limited. Since at least 2014, Nuvei Limited has also been registered with the Central Bank of Cyprus as an electronic money transmitter in Europe, and as a principal member of Visa and Mastercard, meaning it is licensed to issue and acquire payments under its own brand. As principal member, Nuvei Limited may acquire merchants directly and open merchant accounts through its bank identification number. Nuvei Limited is also registered with Visa as a "high integrity risk" payment facilitator. In these roles and through these relationships, Nuvei Limited provides payment processing services to merchants targeting consumers in the United States and elsewhere. While Nuvei Limited has a registered business address in Nicosia, Cyprus, the company's officers and employees work or reside in the Republic of Bulgaria, Canada or the State of Israel. Nuvei Limited, through its subsidiary SafeCharge USA Inc., has also executed contracts with acquiring banks in the United States and solicited merchants located in the United States to offer Defendants' payment processing services. At all times material to this Complaint, Nuvei Limited has processed credit card and other electronic transactions with consumers in the United States for tech support and other services. Nuvei Limited transacts or has transacted business in this District and throughout the United States.

16. Defendant **SafeCharge Digital Limited ("SC Digital")** is a private company registered in Cyprus in or around 2007. Since at least 2007, SC Digital (formerly known as "GTS Online" and "Gate2Shop") has operated as a "merchant of record" service provider for tech support providers and other merchants targeting consumers in the United States and elsewhere. As a merchant of record, SC Digital has applied for and obtained merchant accounts in its own name and used these accounts to process payments for unaffiliated, third-party sellers and telemarketers. SC Digital is an

indirect subsidiary of Nuvei Limited and has the same executives, employees and business address as Nuvei Limited. At all times material to this Complaint, SC Digital has processed credit card and other electronic transactions with consumers in the United States for tech support and other services. SC Digital transacts or has transacted business in this District and throughout the United States.

17. Defendant **Nuvei Technologies Inc. ("Nuvei Tech")** is a private company incorporated in Delaware in or around 2003. Nuvei Tech is located at 1375 N Scottsdale Road, Suite 400, Scottsdale, Arizona. Nuvei Tech previously conducted business under the name Pivotal Payments until October 2018, after which it rebranded the company name to Nuvei. In or around January 2021, Defendants acquired Base Commerce LLC, a payment processor based in Arizona, and formed the Delaware company, Nuvei Commerce LLC, to succeed Base Commerce LLC and take over its operations. As illustrated in the corporate hierarchy diagram below, Nuvei Tech is an indirect subsidiary of Nuvei Canada and the corporate parent of Nuvei Commerce LLC. At all times material to this Complaint, Nuvei Tech has processed credit card and other electronic transactions with consumers in the United States for tech support and other services. Nuvei Tech transacts or has transacted business in this District and throughout the United States.

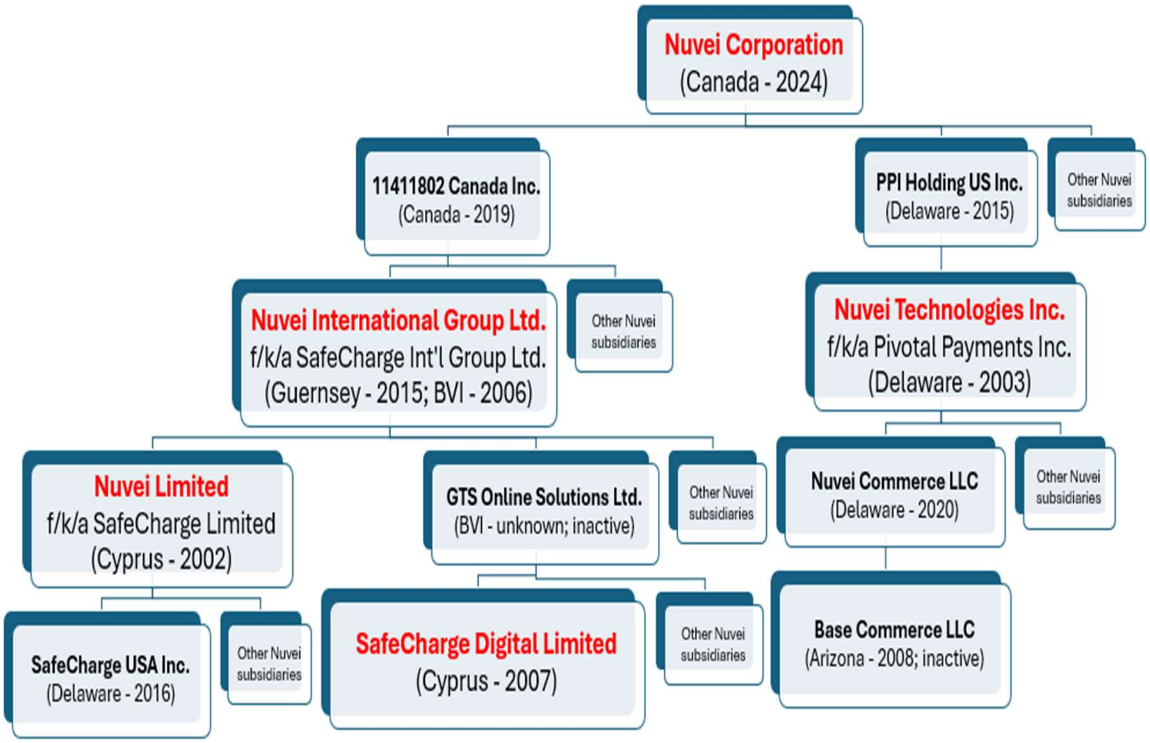

Figure 1: Nuvei corporate hierarchy diagram (named Defendants in red)

COMMON ENTERPRISE

18. Defendants have operated as a common enterprise while engaging in the unlawful acts and practices alleged in the Complaint. Defendants have conducted the business practices described herein through the interrelated Nuvei corporate entities, which have a common business purpose, business functions, and overlapping employees and officers, have commingled funds, and are all controlled by corporate officers of Nuvei Canada and others acting at their behest. Defendants utilize the same website, nuvei.com, to promote their services. Nuvei Limited has entered into partnership agreements with third parties located in the United States, such as PayPal Holdings, Inc, on behalf of itself and other Defendants, for the provision of payment processing services

in the United States and elsewhere. Because the Defendants have operated as a common enterprise, each of them is liable for the acts and practices alleged herein.

COMMERCE

19. 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.

THE CREDIT CARD SYSTEM AND MERCHANT ACCOUNTS

The Acquirer, Payment Facilitator and "Merchant of Record"

20. A merchant account allows merchants to process consumer payments by a credit or debit card. Merchant accounts are available through financial institutions referred to as acquiring banks or "acquirers" that are members of the card networks, such as Visa or Mastercard. Without access to a merchant account through an acquirer, merchants cannot accept consumer credit or debit card payments.

21. Some entities act as intermediaries between merchants and acquirers. They include independent sales organizations, sales agents, and payment facilitators. The card networks require these payment intermediaries to register with the networks and obtain sponsorship from an acquirer to provide payment processing services to third-party merchants.

22. Unlike other payment intermediaries, a payment facilitator ("payfac") often does not procure a separate merchant account for each of its merchant clients. Instead, the payfac stands in as a "master merchant," registered by an acquirer to facilitate transactions on behalf of the payfac's merchant clients (commonly referred to as "submerchants"). The payfac typically receives settlement of consumer transaction proceeds from the acquirer on behalf of each submerchant and disburses the funds to each submerchant.

23. The payfac contracts with acquirers to provide payment services to submerchants, and it enters into a separate agreement with each submerchant to enable payment acceptance. When a cardholder makes a purchase from a submerchant, the

transaction typically is processed through the payfac's master merchant account. The payfac solicits merchants in need of credit and debit card processing services and charges commissions or fees based on the volume of sales processed for each submerchant. The payfac typically charges its submerchants different rates depending on, among other factors, the level of risk associated with the submerchant or its business.

24. Over the past decade, some payment intermediaries have begun providing payment processing services to third-party merchants through the MoR model. Under this model, the payment intermediary (i.e., MoR) stands in as the submerchant or "reseller" of the product or service for purposes of procuring a merchant account from either an acquirer or a payfac and collecting card payments from the cardholder. As with other payment intermediaries, the MoR remits the funds back to the actual merchant or seller of the product. In this instance, the MoR is functionally equivalent to a payfac but is not registered with the card networks to operate as a payfac.

25. Since at least 2016, the card network rules have provided that a payfac "may not be a Submerchant of any other Payment Facilitator, nor may a Payment Facilitator be a Payment Facilitator for another Payment Facilitator." *MasterCard Rules*, Chapter 7.6.5, Payment Facilitators and Submerchants (published July 7, 2016); *see also* Visa Core Rules, Part 5.3.2.2 (published October 15, 2016).

26. At all times materials to the Complaint, Defendants have offered payment processing services to merchants under the various payment acceptance models described above, including: (a) as an acquirer directly issuing merchant accounts to its merchant clients; (b) as a registered payfac opening submerchant accounts for its merchant clients through its relationship with acquirers; and (c) as an MoR enabling its merchant clients to access merchant accounts through the MoR's contracts with other payfacs.

27. To deter fraud, increase transparency, and reduce risk to consumers, businesses, and the payment system, the card networks impose rules and restrictions on acquirers, payfacs, and other entities in the card payment ecosystem. These rules require

acquirers, payfacs and other payment intermediaries to monitor their merchant clients' sales transaction activity for indicators of unlawful or deceptive conduct.

28. The card networks rules require acquirers and payment intermediaries to conduct due diligence prior to onboarding a merchant to ensure that the merchant is engaged in a legitimate business and to screen out merchants engaged in deceptive or other illegal activity. Such due diligence includes ascertaining, among other things: the identity of the merchant and its principals; the location of the merchant's business; the products or services the merchant sells; how the merchant's products or services are sold and provided (e.g., telemarketing, online, retail store); the merchant's marketing practices; and the merchant's transaction volume.

29. The card networks' rules prohibit acquirers, payfacs and other payment intermediaries from misrepresenting the location of a merchant, which is required to be in the same geographic jurisdiction (or area of use) as the acquirer.

30. The card networks also prohibit acquirers from allowing merchants to use merchant accounts that were previously underwritten and approved by the card networks or the acquirer for a particular line of business to process transactions for a different, unauthorized service or product.

Card Networks' Chargeback and Other Fraud Monitoring Programs

31. One of the primary indicators of fraudulent or deceptive conduct is a high chargeback rate. Chargebacks occur when cardholders contact their card's issuing bank to dispute a charge appearing on their credit card statement.

32. When a cardholder successfully disputes a transaction through a chargeback, the acquirer is required to refund the cardholder's money. The acquirer will then seek reimbursement from the holder of the merchant account through which the card transaction was processed. When the holder of the account is a payfac, the payfac will seek reimbursement from the submerchant responsible for the sale to the cardholder.

33. The card networks have developed programs to monitor merchant accounts with excessive chargebacks. Accounts that trigger certain chargeback thresholds are

subject to heightened monitoring requirements, and the card networks may impose fines or even terminate merchant accounts when chargeback rates do not decrease to an acceptable level after being monitored under these programs.

34. Prior to April 2025, Visa monitored merchants through its Visa Dispute Monitoring Program ("VDMP") when the merchant had at least 100 disputes (chargebacks) in a single month and the ratio of disputed transactions to total transactions (the "chargeback ratio") was higher than 1% (in some years, Visa set the acceptable threshold rate at 0.9%). Visa also monitored merchants that generated an excessive level of fraud through the Visa Fraud Monitoring Program ("VFMP") and placed merchants on the VFMP when the merchant exceeded $75,000 in transactions marked as fraudulent in a single month, and its fraud-to-sales ratio (measured in dollars) was 0.9% or higher. In or around April 2025, Visa introduced its amended Visa Acquirer Monitoring Program ("VAMP") and announced that VDMP and VFMP would be consolidated into and replaced by the amended program.

35. Mastercard has maintained a chargeback monitoring program similar to Visa's VDMP, where merchant accounts that generate 100 or more chargebacks and monthly chargeback rates of over 1% are subject to warning letters and placement in Mastercard's merchant chargeback monitoring program. Merchants whose monthly chargeback rates are over 1.5% for two consecutive months are deemed excessive chargeback merchants and subject to fines and potential termination.

36. Attempting to avoid triggering the card networks' chargeback monitoring programs, dishonest merchants often spread out their sales transaction volume across multiple merchant accounts—a practice commonly referred to as "load balancing." Doing so may allow such merchants to keep the total number of chargebacks or chargeback rates associated with each merchant account below the triggering threshold.

37. Acquirers and payment processors that terminate merchants for cause are required to place those merchants on a database maintained by Mastercard known as the Mastercard Alert to Control High-risk Merchants ("MATCH"). Reasons for adding a

merchant to MATCH include excessive chargebacks, fraud, laundering activity, bankruptcy, or violations of card networks' rules and standards.

38. Acquirers and payment processors, including payfacs, are required to check whether a prospective merchant is listed on MATCH when they perform due diligence on prospective merchant clients. Acquirers and payment processors routinely reject account applications from MATCH listed merchants, deeming them to be too risky.

39. Dishonest merchants often seek to have multiple merchant accounts so that they may maintain continued access to the card networks in the event any of their accounts are terminated.

40. In addition to chargeback monitoring, Visa and Mastercard each have other compliance programs to monitor and prevent illegal or brand-damaging transactions, such as Visa's Integrity Risk Program (formerly known as Global Brand Protection Program or "GBPP") and Mastercard's Business Risk Assessment and Mitigation ("BRAM"). These programs will also impose fines on acquirers that process payments for merchants engaged in fraud, illegal activity, or other activity that may pose legal or reputational risk, such as illegal sale of prescription drugs or counterfeit goods, miscoded gambling transactions, child exploitation and prohibited adult content, and transaction laundering. For such merchants, BRAM or GBPP violations can result in financial penalties (passed down from acquirers), account termination and placement on MATCH.

Restrictions on "High Integrity Risk or High Risk" Merchants and Telemarketing

41. The card networks and registered payment processors and acquirers impose additional restrictions on certain categories of merchants they deem to present a higher risk to the payment system. Merchants are typically classified as "high integrity risk or high risk" based on the nature of the products or services they sell, or the manner in which they sell them.

42. Generally, merchants with physical retail locations that accept payments from customers in person ("card present" transactions) are considered lower risk than merchants that process payments over the phone or the internet ("card not present" or

"card absent" transactions). Merchants and merchant categories that tend to generate higher than average levels of disputed transactions are typically considered "high integrity risk or high risk."

43. The card networks use a four-digit code, called the Merchant Category Code ("MCC"), to classify the type of business in which a merchant is engaged. A merchant is assigned an MCC when it first obtains a merchant account, and card network rules require that merchants be assigned the MCC that most accurately describes their business. Proper MCC classification helps to ensure that merchant accounts are subjected to the appropriate level of risk monitoring.

44. The card networks' rules require payment processors to classify merchants engaged in "outbound telemarketing" with MCC 5966. For example, Mastercard's guidelines for processors state that MCC 5966 should be used to designate merchants that "initiate direct contact with consumers to sell products or service … by phone, advertising, direct mail (other than a catalog), or other direct marketing method that includes either a toll-free phone number or a mailing address." Nuvei Limited's written risk policy also provides that an "outbound telemarketer" includes any "up-sellers" or merchants who sell products when cardholders contact the merchants' call centers.

45. The card networks' rules and Nuvei Limited's policy deem merchants classified as MCC 5966 to be "high integrity risk or high risk" and require that such merchants be subject to enhanced screening and monitoring.

46. Thus, according to the card networks' rules and Nuvei Limited's own written policy, Reimage would qualify as a merchant engaged in outbound telemarketing, and thus a merchant subject to enhanced screening and monitoring.

DEFENDANTS' BUSINESS PRACTICES

47. At various times material to this Complaint, Defendants have operated as an acquirer, a registered payfac, and a MoR, and deployed each of these payment processing arrangements to provide merchants—including merchants engaged in

deceptive marketing of tech support services such as Reimage—with the ability to accept card payments from consumers.

48. As a licensed electronic payments intermediary and principal member of Visa and Mastercard, Defendant Nuvei Limited is subject to periodic audits by the card networks as well as the Cyprus central banking authority (the "Central Bank of Cyprus" or "CBC"). Nuvei Limited is required to submit written policies and other evidence to the card networks and CBC demonstrating its adherence to sound underwriting procedures.

49. Nuvei Limited is also registered with the card networks as a payfac, and as a registered payfac, its due diligence procedures are subject to oversight by acquirers it has contracted with to provide payment facilitation services to merchants.

50. Nuvei Limited's written merchant onboarding policies and procedures purport to mandate the review and collection of information regarding each merchant applicant, including a signed application from the merchant; review of third-party websites or forums discussing the merchant (with "attention paid to the scam notifications in forums"); "Know Your Customer" (KYC) checks; checks on MATCH and other merchant screening databases; searches on company name and names of directors and owners; business model review and website compliance check; and review of past six months of payment processing history for high chargeback and refund levels or ratios.

51. Nuvei Limited's written policies also enumerate a large list of "prohibited industries" that Nuvei purportedly will not sponsor or onboard, including "get rich quick schemes," merchants or related parties "previously identified by any Card Brand for deceptive practices or any violation of Card Brand Rules," and "[c]omputer software (e.g., anti-virus) sold via inaccurate advertisements."

52. Since at least 2018, Nuvei Limited's policies have generally described tech support software providers as follows:

> These firms may induce cardholders to purchase software by provid[ing] false information regarding the status of their computer or the capabilities of their existing software. For example, the merchant may infer [sic] that the cardholder's computer is infected with a virus and is required to purchase anti-virus software from the merchant to remove the virus. The merchants may also falsely claim to increase the computer's speed. Furthermore, these merchants may also infer [sic] that they are the manufacturer or operating system provider of the cardholder's computer.

Despite this prohibition, Nuvei Limited has often onboarded tech support merchants engaged in these types of practices, including those engaged in outbound telemarketing, such as Reimage.

53. Nuvei Limited's written policies also purport to prohibit its sales and account managers from soliciting or accepting account applications from merchants "with known current or prior fraudulent activity," online merchants "suspected of aggregating transactions of other Merchants or Web sites under their Web site," merchants with a "history of excessive chargebacks or fraud," and merchants "where the true beneficial ownership is not clear or is masked by use of Local registered agents, attorneys or payment service providers."

The Reimage Tech Support Scam

54. During the times material to this Complaint, Defendants processed over $30 million in credit card charges for an offshore deceptive tech support scheme that went by the names "Reimage," "Reimage Limited," "Restoro" and "Restoro Limited" (collectively, "Reimage").

55. From at least 2011 to 2023, Reimage sold its tech support software through various websites, such as reimageplus.com, reimage-express.com, reimage.com, efix.com, reimagemac.com, and reimagetechsupport.com. In or around 2018 until 2023, Reimage also sold its tech support software to consumers using the brand name "Restoro" and offered the software through its website at restoro.com.

56. The corporate entity "Reimage Limited" was initially registered in the British Virgin Islands in or around 2009, re-domiciled in Isle of Man in 2016, and then

re-domiciled again in Cyprus in or around March 2023. The key principals and employees of Reimage worked out of an office in Israel and operated a telemarketing call center based in the Philippines. Reimage also contracted various third-party telemarketing call centers based in India since at least 2017.

57. Reimage targeted consumers in the U.S., harming older adults in particular, using deceptive pop-ups, bogus diagnostic software, scare tactics and deceptive telemarketing to convince consumers to buy costly tech support services. Consumers would typically first encounter pop-up windows or messages stating that their computers were infected with viruses or that their "Windows system is damaged." These pop-ups were often made to appear as messages from the Microsoft operating system.

58. Reimage's pop-ups would direct consumers to download free software that purported to confirm the fake virus or malware findings and prompted consumers to purchase the Reimage or Restoro "repair" software costing between $30 to $60. Consumers who purchased the "repair" software would receive an email or pop-up message directing them to call a toll-free number for "step by step online repair instructions" and "[f]ree support available 24 hours a day 7 a week."

59. Consumers who called the toll-free number were connected to a Reimage telemarketer—either a direct employee of Reimage or a contractor—posing as a tech support specialist. Under the pretense of providing free tech support, the telemarketer would remotely access consumers' computers and claim to find critical system failures, viruses or security risks purportedly requiring immediate repair. The telemarketer would then sell consumers additional tech support services over the phone.

60. An excerpt of Reimage's website below (at reimagetechsupport.com) shows how Reimage's tech support agents connected and infiltrated consumer's computers and lists the tech support service plans that were sold over the phone:

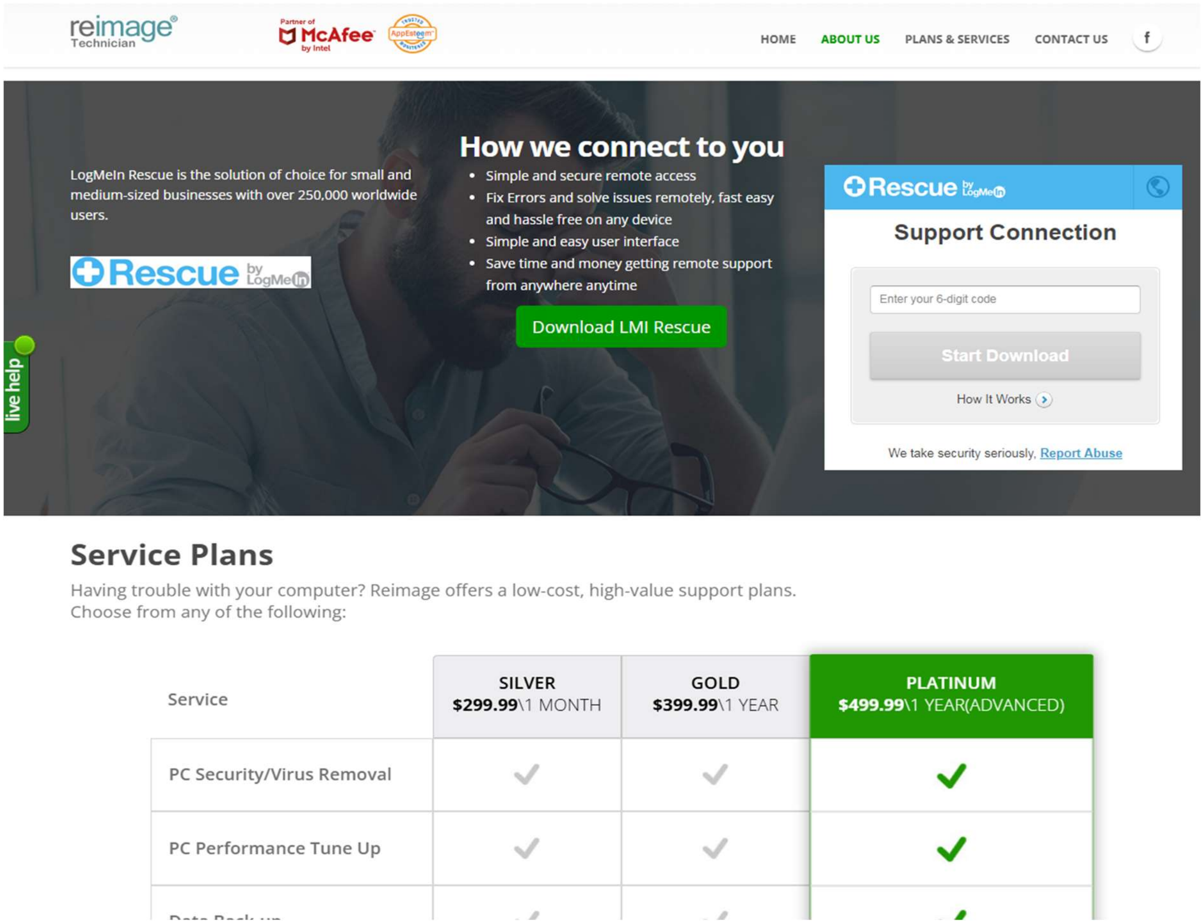

Figure 2: Excerpt of reimagetechsupport.com (archived February 2020)

61. The costs for Reimage's remote tech support services generally started at about $300 for the Silver plan, $400 for the Gold plan, and $500 for the Platinum plan. Reimage telemarketers may charge significantly more for the same service to consumers who were not informed of the listed prices of these plans. For example, one consumer was charged $500 for the Platinum package, whereas a different consumer in early 2021 was charged $1,000 for the same package.

62. In March 2024, the FTC filed a law enforcement action against Reimage for its violations of the FTC Act and TSR and obtained a stipulated federal court order with a permanent injunction and a judgment of $26 million for consumer redress. *See FTC v. Restoro Cyprus Limited et al.*, No. 24-cv-735 (D.D.C. Mar. 14, 2024).

Defendants Processed for Reimage Using Multiple Merchant Accounts

63. Defendants processed consumer card payments for Reimage from at least 2011 until July 2023, when Reimage shut down its operations after learning of the FTC's investigation and potential lawsuit. Depicted in the diagram below are the various payment channels Defendants arranged and used to take payments on behalf of Reimage from consumers, including consumers in the United States.

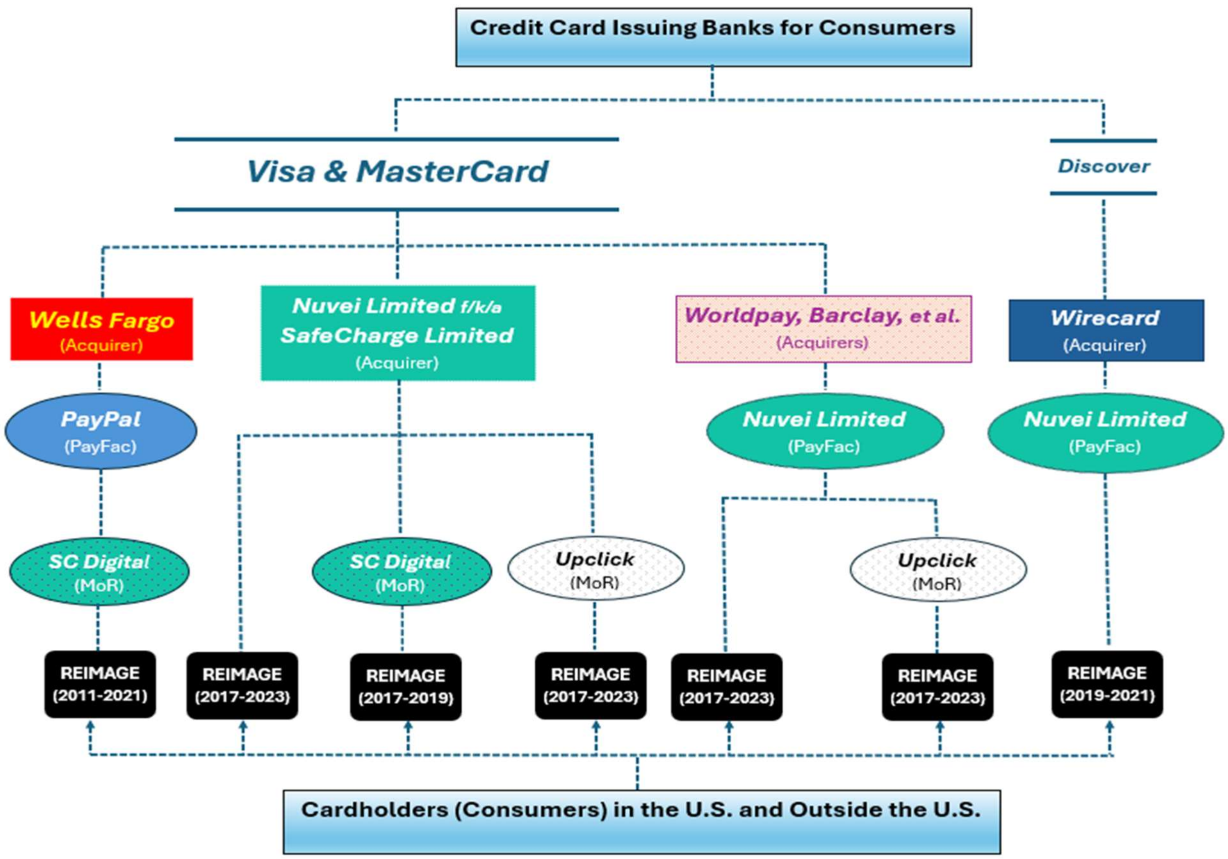

Figure 3: Overview of Defendants' Payment Processing Channels for Reimage

64. As shown above, from at least 2011 to about 2021, Defendants processed Reimage charges through merchant accounts opened under Defendant SC Digital, an unregistered payment aggregator. SC Digital contracted with registered payfacs, including PayPal, to obtain merchant accounts in its own name and then used the accounts to process payments for hundreds of unaffiliated third-party merchants, including Reimage. By March 2021, Defendants were forced to stop using SC Digital's

merchant accounts to process Reimage sales transactions, when PayPal terminated SC Digital's merchant accounts.

65. From around June 2017 until July 2023, Defendants processed Reimage charges through direct merchant accounts that Nuvei Limited opened for Reimage in Nuvei Limited's capacity as an acquirer and a registered payfac. By this time, Defendants had payment processing agreements in place with the card networks Visa and Mastercard, and other acquirers, such as Worldpay, Barclays, and Wirecard. These contracts enabled Defendants to process cross-border payments from cardholders in the United States and elsewhere for merchants such as Reimage that are located outside the United States.

66. From around September 2017 to July 2023, Defendants also processed Reimage charges through a third-party payment intermediary called Upclick Malta Limited ("Upclick"). Upclick is a Canadian-based payment processor that provides MoR services to tech support merchants, such as Reimage, many of whom target consumers in the United States. Upclick is not a merchant and does not sell goods or services to consumers. Instead, like SC Digital, it is an aggregator and conducts its business like a payfac.

67. Defendants opened multiple merchant accounts for Upclick in Nuvei Limited's capacity as an acquirer and as a payfac. When Defendants opened merchant accounts for Upclick in 2017, they were aware that Upclick was operating as a payfac and processing payments for Reimage.

68. From January 2017 to July 2023, Defendants processed over 310,000 separate Reimage sales transactions, with net sales totaling $28 million, through the various merchant accounts opened by Defendants under the name of Reimage Limited and SC Digital.

69. During that period, Defendants processed an additional 89,000 Reimage sales transactions with net sales totaling $3.8 million through merchant accounts opened under Upclick's name.

70. Over 41,000 of the sales transactions that Defendants processed through the Reimage and SC Digital merchant accounts involved consumers and issuing banks in the United States, and over 12,000 of the transactions that Defendants processed through Upclick's merchant accounts involved consumers and issuing banks in the United States.

71. During this period, Defendants processed tens of thousands of Reimage's telemarketing sales transactions through the Reimage and SC Digital merchant accounts, while processing mostly software charges through the Upclick merchant account.

Defendants Ignored Glaring Signs of Reimage's Deceptive Business Practices

72. Since at least 2015, Defendants have known that Reimage was operating a tech support scam and engaged in deceptive telemarketing to sell tech support services costing hundreds of dollars.

73. Because Defendants were processing payments for Reimage through the MoR SC Digital at this time, SC Digital's contact information would often appear on consumer invoices or credit card statements. As a result, Defendants received complaints and refund demands directly from consumers who were charged by SC Digital for Reimage's deceptively marketed software and telemarketing services. For example, in February 2015, a consumer apprised SC Digital that, after paying $34.95 for the Reimage "PC repair" software, the consumer was routed to a Reimage telemarketer who began to pitch expensive tech support services, after telling the consumer that the purchased software would not work to fix the purported laptop issue.

74. Through SC Digital, Defendants also saw that Reimage was incurring excessive chargebacks levels. In July 2015, Nuvei Limited prepared a report of Reimage's sales and chargeback data processed by SC Digital to assess Nuvei Limited's risk in onboarding Reimage. The report showed consistently excessive chargeback levels for Reimage sales processed across all major card networks (i.e., Visa, Mastercard, Amex and Discover) over the prior nine-month period, with chargeback rates averaging as high as 8.5% for payments processed through Discover.

75. In 2016, Nuvei Limited's credit risk team reviewed Reimage's chargeback rates through SC Digital's accounts for February 2016 through July 2016, reporting rates exceeding the 1% threshold every month, with one month rate reaching as high as 4.91%.

76. In February 2017, Defendants reviewed Reimage's chargeback levels for Visa and Mastercard, which showed monthly chargeback rates as high as 2.85% (Visa) and 1.72% (Mastercard). Reimage's excessive chargeback rates prompted Defendants to flag Reimage as one of the top 10 merchant clients whose migration to Nuvei Limited's portfolio will be "[r]isky" and "[p]roblematic with the chargebacks in the past."

77. Despite knowledge of these chargeback problems, the chief operating officer of Nuvei Limited and Nuvei Guernsey at the time continued to exert pressure on his staff to hasten the opening of the Reimage merchant accounts with Nuvei Limited in 2017.

78. In May 2017, Nuvei Limited looked to load balancing as a way to manage and mask Reimage's high chargeback levels from the card networks. For example, after opening accounts for Reimage at Nuvei Limited, Defendants continued to use the SC Digital merchant accounts to process payments for Reimage to spread Reimage's transaction volumes, and the corresponding chargeback counts, across multiple accounts. When a Nuvei Limited employee expressed concern with onboarding Reimage given its high chargeback problems, Nuvei Limited's head of risk management replied: "We will manage, will split their traffic with more banks…." He also warned others at Nuvei Limited to monitor the processing volume being sent through Reimage's merchant account at Nuvei Limited, stating that Reimage has "a high [chargeback] ratio and might exceed [the allowable threshold] if all [charges] will be in one [merchant account]."

79. Defendants also opened accounts for Reimage and other merchant clients through Nuvei Limited's payfac contracts with other acquirers, such as Worldpay and Wirecard, to facilitate load balancing and further spread their problematic merchant clients' transaction volumes across multiple merchant accounts and payment processors. For example, Nuvei Limited's head of risk management noted internally in July 2018, "I

need the [Worldpay accounts] open, our Fraud amount and ratio in [the direct merchant accounts at Nuvei Limited] is on the rise, we exceeded the early warning in Visa this month and I am planning to use [Worldpay accounts] as backup."

80. Because card networks monitor fraud and chargeback levels closely, Defendants manipulated chargeback rates to avoid network scrutiny. For example, in October 2017, after a spike in Reimage's chargebacks, a Reimage employee solicited Nuvei Limited's advice on how to reduce the chargebacks going forward, recognizing that "such numbers are unsustainable." Nuvei Limited's fraud investigator who looked into the root causes of these chargebacks found that all of the chargebacks were due to "fraud reason." Nuvei Limited advised Reimage that it should immediately issue refunds to dissatisfied consumers to reduce Reimage's chargeback counts. By issuing a refund before the chargeback is processed, Reimage would be able to reduce the number of chargebacks reported to the card networks and avoid triggering fraud and chargeback compliance violation notices from the card networks.

81. According to Defendants' internal records, Reimage's monthly chargeback rates consistently exceeded the 1% threshold between January 2018 and December 2022 (in 57 out of the 60 months), with chargeback rates ranging from 4% to 9% in many of these months. Defendants knew that the root cause of Reimage's excessive chargebacks was its deceptive marketing practices. In many of these months, Reimage's excessive chargeback rates did not trigger warnings or fines from Visa or Mastercard because, with the help of Defendants, Reimage was able to spread its sales and chargeback transactions across multiple payment processors and multiple merchant accounts—including accounts opened by SC Digital or by Nuvei Limited for Reimage—and thus avoid triggering the 100 or 150 monthly chargeback count threshold set by Visa or Mastercard.

82. Despite Defendants' load balancing tactics, in some months Reimage's monthly chargeback counts and fraud-to-sale ratios exceeded thresholds and triggered warnings from the card networks. In or around September 2018, for example, Mastercard flagged one of the billing descriptors used by SC Digital for Reimage transactions—

"SCD* rmg24.com"—for excessive number of chargebacks and a high fraud to sales ratio for the prior six months. As a result, this billing descriptor was placed in Mastercard's Global Merchant Audit Program ("GMAP"), which is a compliance monitoring program designed to alert payment processors of deceptive merchants and to reduce merchant fraud. Defendants sent Reimage a copy of the Mastercard violation notice but took no steps to address the root causes of the fraud complaints with Reimage.

83. In January 2019, Mastercard conducted an audit across Nuvei Limited's merchant portfolio and flagged 82 of its clients' accounts for multiple violations of Mastercard rules. The flagged clients included merchants suspected of selling prohibited goods, 28 merchants located outside Nuvei Limited's permitted geographic area, 39 merchant accounts "processing as unregistered [payfacs]," 18 accounts suspected of "using shell company," at least 20 accounts suspected of "load balancing of [chargebacks]," and merchants lacking bona fide businesses, among other issues. Mastercard threatened to assess a $25,000 fine to Defendants for each violation.

84. Reimage was one of the merchants flagged in this audit as a "scam." Upclick's merchant accounts at Nuvei Limited, used to process payments for Reimage at this time, were separately flagged by Mastercard for load balancing.

85. Mastercard reported its findings to Nuvei Limited showing that Reimage's "business phone number appeared on multiple scam complaint boards." A Nuvei Limited underwriter found that Reimage was reported on the Better Business Bureau ("BBB") website and other consumer complaint boards for running a tech support scam. She also found that Nuvei Limited's client monitoring system had flagged all of Reimage's websites as "negative due to content violation." She informed her manager that Reimage is a "PC support merchant" and suggested "maybe we should consider closing them."

86. In February 2019, Defendants relayed these findings to Reimage and asked Reimage to "clarify those issues" surrounding the scam reports. Reimage told Nuvei Limited that the "scam" complaints were over a year old and that Reimage was "working on improving [its] customer service on an ongoing basis."

87. In June 2019, anticipating a follow up audit from Mastercard, a Nuvei Limited underwriter visited Reimage's websites and found additional problems and red flags, including discrepancies in Reimage's business location displayed on some of these websites. She also noticed that many of the Reimage websites that were disclosed on its merchant account applications were taken down or "under construction."

88. In early 2020, Microsoft conducted a test purchase of the Reimage software and issued a report detailing how the computer user was first alerted with a fake virus and "Windows system" warning pop ups appearing to be from Microsoft. The pop up redirected the user to Reimage's website to download a software to fix the problem, then the user was directed to call a phone number for further "support." The phone number connected the user to a Reimage tech support agent who remoted into the computer, ran some "tests" and claimed to find critical system errors and security threats requiring the purchase of a "Platinum" tech support service package from Reimage. Before contacting Reimage's tech support agent, the Microsoft investigator ran Microsoft's anti-virus software on the computer and found "no threats prior to the test event," according to the report. The report also detailed how the Reimage support agent used "secure.safecharge.com" to process the payment and told the user that "Safecharge was processing the payment." Microsoft sent a copy of this report to Visa. In March 2020, Visa sent Nuvei Limited a GBPP violation notice letter based on Microsoft's independent investigation, along with a copy of Microsoft's report.

89. Upon receiving the Microsoft scam report in March 2020, a Nuvei Limited underwriter ran a merchant risk query (termed "transaction laundering") on Reimage with Nuvei Limited's third-party risk management solution provider, G2. G2 immediately issued a report stating that "we've found that reimageplus.com is part of a tech support scam network" and the "phone number historically listed on the URL [i.e., reimageplus.com] is tied to numerous postings of scam complaint forums." G2's report also identified additional Reimage websites, such as reimagetechsupport.com, that were being used to further the telemarketing scam and included a link to a YouTube video

describing how the Reimage scam was operating. G2's report concluded that "there is solid evidence that this URL [i.e., reimageplus.com] is run by scammers who send pop-ups to computers and claim they can 'fix' the problem … charging high amounts of money whilst also damaging their computers and stealing card info in the process." G2 also noted that the few positive online reviews about Reimage's service were "most likely bought because they seem fake."

90. Shortly after the G2 report was generated, G2's merchant monitoring system issued an "adverse merchant alert" to Nuvei Limited, stating: "We have discovered a tech scam laundering merchant that resides within your dataset," identifying Reimage as the merchant.

91. In response to the Microsoft and G2 reports exposing Reimage's scam, several employees in Nuvei Limited's underwriting and risk group voiced their concerns with Reimage to Nuvei Limited's COO. For example, one underwriter wrote: "[Transaction Laundering] report below - very bad." Nuvei's then Global Head of Risk and Underwriting also advised terminating Reimage. Nuvei Limited's VP of risk management agreed that the reports were "very bad," but noted the amount of business Reimage was sending to Nuvei Limited and SC Digital, suggesting they "try to push back to Visa."

92. After seeing the reports and recommendations from Nuvei Limited's underwriters to terminate Reimage, Nuvei Limited's COO responded:

> Hi Guys,
> We know reimage (and the owner 😊)
> I wouldn't jump into conclusions, its [sic] very stable account, and there is no real justification to this breach[.] [We] can speak with them and solve it, I don't think they are indeed at breach[.]

The COO then instructed the account management team at Nuvei Limited to assist Reimage in devising a response to Visa to explain the Microsoft scam report.

93. In its response to Visa, Reimage blamed its advertisers for proliferating the fake Microsoft pop-up ads and claimed that these marketers were acting without

Reimage's knowledge or approval. Reimage's response also stated that the company would keep a look out for "users with similar experiences."

94. Reimage separately assured Defendants that Reimage was no longer contracting out its call center services, instead relying exclusively on its own in-house call center for telemarketing, and that this should reduce fraud complaints volume.

95. While waiting for Visa's response on Reimage's GBPP violation, Nuvei Limited agreed to increase its Reimage processing volume by processing auto-renewing subscription charges on Reimage's tech support services and software. In April 2020, a Nuvei account manager pressed Nuvei Limited's risk group to approve the Reimage accounts to process more volume, noting that the COO "is pushing to get all traffic from this merchant and we could be waiting a year to hear back from Visa."

96. In May 2020, Visa sent Nuvei Limited a letter rejecting Reimage's response to the GBPP violation and issued a fine of 25,000 Euros. Defendants paid the fine by deducting it against Reimage's sales proceeds. Despite Visa's determination and the fine, Defendants continued to process millions of dollars in card payments for Reimage, including the Reimage auto-renewing subscription charges. When a Nuvei underwriting manager voiced concerns with taking on more of Reimage's processing volume given Visa's determination, Nuvei Limited's head of risk management replied: "The only [thing] that we can do is to trust them that they stopped it."

97. Defendants' underwriters and risk analysts, however, continued to believe that tech support sellers such as Reimage posed a substantial risk of fraud. In July 2020, when reviewing an application from a merchant whose owner used to work for Reimage, a Nuvei Limited underwriter recommended to her manager to reject the application because tech support merchants like Reimage are "usually using scamming techniques" to sell their tech support services and were "[t]oo high risk in terms of card schemes violations."

98. Defendants also continued to receive a steady stream of complaints from consumers about Reimage's misconduct. For example, in December 2020, a consumer

notified SC Digital that there was an unauthorized charge of $150 from SC Digital and wrote "If this item was concerning purchasing a security device which promised to clean my PC/iPad of virus, etc; or some such promise then I also require a refund" and noted that she was subjected to "high pressure selling."

99. Another consumer informed SC Digital in December 2020 that she was being charged $599.99 and $44.77 from SC Digital but "never got issues resolved on my PC." Yet another consumer wrote that she was charged over $2700 in December 2020 by SC Digital for a service that was "non existent" and a "scam."

100. In January 2021, another consumer wrote to SC Digital: "I believed your company was a computer technician company and that you could repair my computer. Your company took over my computer when trying to fix it. It did not work… I have no need for this support as I am not a company nor am I in any business. I am a retired person. I want my full payment returned to me of [$350.00 Australian dollars] paid via PayPal…."

101. In February 2021, a consumer provided SC Digital with a detailed report of the Reimage tech support scam, which was nearly identical to the findings from the Microsoft March 2020 report, showing that Reimage had not changed its deceptive practices. The consumer stated: "The company is obviously a scam or dishonest or hackers or maybe criminals."

102. In April 2021, another consumer told SC Digital that, after paying over $500 to a Reimage call center agent and repeated attempt to get tech support service, she was left with a computer that "now is inoperable and the technicians just keep changing settings on the computer with no change."

103. SC Digital responded to these complaints by telling the consumer that SC Digital was not the merchant but only the "payment facilitator for online businesses," that "as a separate payment provider company we are unable to assist you further," and to "communicate with Reimage's representatives directly."

104. In early 2021, a consumer targeted by the Reimage tech support scam reported to the German police that, after visiting the Reimage website in February 2021, he was directed to a Reimage telemarketer who accessed his PC through a "remote maintenance tool" and pitched the consumer Reimage security software and services. The consumer reported paying for the tech support services but "did not receive any service in return for the payment." The transaction was processed through SC Digital's merchant account at PayPal. The complaint prompted the German authorities to open a criminal investigation. On or about March 19, 2021, the German police contacted Defendants and flagged the transaction involving this consumer. The police inquiry referred to the Reimage telemarketer as an "unknown perpetrator" and "suspect" in a crime.

105. The German police inquiry was escalated to the head of Nuvei Limited's risk management group, who identified the transaction as involving the sale of tech support services by Reimage. A Nuvei Limited risk analysis director noted at this time that "since [Reimage] is a very old software merchant and [SC Digital's merchant account at PayPal] is closed already, I think that no further actions should be taken."

106. When Nuvei Limited's anti-money laundering (AML) compliance group learned of the German police inquiry, they contacted Nuvei Limited's underwriting group to get more information about Reimage and whether proper due diligence was conducted on Reimage. A Nuvei Limited underwriter responded to the AML compliance group by mentioning that Reimage had previously been flagged for a "similar reason" by Visa, but that Reimage was an "old and well-known client to everyone." Specifically, she stated:

> The issue with such businesses [i.e. tech support software providers] is that they use some affiliates and distribution channels and the user gets pop-up messages while browsing that the PC is at risk and they are prompted to download and install some software (in the past we had GBBP case for [Reimage] for similar reason but they assured us that very strict corrective measures have been taken to prevent this). Most probably this is where the [German police inquiry] is coming from.

Defendants did not launch any further investigation, did not conduct additional due diligence, and did not take any remedial action as to Reimage at this time.

107. Reimage's excessive chargeback rates persisted after the early 2020 Microsoft scam report. In April 2021, Defendants sent Reimage a notification from Mastercard stating that Reimage's merchant account with Nuvei Limited had a chargeback count ratio of 89.75% (184 chargebacks out of 205 sales) for the prior month. In May 2021, Defendants notified Reimage that its merchant account at Nuvei Limited had been flagged a second consecutive month for excessive chargebacks on Mastercard's ECM, with a chargeback rate of 4.30% (i.e., 112 chargebacks out of 2600 Reimage sales transactions processed through the Mastercard network) in April 2021. Defendants informed Reimage that Mastercard would assess Nuvei a fine of 1,000 Euros, which Defendants would pass onto Reimage.

108. In the ensuing months, Reimage reduced the sales transaction volume—and corresponding chargeback count—that was to be processed through its merchant account at Nuvei Limited and diverted a substantial portion of that sales volume to Reimage's other MoR payment processors, mainly Paddle and Bluesnap. While this enabled Reimage to simultaneously reduce the number of monthly chargebacks processed through Reimage's merchant account at Nuvei Limited, and thus avoid placement on Mastercard's ECM for a third consecutive month, the account continued to have high chargeback rates throughout 2021 and 2022. In September 2021, Nuvei Limited's head of risk management circulated an internal report to the Nuvei Limited risk group showing that the annual chargeback rate from Reimage's merchant account averaged over 8.5% (1108 chargebacks out of 12,934 total sales) in 2021.

109. In December 2021, Nuvei Limited's underwriting group conducted a periodic review of Reimage's merchant profile as part of the acquirer's periodic security and credit exposure risk assessment. The assessment for Reimage included "potential deceptive marketing indications detected," "indications for potential reputation issues detected," "potential content violations detected," "multiple domains identified on Ip address," and "high risk content sites detected." The assessment included a cursory

Google search, which came back with complaints about Reimage from BBB, Microsoft user forums, Reddit, malwaretips.com, and scammer.info, among other sites.

110. In September 2022, Nuvei's global risk group held a meeting where one of the items discussed was Reimage and the high levels of fraud and chargeback disputes associated with tech support and computer repair services. The group called attention to Reimage's excessive chargeback rates at the time, with some monthly rates up over 9%.

111. Despite the cumulative evidence of Reimage's deception, Defendants did not terminate Reimage and continually sought to maximize their profits by seeking ways to expand Nuvei Limited's processing volume for Reimage and its owners. In September 2022, a Nuvei Limited sales account manager reminded the Nuvei Limited risk group that "we have direct pressure from [the COO] to increase the volume with [Reimage and its owners]."

112. From the time Defendants received the Microsoft scam report in March 2020 to when Reimage shut down its operations in June 2023, Defendants processed over 115,000 individual sales transactions for Reimage, totaling over $9.5 million.

Defendants Opened and Maintained Merchant Accounts for Reimage Using a Straw Signor and Shell Company Address

113. Visa and Mastercard prohibit acquirers from onboarding merchants located outside their geographic territory. The card networks' rules requiring the merchant to have a legal and operational presence within the acquirer's jurisdiction seek to ensure an appropriate level of risk management by acquirers and to mitigate against merchant fraud, credit card laundering, and other risks to consumers and the credit card system.

114. For online merchants, telemarketers, or other card-not-present transactions, the card networks define the merchant's location as its principal place of business—i.e., the company's headquarters or where executive officers direct, control, and coordinate

the company's activities—or a permanent location where the merchant conducts its business or sales activities, such as telemarketing call centers.

115. From 2017 to 2023, Nuvei Limited opened and maintained merchant accounts for Reimage based on Reimage's shell entity registered in the Isle of Man, and then used these accounts to process tens of thousands of illicit telemarketing transactions.

116. Throughout this time, Defendants knew that Reimage's operations and executives were located in Israel, and that its telemarketing sales were conducted by call centers in the Philippines and India, which Reimage either owned or had hired.

117. For example, in 2014, Nuvei Limited approached the operators of Reimage to discuss moving its sales processing volume to Nuvei Limited's acquiring bank division, which had just obtained approval by Visa and Mastercard to operate as an acquirer. At the time, Defendants had been processing for Reimage through their MoR entity, SC Digital. Moving Reimage's processing volume to Nuvei Limited would allow Defendants to capture a larger portion of the processing fees from Reimage's sales and increase Defendants' profits.

118. At this time, Reimage, which was registered in the British Virgin Islands, informed Nuvei Limited that it did not have an active company located and registered in Europe that could sign a merchant contract with an acquirer in the European Union (EU).

119. In 2016, Nuvei Limited's then COO pressed Reimage to form an EU entity and noted that this project "is actually pending on your end for few months now, but no cooperation." After consulting with Nuvei Limited, the operators of Reimage set up a shell company, Reimage Limited, in the Isle of Man.

120. In February 2017, Reimage Limited submitted its merchant application to Nuvei Limited, listing a paid nominee director from Cyprus as the company's beneficial owner and authorized merchant account signatory. Defendants knew that this nominee director did not exercise any control or authority over Reimage's operations and was serving as a cover for Reimage's employees and executives located in Israel. Reimage

Limited's merchant account application listed as its primary business location an Isle of Man address that belonged to an incorporation service provider.

121. Despite Reimage's faulty merchant disclosures, Nuvei Limited's COO directed account managers at Nuvei Limited to open the Reimage merchant accounts even before conducting a KYC (know your customer), stating, "[w]e need to open [Reimage] with [Nuvei Limited] at the earliest in order to gain more volume and KYC can follow later on." He also directed its account managers to make daily in-person contact with Reimage to execute the merchant services agreement, noting that Reimage was located only "one floor between us and them" in the same office building in Israel.

122. In early 2019, Mastercard commenced an audit of Nuvei Limited's merchant portfolio and raised concerns with the Reimage account specifically. Nuvei Limited's head of underwriting at the time informed Reimage that "Mastercard believes we are processing an Israeli company" and is asking if Reimage had any departments located in the Isle of Man. A Nuvei Limited underwriting manager assured Reimage that "we will make sure to structure a good argument to Mastercard." At this time, a Nuvei Limited underwriter asked if Reimage was able to provide a copy of a rental agreement or an address of a single employee to substantiate Reimage's purported business operations in the Isle of Man. Reimage was unable to provide any of these records. In Nuvei Limited's internal merchant risk log, the underwriters noted that Reimage's Isle of Man address is associated with a "Trust company linked to Panama Papers" and that Reimage's nominee director is linked to "Paradise Papers—Appleby Officer." The underwriters also noted that there was "no real evidence" that Reimage's headquarters were located in the Isle of Man.

123. As a result of the red flags raised in Mastercard's audit in early 2019, Nuvei Limited was required to engage a third-party auditor to review its onboarding procedures and AML practices for compliance with Cyprus banking regulations and card networks' rules. In November 2019, the third-party auditor that Defendants hired, PaymentCounsel,

issued a report documenting a laundry list of problems with Nuvei Limited's merchant screening over the past three years.

124. With respect to Nuvei Limited's screening of Reimage, PaymentCounsel's audit noted the lack of "any checks performed on actual operating office location" given that the address belonged to an Isle of Man "trust provider" who also was listed as a corporate director of Reimage Limited. The auditor noted the "frequent changes in directors" and a "director living in Cyprus," and "having a registered address provided by a trust provider and a director with foreign nationality registered," as red flags indicative of money laundering. The auditor's report also noted that Nuvei Limited implemented no "measures against shell entity setups" and that jurisdictions such as Guernsey, the British Virgin Islands, or the Isle of Man present increased AML risks.

125. In early 2021, Visa initiated an AML review of Nuvei Limited's merchant processing activities. In anticipation of the review, Nuvei's AML compliance group revisited its internal records and identified Reimage as a merchant with "KYC gaps" and where "proof of EU operational address [was] not provided." When Nuvei Limited's CEO learned that the compliance group was planning to send a detailed AML questionnaire to Reimage and other clients to supply the missing KYC information, he instructed the group to use existing merchant applications to fill in missing information.

126. Nuvei Limited continued to process payments for Reimage and maintained its merchant accounts with a sham business location and straw owner and signatory listed on the account until July 2023, when Reimage ceased operations.

Defendants Processed Substantial Sums of Illicit Telemarketing Charges Through Reimage's Merchant Accounts Opened Only for Software Sales

127. When Defendants opened a direct merchant account for Reimage in 2017 through its acquiring bank division, Nuvei Limited, Defendants knew that Reimage was engaged in telemarketing, using purported "diagnostic" software to lure consumers to its telemarketing call centers. In fact, prior to 2017 Defendant SC Digital had been processing Reimage's telemarketing charges for years through merchant accounts in SC

Digital's name, concealing the fact that these charges stemmed from Reimage's telemarketing. While processing Reimage telemarketing charges through SC Digital's merchant accounts, Defendants routinely received complaints and disputes from consumers about Reimage's telemarketing practices and charges.

128. The card networks require acquirers and payment processors to register merchants engaged in telemarketing (especially outbound) as "high integrity risk" and employ enhanced screening and monitoring of such merchants. Reimage's use of deceptive pop up ads and purported diagnostic software to lure consumers to its telemarketing call centers falls squarely within the meaning of "outbound telemarketing" (MCC 5966) as delineated by Visa and Mastercard.

129. Nuvei Limited, however, did not assign MCC 5966 to the Reimage merchant account opened in 2017, did not register Reimage as a "high integrity risk" merchant, and did not disclose to the card networks that the Reimage merchant account was to be used to process telemarketing charges. Instead, Nuvei Limited designated Reimage as an "e-commerce" merchant (under MCC 5964), which allowed Nuvei Limited to avoid registering Reimage as a "high integrity risk" merchant subject to enhanced screening and monitoring. In early 2018, Defendants re-classified Reimage as a "Computer Software Stores" merchant (MCC 5734), which is a code used to classify businesses that primarily sell computer software programs and are not deemed by the card networks to be "high integrity risk." This code does not indicate that the transaction involves telemarketing.

130. Even though the Reimage merchant account was not approved and authorized by the card networks for telemarketing, Defendants assisted Reimage with using the account to process telemarketing charges. In September 2017, for example, a Reimage telemarketer contacted Nuvei Limited directly to seek technical assistance with clearing a $649 telemarketing charge, which had been blocked because the maximum single purchase price on the Reimage merchant account when it was opened was set at $100. A few months later, after Nuvei Limited raised the single purchase limit on the

Reimage account to $800 (without any additional underwriting), Reimage was able to use its direct merchant account to process its telemarketing charges.

131. In June 2019, Nuvei Limited submitted a merchant application for Reimage to acquirer Wirecard Bank AG ("Wirecard") to enable Reimage to accept Discover card payments. Wirecard rejected the application initially, informing Nuvei Limited that Reimage was mis-coded as "Computer Software Stores," while Reimage's website showed the merchant was offering tech support services. Wirecard's account application also required the applicant to disclose whether the merchant is engaged in telemarketing. Defendants submitted the revised application for Reimage to Wirecard with the "Computer Maintenance, Repair and Services" (MCC 7379) designation, but did not disclose that Reimage was engaged in telemarketing. Wirecard approved the revised application.

132. Since at least December 2020, Nuvei's risk account managers communicated regularly with Reimage's call center in the Philippines to manage chargeback disputes initiated by consumers who purchased Reimage tech support services through SC Digital and PayPal. Reimage instructed Defendants to forward chargeback notifications from PayPal that Defendants received to two Reimage call center managers and to a group email account called "Reports Manila."

133. Defendants continued to process telemarketing charges for Reimage until October 2022, when Reimage shut down its call center operations after learning about the FTC's investigation into Reimage's alleged misconduct.

134. Between January 2017 to October 2022, Defendants processed over 35,200 separate charges of $299 or more, totaling over $15.6 million, for Reimage's remote tech support services. Approximately 68% of these charges (totaling over $10.6 million) were billed to consumers in the United States.

SC Digital Used Its Own Merchant Accounts to Process Reimage Charges

135. From at least 2011 to 2021, Defendants used merchant accounts opened in the name of its MoR company, SC Digital, to process payments for Reimage and hundreds of other unaffiliated merchants.

136. To procure merchant accounts under SC Digital's name, Defendants entered into merchant services contracts with registered payfacs, such as PayPal. SC Digital submitted merchant account applications to registered payfacs purporting to be the "merchant" in the credit card transactions with consumers. In reality, SC Digital was operating as an unregistered payfac.

137. By processing Reimage and other merchant sales in aggregation through an MoR, Defendants were able to mask the excessive chargeback levels of specific high chargeback merchant-clients, such as Reimage, from the card networks and acquirers. Thus, while Defendants, through Nuvei Limited, had agreements with acquirers and the networks that allowed Defendants to open standalone merchant accounts directly for their merchant clients, Defendants also continued to process payments for high chargeback clients, like Reimage, through SC Digital's merchant accounts.

138. By processing Reimage charges through its MoR company, Defendants also were able to circumvent the card networks' restrictions on cross-border processing, as noted above in Paragraph 113. For example, with SC Digital registered in Cyprus as an MoR with European-based acquirers, SC Digital enabled sellers that were located outside the EU, such as Reimage, to surreptitiously access and process their charges through SC Digital's merchant accounts for years without detection by the card networks. In fact, prior to advising Reimage to create a shell entity in the Isle of Man and open a direct merchant account with Nuvei Limited in 2017, SC Digital served as the primary vehicle for Defendants to facilitate and process payments for Reimage's telemarketing call centers based out of the Philippines or in India.

139. Since at least 2015, SC Digital processed both software and telemarketing transactions for Reimage. As with Reimage's merchant accounts at Nuvei Limited,

Defendants classified SC Digital as a "computer software stores" merchant or "e-commerce" merchant.

140. By 2016, Defendants knew that Reimage was working with at least four MoR service providers—SC Digital, Bluesnap, Upclick, and Cleverbridge—to spread its sales volume and further conceal its chargeback rates.

141. In March 2018, Defendants received a compliance violation notice from Mastercard for using merchant accounts under SC Digital's name to process payments for third-party merchants. Mastercard found that SC Digital was operating as an unregistered payfac and rejected Defendants' claim that SC Digital was the "merchant" or "reseller of the goods." According to Mastercard, SC Digital was also improperly using the same generic MCC and its own address for each of its submerchants. Mastercard instructed Defendants to migrate all of SC Digital's merchant clients to a "compliant solution."

142. Defendants did not terminate or close all merchant accounts held by SC Digital at this time. Instead, they moved a portion of SC Digital's processing volume that passed through the Mastercard network to non-Nuvei payment processors, while continuing to process payments through SC Digital's merchant accounts for non-Mastercard payments. This caused Nuvei's chief compliance officer to warn Nuvei Limited's management that "we have effectively moved the bulk of the merchants from one non compliant solution to others," "we are at risk of damaging the relationship with [other acquirers] by processing knowingly non compliant traffic through them," and "we are effectively running two models for each merchant: one to cater for the Mastercard position and the other for Visa [and other payment methods]."

143. In January 2019, Mastercard sent another compliance violation letter to Nuvei Limited after reviewing transactions processed by the acquirer in the previous month. Mastercard flagged 82 out of 382 merchant accounts for suspected violations of its rules, including "28 accounts [suspected] in location violation," "39 accounts [suspected] in processing as unregistered [payfac]," "18 accounts [suspected] to be using shell company," and "20 accounts [suspected] in doing load balancing of the

[chargebacks].” One of the accounts flagged by Mastercard was Reimage’s account. Mastercard suspected Reimage of operating a “scam” and of processing through Bluesnap, an unregistered payfac based in Israel.

144. Defendants told Mastercard that Nuvei Limited would be investigating and taking seriously each of the compliance violations and would terminate any non-compliant merchants. Defendants, however, did not terminate Reimage and did not stop processing payments for Reimage. Instead, Defendants advised Reimage to modify its credit card billing descriptor so as to avoid “suggest[ing] an unregistered [payfac] relationship” to the card networks.

145. Defendants continued to use SC Digital to mask Reimage’s illicit transactions until early 2021, when PayPal terminated SC Digital’s merchant accounts.

Nuvei Limited Processed Reimage Charges Through Upclick’s MoR Accounts

146. In addition to SC Digital, Defendants also processed payments for Reimage through merchant accounts that Nuvei Limited—as an acquirer and registered payfac—opened for Upclick, a third-party MoR that caters to tech support merchants and who began processing for Reimage in or around 2016.

147. In early 2017, Upclick contacted Nuvei Limited to obtain merchant accounts under Upclick’s name, which it would use to process payments for Upclick’s merchant clients. Nuvei Limited knew that Upclick used an MoR model to process payments for at least four tech support merchants, including Reimage. Nuvei Limited knew that Upclick was processing telemarketing charges from call centers in Pakistan, Morocco, and Montreal that generated high chargeback disputes. Nuvei Limited’s COO informed Nuvei Limited’s CEO at the time that the MoR model was not approved by United States banks and the same would likely happen in the EU.

148. Despite this knowledge, Nuvei Limited’s management recommended onboarding Upclick to process the tech support software sales: “They can offer call center solutions to our clients, we should not take the call center in house as margins are low, and operation cost is high.” Nuvei Limited’s management underscored the $5 million in

monthly processing volume to be generated from Upclick and pressed his team to open the accounts quickly: "I have many of the materials of the company, and I want [to] open them fast…."

149. Nuvei's VP of Risk Management noted significant red flags, such as "high risk accounts with [chargebacks] ratio between 1.5% - 6%" and over $1 million in remote tech support services being processed through a Georgian acquirer "with multiple [merchant accounts]." He also noted that Upclick had been terminated by another payment processor and "to keep the [existing] accounts live they are using multiple [merchant identification numbers] and accounts." He concluded that Upclick has a "[v]ery high risk client base that can fade away very quickly," along with "aggressive call centers" that needed to be closed and high chargeback rates.

150. When a Nuvei underwriter reviewed Upclick's application and financials, she found additional discrepancies and red flags. She noted that the merchant application stated that Upclick's customer base was in France, but the actual product websites showed they were targeting consumers all over the world, including the United States. She also noted that Upclick's accounts were terminated or closed by seven different banks and used various, conflicting MCCs to describe their services.

151. On April 7, 2017, when Upclick's merchant application stalled due to the red flags, Nuvei Limited's COO directed Nuvei Limited's head of merchant services to "just make sure they go live ASAP, I want to start processing their traffic asap." He relayed that Upclick's owners "told me that they feel like they are losing the momentum," and that "you lose this merchant" if Nuvei Limited did not onboard them quickly.

152. In May 2017, Defendants opened the Upclick accounts and assigned MCC 5734 (Computer Software Store) to Upclick, despite their knowledge that Upclick was operating as an unregistered payfac. Nuvei Limited also knew that Upclick was headquartered in Canada. Nuvei Limited, however, opened these merchant accounts for Upclick using a shell corporate entity registered in the Republic of Malta.

153. About two months after Defendants onboarded Upclick, Nuvei Limited's COO asked Upclick to "increase the processing volumes to over $2M per month … per our initial discussions." Upclick wrote back: "We're happy to send you more volume asap but in order to keep the risk profile low in terms of [chargeback] count, would it be possible to simply open 4 new additional accounts instead of adding more volume to the existing ones? We could then double your volume while balancing the [chargebacks] and Refunds. It would be ideal situation for [Nuvei] and us." Nuvei Limited agreed to open these additional merchant accounts for Upclick to process payments from additional websites and with additional merchant billing descriptors.

154. In January 2019, Mastercard's audit flagged Upclick's merchant accounts at Nuvei Limited for impermissible load balancing. Mastercard's audit did not cause Defendants to terminate Upclick's merchant accounts.

155. In April 2019, Defendants advised Upclick to move some of its processing volume to other acquirers due to the high ratios of chargebacks (2% to 10%) and fraud (4% to 10%) on Upclick's accounts at Nuvei Limited. Upclick tried to explain away these fraud incidents as being caused by consumer confusion, but Nuvei Limited's account manager attached examples of the "many" consumer complaints and negative reviews, and noted that with Upclick, "it is not third party fraud, the users feel[] that they were scammed so they are processing [chargebacks] and reporting the [transaction] as fraud." Defendants urged Upclick to move quickly "to split the traffic [across processors] and have backups."

156. In May 2019, Defendants learned that Upclick's merchant account applications were being rejected by Nuvei Limited's payfac sponsoring bank, E-Comprocessing (an EU-based acquirer), due to known risks associated with tech support merchant processing and unresolved questions relating to the ownership of websites associated with Upclick. E-Comprocessing informed Nuvei Limited that it was rejecting Upclick's applications because "online PC support services involving any sort of remote PC repair services are traditionally associated with a high chargeback and fraud ratios

significantly increasing the risk exposure for the Acquirer, especially with the involvement of US traffic."

157. Defendants continue to process payments for Upclick and its merchant clients, despite repeated warnings from other acquirers about Upclick's merchant clients, and despite findings from Mastercard that MoRs are unregistered payfacs. As of June 2025, Nuvei Limited is still processing tech support payments for Upclick and its merchant clients.

158. From 2017 to July 2023, Defendants processed over 89,000 in Reimage charges through Upclick totaling approximately $4.1 million, after refunds and chargebacks. Over 12,000 of these Reimage charges routed through the Upclick merchant accounts were billed to consumers in the United States.

Defendants' Payment Processing for Other Deceptive Tech Support Merchants

159. Defendants are aware that tech support merchants seeking Nuvei Limited's payment processing services are often engaged in deceptive marketing practices and associated with high chargebacks. Despite the well-known risks involving tech support merchants, Defendants continue to process payments for tech support merchants.

160. Nuvei Limited's initial screening reports for prospective tech support merchant clients would often find signs of fraud and other red flags associated with these merchants' business practices, including online consumer complaints, payment processing histories showing excessive chargebacks, account terminations by prior payment service providers, domain registrant information shared with potential scam sites, anonymous domain registrations concealing a website's true owner, and merchants' telephone numbers connecting consumers to telemarketing call centers.

161. Despite these warnings, Nuvei Limited would onboard such tech support merchants whenever the merchant's expected processing volume is deemed to be substantial enough to justify the risk.

162. For example, in late 2020, Nuvei Limited opened merchant accounts for a tech support merchant that went by the names Innovana Thinklabs, Digital Protection

Services and PC Vark ("PC Vark"). PC Vark offered "software" designed to find purported problems and lure the consumer to their call centers where the consumers would be upsold tech support packages costing several hundred dollars or more.

163. Operating out of India, PC Vark was a key member of the telemarketing tech support fraud ring referred to as "Tech Live Connect." In October 2020, the Department of Justice ("DOJ") sued and enjoined several U.S.-based members of the Tech Live Connect enterprise. *See United States v. Cotter et al.*, No. 20-cv-24216 (S.D. Fla. Oct. 15, 2020). In coordination with the DOJ's action, the Indian Central Bureau of Investigation ("CBI") raided PC Vark's offices and call centers in India in or around September 2020.

164. Like Reimage, PC Vark's merchant application to Nuvei Limited was riddled with red flags, including the company's beneficial owner and associates showing up on MATCH for "excessive fraud," and publicly available information about the CBI's raid of PC Vark's offices in September 2020. Yet, Nuvei Limited approved PC Vark's merchant application and processed for it from October 2020 through February 2021.

165. As with Reimage and other tech support merchant clients, Nuvei Limited opened PC Vark's merchant accounts under the name of a straw owner and a shell company, which in PC Vark's case was registered in Romania under the name "Digital Protection Services." By the time Nuvei Limited paused PC Vark's processing in February 2021, Nuvei Limited had already processed tens of thousands of transactions a month for the scam. Nuvei Limited eventually terminated the accounts because, even with the use of tactics to reduce and mask chargebacks from the card networks, there were still excessive levels of chargebacks and fraud triggering warnings and penalty notices from the card networks.

Defendants' Payment Processing for the DK Automation Business Opportunity Scheme

166. Between April 2019 through June 2020, Defendant Nuvei Tech opened at least four separate merchant accounts for a deceptive business opportunity scam operated

by Kevin David, that used the brand names: "DK Automation," "The Official Kevin David," "Digital Ninjaz" and "That Lifestyle Ninja" (collectively "DK Automation").

167. DK Automation used false and unfounded earnings claims to sell business coaching programs and "turn-key Amazon stores" to consumers. Many consumers lost tens of thousands of dollars from DK Automation's scheme.

168. The FTC filed a law enforcement action against DK Automation in November 2022 for violating the FTC Act and other federal statutes or regulations, which the FTC alleged led to at least $52.9 million in consumer injury. *See FTC v. DK Automation LLC, et al.*, No. 22-cv-23760 (S.D. Fla. Nov. 16, 2022).

169. Nuvei Tech ignored numerous red flags that arose during the underwriting of DK Automation's accounts, including excessive chargeback levels with other processors, publicly available complaints in consumer review boards stating that DK Automation was a scam, and websites and social media posts indicating that DK Automation was a scam.

170. Nuvei Tech's underwriting file of DK Automation included a website replete with suspicious earnings claims, such as "how I made $20k profit my first month running Facebook ads" and "discover the invisible line that separates all six-figure drop shipping store owners from newbies who get no results."

171. Nuvei Tech's underwriting notes from that time state: "No heavy concerns found[] however a lot of reviews of it being a scam as much of what is taught, for the price, can be researched for free or lesser amount elsewhere" and "[a]dvertising is gimmicky with deception of earning a lot of money." Nuvei Tech opened merchant accounts for DK Automation and increased the purchase limit without taking any steps to look further into any of the earnings claims or testimonials that Nuvei Tech's underwriters found to be questionable.

172. Immediately, Nuvei Tech began to see elevated chargeback and refund rates for DK Automation. Due to these excessive rates, Defendants temporarily placed a 100%

hold on remitting any processed funds to DK Automation, while allowing it to continue and process consumer charges.

173. Despite the concerning chargeback and refund levels, in July 2020, Nuvei Tech approved DK Automation's request to increase the purchase limit on a single sale, up to $10,000. When Defendants raised the purchase limit, they already knew that DK Automation was charging consumers for more than this amount. In August 2020, for example, when Nuvei Tech flagged a purchase of $23,500 that DK Automation's sale agents tried to charge on a consumer's credit card, DK Automation explained to Nuvei Tech that the amount should have been transferred instead through wire payment.

174. In July 2020, Nuvei Tech notified DK Automation that while it would lift the 100% hold, it would be increasing the DK Automation reserve funds maintained by Nuvei Tech from 10% to 20%, as insurance against financial exposure to Nuvei Tech arising from DK Automation's business practices, including chargebacks or fines from the card networks.

175. At around the same time, Nuvei Tech's underwriting notes stated that the merchant had been incurring excessive chargeback and refund rates and that the merchant had taken down its website.

176. As DK Automation's chargeback levels continued to rise, by late 2021, Nuvei Tech notified DK Automation that it would be closing the merchant accounts "due to reputation risk and excessive refund activity."

177. From April 2019 to November 2021, Nuvei Tech processed over 17,000 sales totaling over $10 million for DK Automation.

Defendants' Payment Processing for Other Merchants Subject to Law Enforcement Actions or Court Orders and the Likelihood of Recurring Violations

178. In addition to the foregoing, Defendants, and specifically Nuvei Canada and Nuvei Tech, have failed to exercise proper due diligence, and have onboarded and processed payments for merchants subject to FTC or other law enforcement actions, or merchants placed on terminated merchant lists such as MATCH.

179. For example, in or around 2019, Nuvei Tech opened several merchant accounts and began processing for a tax "consulting" and government impersonation scam called American Tax Service, also known as American Tax Solutions ("ATS"). Prior to opening ATS's merchant accounts, Nuvei Tech obtained a personal guarantee from each of ATS's owners.

180. Nuvei Tech's underwriters designated ATS as a "high volume-high risk" merchant that transacts entirely through mail orders or telemarketing. Defendants failed to conduct proper due diligence of ATS, including ignoring numerous red flags, such as excessive chargeback history, publicly available consumer complaints about ATS's government impersonation tactics and the criminal history of an ATS owner and account signatory, who had pled guilty to bank fraud. Nuvei Tech opened merchant accounts for ATS and approved the merchant to process $300,000 in monthly volume. From January 2020 to January 2021, Nuvei Tech processed over $6.6 million in net sales for ATS.

181. In 2023, Nuvei Tech submitted additional merchant applications for ATS with additional acquiring banks in the U.S., seeking to increase the monthly processing volume to $1.2 million. In October 2025, the FTC and the State of Nevada sued ATS and its principals, and obtained a preliminary injunctive relief freezing defendants' assets and placing the company under the control of a court-appointed receiver. *FTC v. American Tax Service LLC, et al.*, No. 25-cv-01894 (D. Nev.).

182. Nuvei Tech has also opened at least five separate merchant accounts for a medical discount plan seller called Premier Health Solutions ("PHS"), despite Nuvei Tech's knowledge that this merchant was previously placed on MATCH in 2020 for excessive chargebacks. In 2022, state regulators in California brought license revocation proceedings, issued cease and orders, and imposed fines and penalties against PHS for, among other things, allegedly selling "illegal insurance" that "is not intended to be a primary health insurance policy, although [PHS] sold it as such." Similar proceedings against PHS were brought earlier in 2022 by state regulators in Vermont and Oklahoma, finding that PHS was "publishing materially false and misleading statements regarding

the nature and coverage of the benefit plans [PHS was] responsible for administering." In June 2023, PHS waived its right to an evidentiary hearing to contest the California proceeding and stipulated to an order imposing penalties and conditions.

183. Nuvei Tech onboarded PHS in late 2023 and began processing for this merchant starting in January 2024. In eighteen months (from January 2024 to June 2025), Nuvei Tech processed over $90 million for PHS's products and services. In June 2025, Nuvei Tech's sponsoring bank instructed Nuvei Tech to terminate PHS due to its growing chargeback problems and warned Nuvei Tech that reducing chargeback numbers through issuing refunds or credits "does not address the root cause of customer dissatisfaction" with PHS.

* * *

184. 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 engaged in their unlawful acts and practices repeatedly over a number of years; Defendants engaged in their unlawful acts and practices knowingly; Defendants continued their unlawful acts and practices despite knowledge of numerous complaints from consumers as well as warnings from banks, payment processors, and card networks; and Defendants remain in the business of payment processing, which is their core business, and maintain the means, ability and incentive to continue their unlawful conduct.

VIOLATIONS OF SECTION 5 OF THE FTC ACT

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

186. 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 and that is not outweighed by countervailing benefits to consumers or competition. 15 U.S.C. § 45(n).

COUNT I

Unfair Payment Processing Practices

187. In numerous instances, Defendants have:

(a) opened and maintained payment processing accounts for merchants that Defendants knew or should have known were engaged in unlawful practices;

(b) opened and maintained payment processing accounts for merchants that Defendants knew or should have known were engaged in load balancing, and which, among other things, enabled the accounts to avoid triggering the networks' chargeback monitoring systems;

(c) provided credit card networks, financial institutions and other payment processors information that Defendants knew or should have known was false or deceptive;

(d) failed to timely terminate merchants that Defendants knew or should have known were engaged in fraud or deceptive practices;

(e) ignored evidence of deceptive or other illegal activity on merchant accounts that Defendants opened or maintained and even took steps to shield deceptive merchants from further scrutiny, such as load balancing; or

(f) processed transactions to consumers' accounts for merchants that Defendants knew or should have known were shell companies or that engaged in deception.

188. 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.

189. Therefore, Defendants' practices as described in Paragraph 187 constitute unfair acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(a).

VIOLATIONS OF THE TELEMARKETING SALES RULE

190. 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.

191. Reimage 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).

192. It is a violation of the TSR 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(b).

193. 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). Pursuant to Section 4 of the Telemarketing Act, 15 U.S.C. § 6013(f)(2), the FTC is authorized to bring civil actions to enforce the TSR.

COUNT II

Assisting and Facilitating Violations of the TSR

194. 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 by making misleading statements to induce a person to pay for goods or service.

195. Therefore, Defendants' acts or practices as set forth in Paragraph 194 are deceptive telemarketing acts or practices that violate the TSR, 16 C.F.R. § 310.3(b).

CONSUMER INJURY

196. Consumers have suffered and will continue to suffer substantial injury as a result of Defendants' violations of the FTC Act and the TSR. Absent injunctive relief by

this Court, Defendants are likely to continue to injure consumers and harm the public interest.

PRAYER FOR RELIEF

Wherefore, Plaintiff requests that the Court:

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

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

C. Award any additional relief as the Court determines to be just and proper.

Respectfully submitted,

Dated: September 3, 2026

/s/ Russell Deitch

Russell Deitch
Sung W. Kim
Federal Trade Commission
600 Pennsylvania Ave., NW
Washington, DC 20580
(202) 326-2585 / rdeitch@ftc.gov
(202) 326-2211 / skim6@ftc.gov

Attorneys for Plaintiff
Federal Trade Commission

UNITED STATES DISTRICT COURT DISTRICT OF ARIZONA

Civil Cover Sheet

This automated JS 44 conforms generally to the manual JS 44 approved by the Judicial Conference of the United States in September 1974. The data is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. The information contained herein neither replaces nor supplements the filing and service of pleadings or other papers as required by law. This form is authorized for use only in the District of Arizona.

The completed cover sheet must be printed directly to PDF and filed as an attachment to the Complaint or Notice of Removal.

Plaintiff(s): **Federal Trade Commission , ;**

County of Residence: Outside the State of Arizona

County Where Claim For Relief Arose: Maricopa

Plaintiff's Atty(s):

Russell Deitch ,
Federal Trade Commission
600 Pennsylvania Ave
Washington, DC, District of Columbia 20580
202 326 2585
Sung W. Kim ,
Federal Trade Commission
600 Pennsylvania Ave
Washington, DC, District of Columbia 20580
202 326 2211

Defendant(s): **Nuvei Corporation , ; Nuvei International Group Limited , ; Nuvei Limited , ; SafeCharge Digital Limited , ; Nuvei Technologies, Inc. , ;**

County of Residence: Maricopa

Defendant's Atty(s):

Howard Shelanski ,
Davis Polk & Wardwell LLP
1050 17th St NW
Washington, DC, District of Columbia 20036
202-962-7060
Michael Scheinkman ,
Davis Polk & Wardwell LLP
450 Lexington Ave
New York, New York 10017
212-450-4754
John Atchley III,
Davis Polk & Wardwell LLP
450 Lexington Ave
New York, New York 10017
212-450-3469

IFP REQUESTED

REMOVAL FROM COUNTY, CASE #

II. Basis of Jurisdiction:	**1. U.S. Government Plaintiff**
III. Citizenship of Principal Parties **(Diversity Cases Only)**	
Plaintiff:	**N/A**
Defendant:	**N/A**
IV. Origin :	**1. Original Proceeding**
V. Nature of Suit:	**890 Other Statutory Actions**
VI.Cause of Action:	**15 USC 53(b) & 57b; 15 USC 6105; STATEMENT: Violation 15 USC 45(a) and FTC's Telemarketing Sales Rule, 16 CFR Part 310**

VII. Requested in Complaint

Class Action: **No**

Dollar Demand:

Jury Demand: **No**

VIII. This case **is not related** to another case.

Signature: Sung W. Kim

Date: 9/3/2026

If any of this information is incorrect, please go back to the Civil Cover Sheet Input form using the *Back* button in your browser and change it.
Once correct, save this form as a PDF and include it as an attachment to your case opening documents.

Revised: 01/2014