UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

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

Plaintiff,

v.

PADDLE.COM MARKET LIMITED,
an England and Wales private limited company,
Judd House, 18-29 Mora Street,
London, England, EC1V 8BT, and

PADDLE.COM, INC., a Delaware corporation,
3811 Ditmars Blvd., #1071
Astoria, New York 11105,

Defendants.

Case No. 1:25-cv-01886

COMPLAINT FOR PERMANENT INJUNCTION, MONETARY JUDGMENT, AND OTHER RELIEF

Plaintiff, the Federal Trade Commission ("FTC" or "Commission"), 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), the FTC's Telemarketing Sales Rule ("TSR"), 16 C.F.R. Part 310, and Section 4 of the Restore Online Shoppers' Confidence Act ("ROSCA"), 15 U.S.C. § 8403. 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), the TSR, 16 C.F.R. Part 310, and ROSCA, 15 U.S.C. §§ 8401–05.

SUMMARY OF CASE

2. For years, Paddle.com Market Limited and Paddle.com, Inc. (collectively, "Paddle" or "Defendants"), have assisted and processed payments for deceptive tech support schemes that have bilked tens of millions of dollars from consumers, including older adults.

3. Paddle has opened merchant accounts and processed consumer payments on behalf of tech support schemes that sell bogus "diagnostic" software and operate offshore telemarketing call centers that deceptively pitch costly computer repair services. Some of these schemes have impersonated well-known companies such as Microsoft or McAfee to perpetrate their scams and phishing attacks. Paddle knew these schemes used deceptive advertisements. Paddle has assisted such schemes to evade scrutiny and detection by banks and the card networks (e.g., Visa and Mastercard). In many instances, Paddle has also harmed consumers by enrolling consumers in and charging consumers for automatically renewing subscription plans for tech support products and services without clearly disclosing to and informing consumers they will incur recurring charges.

4. In perpetrating their consumer payment processing scheme, Defendants have violated the FTC Act, the TSR, and ROSCA.

JURISDICTION AND VENUE

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

6. 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

5. The FTC is an agency of the United States Government created by the FTC Act, which authorizes the FTC to commence this district court 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. The FTC also enforces ROSCA, 15 U.S.C. §§ 8401–05, which prohibits certain methods of negative option marketing on the internet.

DEFENDANTS

6. Defendant Paddle.com Market Limited ("Paddle UK") is a private limited company incorporated in England and Wales in 2012. Paddle UK's principal office is located in London, England. Paddle UK provides payment processing services for software companies, including sellers of tech support services. Paddle UK is the registered owner of the "PADDLE" trademark, filed with the United States Patent and Trademark Office in 2012, for the provision of "[c]omputer software for processing electronic payments and transferring funds to and from others … financial services, namely, electronic transfer of funds to purchase products and services offered by others … [and] temporary use of on-line non-downloadable software for processing electronic payments," among other things. Christian Owens ("Owens") is the co-founder of Paddle UK and, from 2012 to at least 2023, Owens served as Paddle UK's CEO and Chairman. Hugo Grimston ("Grimston") served as Paddle UK's CFO and director from 2014 to at least 2022. At all times material to this Complaint, Paddle UK has opened merchant accounts

in the U.S. and processed credit card and other electronic transactions with consumers in the U.S. for tech support products and services. Paddle UK transacts or has transacted business in this District and throughout the United States.

7. Defendant Paddle.com, Inc. ("Paddle USA") is a Delaware corporation. Paddle USA's principal place of business is 3811 Ditmars Blvd., #1071, Astoria, New York 11105, which is a mailbox rental service. Paddle USA provides payment processing services for software companies, including sellers of tech support services. Defendants formed Paddle USA in 2019 in order to establish a U.S.-based merchant account and to further grow Paddle UK's revenues by processing for Defendants' clients marketing to consumers in the U.S. As Defendants told operators of the deceptive Reimage tech support scheme, "Paddle set up a new business entity in the United States … to help improve payment acceptance in the United States" and "create more 'native' payment experiences for US customers." Paddle USA's corporate registration filing lists Owens as its CEO and sole director and owner. Owens and Grimston have signed contracts with banks and financial institutions as the CEO and CFO of Paddle USA, respectively. Paddle USA has an "F" rating from the Better Business Bureau (as of July 2024). At all times material to this Complaint, Paddle USA has opened merchant accounts in the U.S. and processed credit card and other electronic transactions with consumers in the U.S. for tech support products and services. Paddle USA transacts or has transacted business in this District and throughout the United States.

COMMON ENTERPRISE

8. Paddle UK and Paddle USA have operated as a common enterprise while engaging in the deceptive or unfair practices and violations of the FTC Act, the TSR, and ROSCA alleged below. Defendants have conducted their business practices through two

interrelated companies that have common ownership, officers, managers, business functions, employees, customers, websites, and office locations. Indeed, Paddle's Head of Risk and Compliance stated that Defendants formed Paddle USA so that they could "open[] a US merchant account to channel our US traffic through" and have represented to third parties that "all the beneficial owner and website/sales information [between Paddle UK and Paddle USA are] the same." Because Paddle UK and Paddle USA have operated as a common enterprise, each of them is liable for the acts and practices alleged below.

COMMERCE

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

DEFENDANTS' BUSINESS ACTIVITIES

10. Since at least 2017, Paddle has assisted tech support sellers, including sellers engaged in deceptive telemarketing, by processing consumer debit and credit card payments for these tech support sellers. Paddle knew that such sellers used deceptive advertisements. Paddle also has processed card charges for such sellers, presenting those charges under Paddle's own name instead of the actual sellers' names. This has impeded the banks' and card networks' ability to detect and monitor those sellers' transactions.

11. As detailed below, Paddle's payment aggregation practices obscure the deceptive sales practices of its clients. Paddle has failed to adequately screen its clients and ignored warnings of their deceptive practices, and in some instances, has helped to conceal the deceptive practices of its clients, such as "Reimage" and "PC Vark," while profiting from their deception.

12. Paddle has also violated ROSCA by charging consumers for auto-renewing tech support subscription services without clearly disclosing material terms, including the fact that consumers will be charged on a recurring basis unless the subscriptions are canceled.

Paddle's Payment Aggregation Practices

13. Paddle processes consumer credit and debit card payments for software companies, including sellers of tech support services.

14. A merchant is typically required to have an account in good standing with an acquiring bank (also known as a "merchant bank" or "acquirer") to charge consumers' credit or debit cards. The acquirer, in turn, must have payment processing agreements with the card networks, such as Visa and Mastercard, to enable the merchant (i.e., the seller) to accept card payments.

15. The fact that a merchant has a dedicated account with an acquirer helps the card networks and the acquirer monitor risks or problems associated with that specific merchant's card transactions.

16. Over the past decade, the card networks have allowed certain merchants to take card payments from consumers using a "payment facilitator" ("payfac") model. This alternative model has been accepted by the card networks primarily to provide a cost-effective way for small, low-volume merchants that may not have sufficient sales volume or capital to obtain their own payment processing accounts directly from an acquirer.

17. Under this alternative model, the acquirer contracts with a payfac that has entered into merchant services contracts with the merchants. The payfac uses its own "master" merchant processing account with the acquirer to process, in aggregation, cardholder payments for many unaffiliated merchants and distributes the proceeds, minus the payfac's processing fee, to those

merchants who sold the products or services. The card networks and acquirers sometimes refer to payfacs as "payment aggregators" or "aggregators."

18. The card networks refer to the merchants that contract with the payfac as "sponsored merchants" or "submerchants." The payfac serves as the "sponsor" for these merchants and is required by the card networks and the acquirer to screen and monitor sponsored merchants to ensure that they are bona fide businesses and comply with applicable laws and the card network rules.

19. More specifically, the card networks instruct payfacs to manage and control the underwriting and onboarding of sponsored merchants and to assess merchant risk. As such, a payfac is required to screen and monitor each of the sponsored merchant's websites and products "for signs of illegal activity or transaction laundering as well as deceptive marketing practices" and to "terminate sellers engaged in activity harmful to the payment system or in willful violation" of the card network rules. *Visa's Payment Facilitator and Marketplace Risk Guide*, available at https://usa.visa.com/content/dam/VCOM/regional/na/us/partner-with-us/documents/visa-payment-facilitator-and-marketplace-risk-guide.pdf (published April 2021).

20. The card networks require payfacs to register with the networks and relevant acquirers. Paddle has never been registered or approved by an acquirer or the card networks to operate as a payfac.

21. For a payfac to onboard and process for merchants that the card networks consider high-risk—such as outbound telemarketers or merchants in industries with traditionally high levels of refunds and chargeback rates—the card networks require the payfac to register with both the networks and the acquirer as a high-risk payfac. Paddle has never registered as a high-risk payfac.

22. 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). Thus, the card network rules prohibit payfacs from submitting charges into the card networks for other payfacs.

23. This prohibition is vital because such arrangements significantly impede the ability of the card networks and acquirers to detect bad conduct, such as consumer fraud, by merchants. Among other problems, such arrangements place multiple layers between the merchant and the acquirer, obstructing the card networks and acquirers from identifying high chargeback and refund rates and complaints associated with the merchant.

24. Paddle has known for years that the card network rules prohibit payfacs from processing for other payfacs or aggregators. Nevertheless, Paddle has engaged in such conduct by operating as a payment aggregator and processing payments for Paddle's clients through registered payfacs.

25. For years, Paddle has avoided registering as a payfac, failed to comply with the merchant underwriting and monitoring requirements governing payfacs, and claimed to be the "merchant" in the transactions with the customers of Paddle's clients.

26. In Paddle's merchant services contracts with registered payfacs, which currently include PayPal, Stripe, Worldpay, and Checkout.com, Paddle represents that it "acts as a reseller and merchant of record." This has enabled Paddle to open multiple merchant accounts with registered payfacs under its own name. Paddle has then used its own merchant accounts to process payments, in aggregation, for thousands of unaffiliated merchants.

27. Paddle, however, is not the actual seller of the products and services sold by Paddle's clients. Paddle does not market those products or services, or provide technical support, to consumers. It instead provides payment processing services to sellers that offer products and services to consumers. Indeed, Paddle's website, paddle.com, is not used to market or sell any products or services to consumers but is primarily used to promote Paddle's payment processing services to prospective clients. For example, paddle.com has stated at various times (including as late as October 2024) that Paddle will provide "[e]nd-to-end payment processing solution for [software sellers] … you can offload your entire payments tool-chain," and that "merchant of record providers" such as Paddle "exist to take the burden of payment processing and compliance away … [and] handle[] payment processing and the related liabilities, while the [software seller] takes care of customer service, delivery, fulfillment, and customer support for the product or service being sold."

28. Paddle's website paddle.net, to which Paddle often directs consumers when they have questions as to why Paddle charged their credit cards, states: "Paddle provides a payment and billing solution used by thousands of software companies around the world to sell their products" and "[t]housands of software companies partner with Paddle to manage transactions." Paddle's "Merchant of Record Fact Sheet" further states that "product marketing is handled by the [software sellers] to ensure brand consistency."

29. Paddle's contracts with its clients stipulate that "Paddle will have no responsibility to provide ongoing customer service, complaints handling technical or other continuing support for the Product and/or delivery level … with the [consumers], the responsibility for which lies entirely with you [i.e., the seller and Paddle's client] and you undertake to indemnify Paddle in full from and against any such claims or liability." These

contracts also provide that Paddle's clients and consumers "retain ownership of all right, title and interest in and to the Product."

30. When consumers contact Paddle to inquire about any product- or service-related questions, Paddle's representatives routinely respond: "We handle the e-commerce and checkout process but we are unfortunately unable to provide technical assistance." In these communications, Paddle informs the consumers that "we serve as a payment processor for our partner software developers." Paddle routinely uses the term "reseller" interchangeably with "payment processor," as follows: "Paddle acts as a reseller of digital products; we serve as a payment processor for our partner software developers…." Thus, consumers who purchase tech support software products using Paddle's payment website are directed to contact the tech support seller directly in order obtain the software activation key, as described further below.

31. When consumers purchase the tech support and software products from Paddle's clients, the products are presented and sold to the consumer under the software seller's name and brand, not under Paddle's name. The product pricing, refund terms, and other conditions of the sale are determined by Paddle's client, and not by Paddle. As such, Paddle instructs its clients to "[m]ake sure the [consumer] accepts their terms & conditions and refund policy before they make a purchase" and to notify Paddle of "any changes in your refund policy, product T&C or contact details and update your website accordingly." Therefore, many consumers understand that the seller of these products or services is Paddle's client (and not Paddle) and that they are bound to the terms and conditions set by the software seller.

32. Paddle never takes possession of its clients' products and does not buy their software in bulk at wholesale before the products are sold (or resold) to consumers. Instead,

Paddle's contracts with its clients purport to convey momentary title of the products to Paddle at the time of sale to the consumer.

33. When consumers purchase the products from software merchants using Paddle's services, the product payments from consumers are billed and collected by Paddle, but ultimately remitted to Paddle's clients (minus Paddle's fees) each month, which is typical practice for payment processors. Notably, Paddle does not book the full value of the product sales as Paddle's own revenue, and instead only reports the processing fees generated from the payment processing service as Paddle's revenue.

Paddle's Failure to Effectively Screen Its Clients

34. Paddle knows that, under the card network rules, payfacs are required to effectively screen and monitor the merchants that they onboard. Even though Paddle has, in practice, operated as a payfac, it has failed to conduct effective screening and monitoring of the sellers that Paddle has onboarded.

35. Paddle solicits prospective clients to sign up for Paddle's payment services by offering the seller immediate access to all major credit cards and payment methods without the seller having to open its own merchant account.

36. A seller seeking to open a payment processing account with Paddle can do so by filling out a short online form listing the seller's company name, a contact name and email for the account, the website where the seller's software is being offered, a general description of the seller's product, and expected monthly revenue.

37. Before authorizing the seller's account for processing, Paddle may ask the seller to complete a quick "know your customer" (KYC) verification check on the account, which can be passed in a few minutes with the account signor providing their ID (such as a passport) and

answering a few basic questions, such as the business owner's date of birth and nationality. Paddle may request additional information from the seller after the account has been opened, such as business registration records and, in some cases, it may conduct a cursory review of the seller's website.

38. Once the seller agrees to Paddle's service fee and provides a bank account for Paddle to remit the consumer payments to the seller, the seller can immediately start posting charges onto consumers' credit cards or PayPal accounts through Paddle. In some cases, Paddle has allowed these sellers to start billing consumers through Paddle before they had completed their KYC verification.

Paddle's Payment Aggregation Practices Obscure Merchants' Deceptive Activities and Chargeback Problems

39. Merchants that pose a greater risk of fraud or financial loss to the card networks, acquirers, or consumers, may be denied merchant accounts. For example, the acquirer may be concerned that the merchant is engaged in deceptive marketing or other illegal conduct, or that the merchant will generate excessive rates of transactions returned or disputed by consumers, typically known as "chargebacks."

40. Consumers initiate chargebacks when they dispute card charges by contacting their card's "issuing bank"—the bank that issued the credit card to the consumer. When a consumer successfully disputes the charge, the consumer's issuing bank credits the consumer's credit card for the disputed amount and recovers the chargeback amount from the acquirer. The acquirer, in turn, collects the chargeback amount from the merchant, either directly or through its payment processor.

41. To detect and prevent illegal merchant activity, the card networks operate various chargeback monitoring and fraud monitoring programs. For example, if a merchant generates

excessive levels of chargebacks that trigger the thresholds set under Visa's chargeback monitoring program, the merchant is subject to additional monitoring requirements and, in some cases, penalties and ultimately termination.

42. Paddle's operation as a payment aggregator impedes the card networks' ability to identify and monitor the specific merchant involved in the consumer transaction. For example, when a consumer purchases a product from a software or tech support seller that Paddle has onboarded, the charges that are transmitted through the card network and posted to the consumer's credit card or PayPal account appear as "PADDLE.NET" or "PAYPAL* PADDLE.NET," even though Paddle is not the actual merchant in the transaction. In some cases, the product name may additionally appear in the billing descriptor, such as "PADDLE.NET* RESTORO."

43. Regardless of the billing descriptor or other information posted to the consumer's credit card account, each of the unaffiliated sellers' charges for their products and services is aggregated and processed through the same merchant accounts held in Paddle's name.

44. Moreover, because the sellers onboarded by Paddle generally do not have separate accounts in their own name with an acquirer or an authorized payfac, these sellers take card payments from consumers without undergoing basic risk monitoring by the acquirers or registered payfacs.

45. The credit card networks and acquirers monitor merchants by, among other ways, keeping an eye on the chargeback rate associated with the merchant's account with the acquirer. Because Paddle uses its own merchant account to process, in aggregation, transactions for thousands of separate merchants selling different products and services, the card networks and

acquirers do not have visibility into the chargeback rates associated with specific sellers onboarded by Paddle.

46. In effect, Paddle's payment aggregation practices have substantially assisted deceptive tech support sellers with high chargeback rates to evade card networks' and acquirers' detection and scrutiny.

47. In July 2018, Paddle's founder and CEO at the time stated to Paddle's board of directors: "[g]iven that Paddle has a number of sellers on the platform it can absorb the higher chargeback rate as the rate that our payment processors and credit card companies look at is in aggregate."

48. Despite the aggregation of many sellers' charges through Paddle's own merchant accounts, there have been numerous instances when Paddle's merchant accounts with acquirers and payfacs have been put in jeopardy and subject to fines or termination due to an excessive number of chargebacks from deceptive sellers that Paddle onboarded and processed for. In these instances, the chargebacks from these sellers had accumulated and driven up Paddle's overall chargeback rates in a given month.

49. In such instances, Paddle would engage third-party chargeback prevention services, such as Ethoca or Verifi, to artificially reduce chargebacks without investigating and addressing the root cause of the chargebacks.

50. Typically, when a consumer files a chargeback with the bank that issued the credit card ("issuer"), the issuer would alert the credit card network, the credit card network would alert the acquirer, and the acquirer would alert the payfac, which then alerts the merchant. Through this process, the card networks are able to track the number of chargebacks a merchant accrues.

51. Some issuers have agreements with chargeback prevention companies so that, when the cardholder initiates a chargeback with the issuer, the issuer will notify the chargeback prevention company first. The chargeback prevention company then notifies the merchant directly about the cardholder's dispute ("pre-chargeback alert"). In these instances, the issuer will often wait 24 to 72 days before notifying the credit card networks of the chargeback. If, during that window, the merchant refunds the cardholder, the issuer will deem the dispute resolved and will not forward the chargeback to the credit card networks.

52. Here, because Paddle is posing as the merchant and has engaged the chargeback prevention companies directly, Paddle would receive the pre-chargeback alerts arising from chargebacks initiated by consumers who purchased products from those sellers that Paddle has onboarded. Once Paddle receives the pre-chargeback alert, Paddle would immediately issue a refund to the disputing cardholder to resolve the dispute and prevent the dispute from getting logged with the card networks as a chargeback.

53. The refunds that Paddle issued to consumers would be deducted from the sales proceeds that Paddle collects and remits to the seller, without any notice to or detection by the credit card networks or acquirers. Paddle's constant use of chargeback prevention services, sitting atop its aggregation practices, has allowed Paddle to mask the true chargeback dispute rates of specific sellers, including tech support sellers engaged in deception, from the card networks and acquirers.

Paddle's Substantial Assistance to Tech Support Sellers Engaged in Deception

The PC Vark Scam

54. From at least April 2017 to January 2019, Paddle processed over $11 million in credit and debit card charges for an offshore tech support scam called Tech Live Connect

("TLC") through merchant accounts opened under Paddle's name. The operators of the TLC scam formed a company in India called PC Vark to advertise and sell bogus diagnostic software in the U.S. and elsewhere, which the scammers used to lure consumers to call TLC's offshore telemarketing call centers. PC Vark named its call center in India "Premium Techie Support."

55. PC Vark used deceptive pop-ups, bogus diagnostic software, scare tactics, and deceptive telemarketing to convince consumers to buy, typically unnecessary, costly tech support services.

56. PC Vark's deceptive sales process typically started with an unsolicited pop-up message on the consumer's computer, indicating that the computer is infected with a virus or subject to other serious security threats. It directed the consumer to one of PC Vark's websites, where the consumer was invited to download a free "diagnostic" or "optimizer" software.

57. PC Vark's pop-up message and webpage were often styled to appear to come from Microsoft, Google or Apple, but PC Vark had no affiliation with any of these companies.

58. Consumers who downloaded and ran PC Vark's software received a report that their computer had problems that needed immediate attention. These consumers were encouraged to buy online a software program from PC Vark—costing between $60 and $118—to further diagnose and fix the problem. Paddle processed the charges for that initial software purchase.

59. Consumers who bought the software were then directed to call a toll-free number to "activate" the software, or to get assistance from a live "tech support" service agent to help install and run the software.

60. The toll-free number connected consumers with a call center in India, and the tech support service agent was, in truth, a PC Vark telemarketer. The telemarketer would request,

and often gain, remote access to the consumer's computer, make false claims about finding purported problems on the computer, and deceive the consumer into paying for additional tech support services or security software to "repair" the computer and remove any virus or security threat. Paddle did not process the charge for this second transaction.

61. The PC Vark software purchase and its activation process were designed to funnel consumers to PC Vark's deceptive telemarketing call centers and to solicit or induce the purchase of additional tech support services over the phone.

62. In September 2020, India's Central Bureau of Investigation raided several offices of PC Vark in Jaipur, India based on findings that PC Vark was sending pop-up messages on computers with fake virus warnings and directing consumers to install unneeded software. The United States Department of Justice (DOJ) followed with an enforcement action against several U.S.-based members of the TLC enterprise in the Southern District of Florida and obtained a temporary restraining order from the court, and ultimately a permanent injunction against these TLC defendants. *See U.S. v. Cotter et al.*, No. 20-cv-24216 (S.D. Fla. Oct. 15, 2020).

Paddle's Substantial Support to the PC Vark Scam

63. Paddle first onboarded PC Vark in April 2017 under the seller name "PC Vark," and subsequently opened at least nine other accounts for PC Vark at Paddle under various other names, such as "Systweak Software," "Echosoft," "XPortSoft," "AV Signup," "XPortSoft," and "PC Tuneup Tools." Paddle knew that these accounts were linked because they all had the same account representative or account contact information, and because Paddle was asked to redirect consumers who contacted Paddle with questions or complaints about the software to PC Vark's tech support team, Premium Techie Support.

64. Soon after it onboarded PC Vark, Paddle began receiving a steady flow of complaints from consumers reporting that PC Vark was selling malicious software or scareware and harassing consumers with deceptive telemarketing. Paddle routinely responded to these reports by offering to issue a refund for the initial software purchase. However, Paddle disclaimed any liability for the hundreds of dollars consumers paid for the additional tech support services that PC Vark sold over the phone.

65. In November 2017, for example, a consumer wrote to Paddle's customer service about seeing a malware or virus infection warning on her computer, prompting her to purchase PC Vark software for $118.80. The consumer reported that, after the software purchase, the consumer was then directed to a call center where "over the span of 2.5 hours [the consumer] spent over $700 on software the techies in India said I needed." The consumer's report detailed how the tech support agents at PC Vark "commandeer your computer while you watch your screen," claim "they have an agreement with Apple that when a computer is infected, their warning and call numbers come up," and continue to send "menacingly aggressive phone calls" once they "ascertained very quickly" that the consumer was not well versed in computers. The consumer recommended that Paddle "speak with the fraud departments of all the major banks, credit cards and PayPal" about these tech support scams, which her credit card company heard of "dozens of times every single day" and which "seem to target seniors living alone."

66. Paddle issued a refund to this consumer for the initial $118 software purchase, but not for the $700 subsequent purchase. Paddle told the consumer that it was "conducting an investigation with full co-operation of the vendor who supplied this product." In reality, Paddle ramped up its sales processing volume for PC Vark the following months.

67. In January 2018, another consumer wrote to Paddle to report that, after purchasing PC Vark's "Mac Cleaner" software (a PC Vark diagnostic software for Apple Macs), PC Vark's call center "tried to up sell me for various products" and that she had to get Apple's tech support to remove PC Vark's malware from her computer.

68. In April 2018, a consumer informed Paddle that PC Vark conveyed "misinformation" about PC Vark's "Advanced Mac Cleaner" software, which was not approved for use on Apple computers, and that the consumer had to seek assistance from Apple to remove this malicious software.

69. In May 2018, another consumer wrote to Paddle that he received a deceptive virus alert pop-up that prompted him to purchase the PC Vark software. This consumer was then connected to PC Vark's call center and its remote tech support agent who demanded additional payments to "clean up" his computer and was also asked the consumer to pay a "broker fee." That consumer wrote: "I was surprised and confused by all this. What was to be a one time expense of $118.80 (for two years) came in the end [] to be over $900, if I wanted a proper and complete service from you."

70. In June 2018, a consumer wrote to Paddle: "I attempted to purchase MacCleaner but once it loaded it stated I had to call a number to get it properly working. This number took me to a third party support desk who aggressively sold me a support service … because they had control of my computer I felt I had to purchase their products … MacCleaner was just a gateway to this arm twisting experience." The consumer asked Paddle to refund him for the $60 software purchase and the $600 he paid the telemarketers. While Paddle agreed to issue a refund for the initial $60 software purchase, Paddle instructed the consumer to contact PC Vark to seek a refund for the disputed telemarketing charges totaling $600.

71. In July 2018, a consumer told Paddle that "we have been scammed and our computer is now in jeopardy," and that they were directed to call a phone number to activate the software, which "resulted in 4 telemarketers attempting to sell us an expensive product ($404.00 and $4.99 a month, ongoing) which we didn't know if we actually needed or not."

72. In August 2018, one consumer warned Paddle: "What a scam, an hour of my life on the phone with horrible premiumtechiesupport people…. Please know that you are working for a place that is causing people a great deal of strife."

73. In September 2018, another consumer told Paddle: "I thought I was buying Mac Keeper for [$118] and you tricked me. Your site looked the same and I had to call to activate. Next thing I knew you were in my computer."

74. Paddle knew that it was processing for PC Vark and that this seller was engaged in deceptive conduct, including deceptive telemarketing. From at least April 2018 through July 2018, Paddle executives internally discussed how to address PC Vark's deceptive practice of using its software to lure consumers to its offshore call centers. Paddle's head of risk and compliance told Paddle's CEO and CFO (at the time) that PC Vark was "disrupting the order completion flow with cross selling" to consumers and "leading them to the dodgy phone selling where people take over their computers." As he informed Paddle's CEO and CFO, "[w]e know as a fact … that this is what is causing the vast majority of our chargebacks from these guys."

75. PC Vark accounted for a substantial portion of Paddle's processing volume and revenues at the time. Despite its knowledge of PC Vark's deceptive practices, Paddle did not stop processing payments for PC Vark. In fact, between March 2018 and August 2018, Paddle processed over $1 million per month in sales of PC Vark's software. About half of these sales were made to consumers in the U.S.

76. For Paddle to maintain its merchant account in good standing with acquirers and payfacs and avoid fines and placement of its account in the card network's fraud monitoring programs, Paddle is required to maintain monthly chargeback rates below the allowable threshold, which at this time in 2018 was 1%. Paddle knew that PC Vark's chargeback rates regularly exceeded that monthly threshold. For example, of the 17 months Paddle was actively processing charges for PC Vark, from September 2017 to January 2019, the monthly chargeback rate exceeded 1% in 16 of those months. There were many months during this time when the rate climbed over 2% or 3%.

77. In December 2017, Paddle received a warning from Visa, which had been flagging certain transactions flowing through Paddle's merchant account due to an alarming number of chargebacks. Paddle knew that the spike in chargebacks was primarily due to PC Vark's sales transactions. Paddle saw that PC Vark's chargeback rate had climbed to over 7% at this time. Paddle's CEO noted to others at Paddle that "this is getting pretty excessive" and "we should really do something about [PC Vark's] account."

78. In June 2018, Stripe, one of Paddle's payfacs, warned Paddle that its merchant account had been experiencing a high level of chargeback disputes, and that one of the billing descriptors associated with a PC Vark software product had the "highest dispute rate." To address Stripe's concerns, Paddle's Head of Risk told Stripe that Paddle is "providing notices to our vendors with the highest chargeback rates and will cease our relationships with them shortly" and was implementing a "blanket refund policy." However, Paddle continued to process payments for PC Vark for several additional months, until January 2019.

79. In September 2018, Paddle sent PC Vark the chart below showing the excessively high monthly chargeback rates accruing on PC Vark's account at Paddle from January 2018 to August 2018.

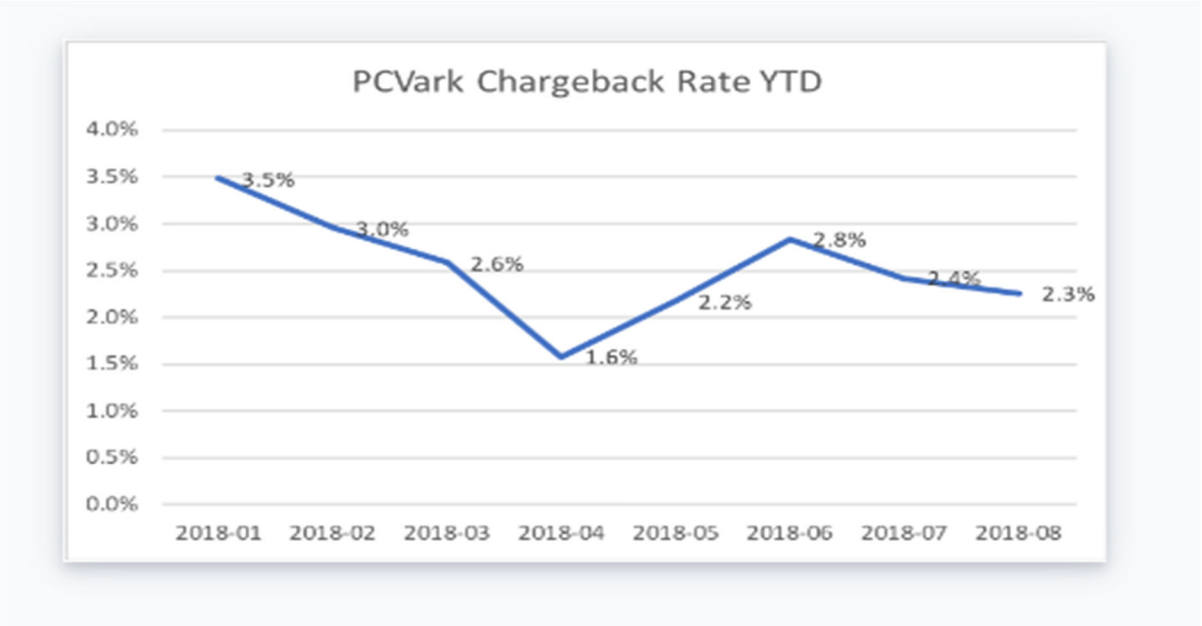

Figure 1: Snapshot of PC Vark chargeback rates at Paddle

80. Since PC Vark was one of the highest-volume accounts at Paddle in 2018, PC Vark's chronically high chargeback rates continued to create monthly chargeback issues for Paddle's own merchant account, even though Paddle was aggregating the charges of thousands of other unaffiliated sellers.

81. Paddle received other red flags regarding PC Vark. In November 2017, for example, a member of Paddle's internal finance team observed that PC Vark was shuffling through different company names (from PC Vark to Innovana Thinklabs and then to Digital Protection Services) in a span of weeks and relocating its bank accounts to different countries. This is a practice that fraudulent companies often adopt when their brand names receive negative reviews. In addition, in February 2018, Paddle employees noted that there were other suspicious

or unusual charges coming from the PC Vark account. Paddle did not underwrite and reexamine the PC Vark account in response to these material changes to PC Vark's account information.

82. In September 2017, the operators of PC Vark opened another vendor account at Paddle under the name "XPortSoft." PC Vark operators told Paddle that they were looking for Paddle to process $30,000 in sales of a software called PC Optimizer Pro. In November 2017, an account manager at Paddle informed Paddle's CEO and other executives that this software "product has a pretty bad rep as a fake product/scam," but that the merchant has already begun selling the product through Paddle. Paddle continued to process for PC Vark and collect payments for PC Optimizing Pro.

83. By 2018, the operators of PC Vark had opened multiple accounts at Paddle, under different seller names, to process consumer payments for PC Vark's antivirus software.

84. In August 2018, an independent software reviewer notified Paddle and McAfee, an antivirus software company, that Paddle was processing payments for a merchant that was using fake domains and pop-up ads that impersonated McAfee, and defrauding consumers into purchasing fake McAfee software. The reviewer noted that there were multiple accounts at Paddle "running this scam against McAfee" and urged Paddle to "vet its vendors and check the sites and links that use paddle to process payments."

85. Paddle found out that the two accounts called to its attention by the reviewer and also by McAfee—the Echosoft account and the AV Sign Up account—were linked to PC Vark and controlled by the same group of individuals operating PC Vark. Paddle's Head of Risk and Compliance informed PC Vark that there were "escalated complaints from various sources such as your customers, Google and McAfee directly claiming that you are defrauding your customers while posing to be McAfee fraudulently and are engaging in phishing attacks."

86. McAfee demanded that Paddle issue refunds to defrauded consumers. Paddle responded by claiming that the seller in question "changed their initially approved website with these malicious weblinks without informing us." In an internal email to Paddle's executives, Paddle's Head of Risk and Compliance reported that these were "phishing attacks … carried out by fraudsters and this is a criminal offense." Despite this knowledge, Paddle did not immediately terminate PC Vark's accounts at Paddle.

87. Instead, in August 2018, Paddle's management discussed how to protect itself from liability from PC Vark's illegal conduct after discovering there could be a shortfall in reserve funds available to indemnify consumers seeking refunds because of PC Vark's McAfee impersonation scam. As part of that discussion, Paddle's CFO at the time decided: "If we get any blow back from this, then we should get PcVark [sic] to cover any costs (taken as a deduct from their seller balance)." Thus, Paddle decided that it would use incoming proceeds from ongoing PC Vark's sales to cover any shortfall caused by PC Vark's illegal conduct.

88. Paddle also sent the PC Vark account holders an indemnification agreement to sign that would require PC Vark to reimburse Paddle for any chargeback exposure caused by the McAfee impersonation scam.

89. By October 2018, the chronically high chargeback levels associated with PC Vark's primary account at Paddle were causing problems for Paddle's own merchant accounts. Paddle's CEO at the time informed the board: "We are approaching MC [i.e., Mastercard] and Visa's excessive chargeback thresholds (1%) which could mean that we may face fines if we cross these thresholds and worst case it may also result in us ceasing processing payments if we are banned (rates would need to be 2-3% without a plan to reduce back down to <1%). If we get banned by MC/Visa for chargeback concerns, then we can't simply skip to another payment

processor since the banning would be at the card schemes level." As a result, Paddle informed PC Vark that it would need to close PC Vark's accounts by the end of 2018.

90. The card network rules require acquirers and payment processors, including payfacs, to not only immediately terminate sellers engaged in fraud or activity harmful to the payment system, but also to add the terminated merchants to a screening database such as the Visa Merchant Screening Service or the Mastercard Alert to Control High-Risk Merchants. A key reason is to warn other acquirers and payment processors from onboarding fraudulent or deceptive merchants. Even though Paddle was effectively terminating PC Vark for cause—*i.e.*, due to excessive chargebacks and other signs that PC Vark was engaged in fraud—Paddle did not report the termination to any acquirers or payfacs, or to the card networks.

91. Moreover, instead of severing its ties with PC Vark outright, in September 2018, Paddle sought out and procured a "revenue share referral" agreement with another payment processor in the U.K. dealing with high-risk merchants. The purpose of this agreement was to enable Paddle to extract a referral fee for transferring PC Vark's processing volume to the other payment processor. Paddle's Head of Risk and Compliance assured PC Vark at this time: "I have spoken to an alternative payment gateway who is experienced at handling high chargeback digital businesses so I believe this could be a good long term fit for your business and cause minimal disruption. They have asked if you currently have a UK entity and if you're keen to begin introductions to start their onboarding process." Paddle's CFO (at the time) signed the referral agreement for Paddle.

92. In the end, Paddle assisted and facilitated PC Vark's tech support scam by processing over $12.5 million in sales of PC Vark's bogus diagnostic software, with knowledge

that PC Vark was using the software to lure consumers to its telemarketing call centers, where it deceptively sold additional costly tech support products.

The Reimage Tech Support Scam

93. From April 2020 to at least June 2023, Paddle processed over $37 million in credit and debit card charges for a pair of affiliated deceptive tech support software merchants, "Restoro Limited" and "Reimage Limited" (collectively, "Reimage"). These Reimage entities were registered in the Isle of Man and later re-domiciled in Cyprus.

94. The Reimage tech support scam was nearly identical to the PC Vark scam. Reimage used deceptive online pop-ups containing false virus or security warnings to lure consumers to download "diagnostic" or "optimizer" software products and ultimately subjected these consumers to deceptive sales pitches from Reimage's offshore telemarketers.

95. The deceptive pop-ups would falsely state that consumers' computers were infected with viruses or that their "Windows system is damaged." The pop-ups were often made to appear as messages that came from Microsoft.

96. Reimage's pop-ups directed consumers to download a free version of a software program from Reimage, sold under the "Reimage" or "Restoro" brand name, which would typically "confirm" the virus or malware findings and prompted consumers to purchase "repair" software, costing between $30 to $60.

97. Paddle aggregated and processed the card charges for this initial software purchase from Reimage through Paddle's own merchant accounts, in the same manner as Paddle did for PC Vark.

98. As with PC Vark, consumers who purchased a software program from Reimage would be directed call a toll-free number to "activate" the software, as shown below:

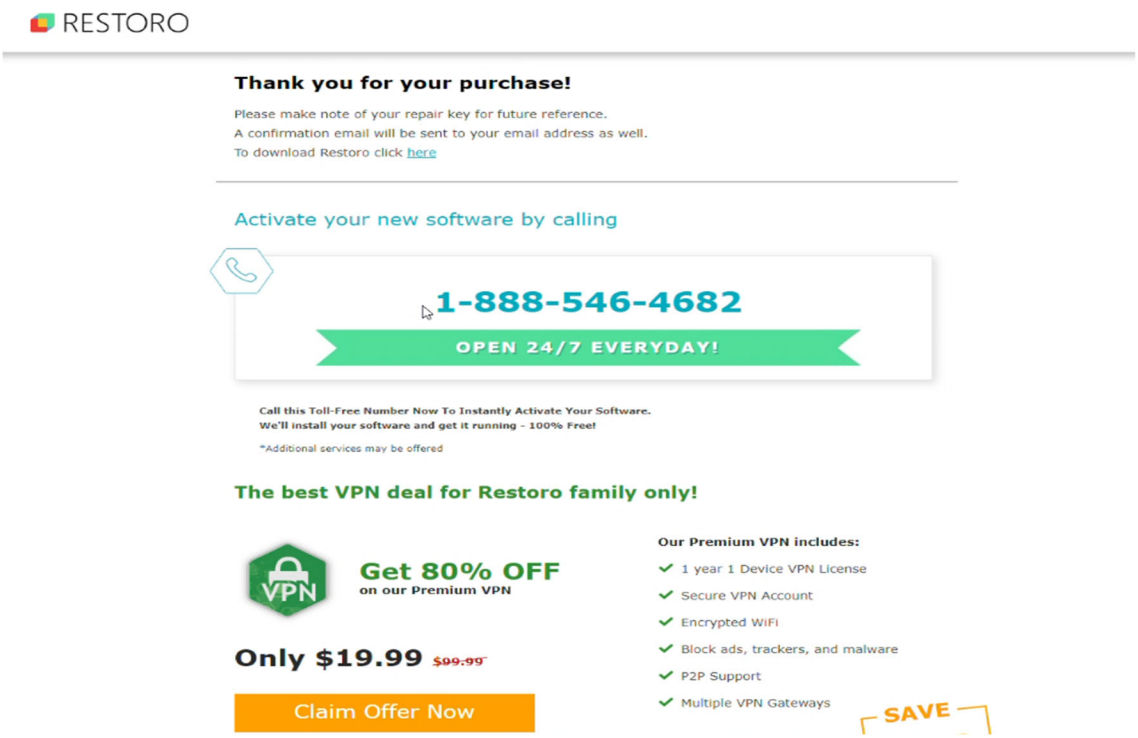

Figure 2: Reimage payment confirmation (www.restoro.com/sale/paddle/success)

99. Consumers who called the toll-free number were connected to a Reimage telemarketer posing as a tech support specialist. Under the pretense of providing tech support, the telemarketer would remotely access the consumer's computer to "find" critical system failures, viruses or security risks purportedly requiring immediate repair and sell consumer tech support services costing hundreds of dollars over the phone. Paddle did not have a contract with Reimage to process the charges for these additional tech support services sold over the phone.

100. As with PC Vark, the software purchase from Reimage and its activation process were designed to funnel consumers to Reimage's deceptive telemarketing call centers and to dupe consumers to purchase costly tech support services over the phone.

101. The FTC filed a law enforcement action against Reimage Limited and Restoro Limited in the District of Columbia in March 2024 for their violations of the FTC Act and TSR, and obtained a stipulated federal court order that prohibits the defendants from misrepresenting

security or performance issues or any other material issues related to the sale, marketing or distribution of any product or service, and from engaging in deceptive telemarketing. The order also provides for $26 million in consumer redress. *See FTC v. Restoro Cyprus Limited et al.*, No. 24-cv-735 (D.D.C. Mar. 14, 2024).

Paddle's Substantial Support to the Reimage Scam

102. Paddle executives approached operators of the Reimage scheme in February 2020 to offer Paddle's payment processing services. During contract negotiations, Paddle came across online complaints about Reimage's deceptive pop-ups and sales practices and learned that Reimage could present a chargeback risk. Paddle also knew that Reimage was using multiple payment aggregators (i.e., unregistered payfacs) and wanted to open accounts at Paddle to spread Reimage's sales processing volume across more providers. Spreading sales volume across multiple accounts or payment processors for the same product is a common tactic used by sellers, including tech support service providers, that anticipate having their accounts terminated for fraudulent or deceptive practices.

103. From the beginning of the relationship, Paddle chose to ignore red flags arising from Reimage's deceptive sales practices. For example, during the onboarding process in February 2020, a Paddle risk and compliance employee alerted Paddle's key executives to consumer complaints about Reimage's deceptive advertising tactics, stating that he had "found articles (also on Microsoft forums) of people complaining the way Reimage Repair flags users they have malware issues vs. Microsoft not detecting any pc bugs," and circulated a link to the executives to see the detailed complaints. Nevertheless, Paddle approved Reimage to open an account with Paddle and offered Reimage discounted service fees to incentivize Reimage to send substantial processing volume over to Paddle.

104. Paddle also knew that Reimage was targeting consumers who lacked technical knowledge of computers, many of whom were older adults. Paddle's account manager once remarked: "Target User for Restoro/Reimage is a non-technical person above 50 I believe."

105. Paddle cleared Reimage to begin processing payments from consumers immediately through Paddle without Reimage having verified basic company details. For example, in April 2020, Paddle's merchant onboarding personnel asked Reimage to answer a few basic questions and provide details about the company's owner, including the "date of birth and nationality," and advised that "anyone from the business who owns more than 25% of the shares can complete the verification." In June 2020, Paddle wrote to Reimage requesting, again, that it complete its answers for Paddle's KYC background check, which "should not take more than 5 mins to complete." By this time, Paddle had already been processing Reimage consumer charges for over two months, totaling over half a million dollars in sales.

106. Had Paddle undertaken any basic screening or background check, it would have discovered from easily accessible records that, at this time in June 2020, Restoro Limited and Reimage Limited were registered to straw owners or directors located in Cyprus and in the Isle of Man, and not to the actual owners or principals of Reimage.

107. Paddle began receiving complaints from consumers about deceptive telemarketing by Reimage as soon as Paddle started processing consumer charges for Reimage. For example, one consumer reported to Paddle in April 2020 that, after receiving a charge of $40 for the Reimage software from Paddle, Reimage's phone agent pretended to find problems with the consumer's computer. The consumer informed Paddle about "extensive complaints and massive numbers of scam accusations" about Reimage based on an internet search.

108. Another consumer informed Paddle in March 2021: "I am only grateful that it was an 0800 [sic] number, given the duration of the call! I expected it to be an automated [activation] call, but was subjected instead to a very (and I mean VERY!) long monologue on the part of the so-called 'Support' person who, instead of providing the license key, spent the next hour taking a tour of my computer and effectively telling me that I really needed to upgrade/renew etc etc, none of which had any bearing at all on the reason for my call."

109. In May 2021, another consumer wrote: "Your rep. tried to sell me a $299 tech support for Microsoft issues. The fact is that Microsoft tech support is free with most Microsoft 365 Office software…. I will not be swindled into buying expensive technical support for issues that can be resolved by a high school student."

110. Paddle routinely responded to these complaints by issuing a refund to the consumer for the initial software purchase, typically $30 to $60, but disclaiming responsibility for the larger charges associated with Reimage's deceptive telemarketing sales.

111. Throughout 2020 and 2021, Paddle's customer support and account management team discussed how to address consumer complaints calling Reimage a "fraud and a hoax" or "reprehensible and predatory," and demands from consumers that Paddle investigate Reimage and stop doing business with this seller "as your customers are being scammed on your phone line."

112. In or around June 2021, Paddle's account manager warned Reimage that consumers were complaining to Paddle about Reimage's call center and reporting that the technical support service being offered were "scam calls." Paddle account managers would remark when seeing these Reimage consumer complaints, "another case of phone scam as it seems."

113. In August 2021, Paddle's account manager reported the problem of Reimage's deceptive telemarketing to Paddle's management: "We regularly have buyers reaching out complaining about Restoro as they've reached out to Restoro because the app wasn't working or so. Restoro then provides additional support to solve the issue but usually charges (not through Paddle) an additional support fee. I've always forwarded these to [Reimage] to investigate and give us feedback what happened. We've also asked risk to look into this, but I don't think they came back with anything." Even though Reimage's deceptive telemarketing persisted well after this report, Paddle continued to process consumer charges for Reimage without investigating Reimage's sales practices.

114. In December 2021, an anonymous Reimage software purchaser wrote to Paddle's risk team to report that Reimage was operating a call center in the Philippines and asked Paddle to "blacklist" the company. The purchaser sent to Paddle's risk team publicly available complaints about Reimage posted on a Microsoft user forum and Reddit. Paddle's risk team also saw at this time that Malwarebytes Labs—a popular third-party anti-malware software developer—had flagged Reimage's software program as a "Virus." Paddle's risk team reported internally that there were complaints, red flags, and evidence of deception, including reports that Reimage was engaged in deceptive telemarketing ("they are [telling consumers that] ad tracking cookies are viruses") and using pop-up ads impersonating Microsoft or other antivirus companies.

115. In April 2022, the anonymous buyer wrote to Paddle's general counsel with the email header "Scam Call Centre" and reported:

> A company known as Restoro … is a known scam organization which is based in the Philippines, their original name was ReimagePlus. They are selling software that is scareware which makes people think there is a non existent problem with their computer, which trick [sic] the person into buying this

> software which does absolutely nothing. I hope that you blacklist / terminate their account with you and stop them from being able to scam anymore people.

The email was forwarded to the Paddle risk team that looked at Reimage several months earlier. That team recommended that Paddle should "open a review and see what the seller has to say."

116. Despite these reports and escalation to Paddle's risk team and legal counsel, Paddle did not halt or suspend the Reimage accounts pending this investigation. Instead, Paddle increased its annual processing volume for Reimage from about $14 million in 2021 to over $18 million in 2022. By 2022, Reimage became a top five seller for Paddle and was consistently processing nearly $1.2 million a month in sales through Paddle.

117. Paddle received complaints from many consumers reporting that the "Restoro" and "Reimage" branded software programs were malicious programs and damaging the consumers' computers and corrupting their operating systems. In October 2020, a Paddle account manager relayed in an internal group chat for Paddle's sales support team: "… do you know if [Reimage] is aware of any known issues with their product causing damage to a user's PC? We're still receiving a fair few complaints regarding this. In the meantime, I think what we're doing is the best solution (i.e. authorizing a refund for these type of complaints to avoid any legal battles)." Paddle continued to receive similar complaints well after October 2020. To address these complaints, Paddle instructed its customer support agents to issue a refund to prevent further escalations.

118. Many consumers also complained to Paddle about receiving unauthorized charges from Paddle for Reimage's services, and often that the consumer's credit card information had been compromised and passed onto unrelated third parties without the consumer's consent. For example, in January 2021, a consumer complained that the credit card data provided to Paddle for a Reimage software purchase had been passed to "other firms in the UK … who used it for

fraudulent transactions," that the consumer had "written this to [P]addle quite a number of times and … don't understand why you obviously didn't look into that and/or react to it," and warned Paddle again that "your payment system is not safe."

119. In February 2021, Paddle's customer support staff reported in connection with another consumer complaint: "The buyer is claiming that a Reimage technician used their credit card to purchase something worth $135.54. This was refunded but he would like to know who processed the charge as he considers this a theft/fraud." Paddle routinely dealt with such complaints by issuing a refund for the initial software purchase and closing the ticket.

120. According to Paddle's customer database, there were thousands of customer "tickets" from purchasers of the "Restoro" branded software program in Paddle's system reported as "Unknown Charge" in 2021. Moreover, a substantial portion of chargebacks—30% to 40%—that these Restoro purchasers initiated were also classified by Paddle as "unauthorized."

121. Similar to PC Vark, there were multiple months when monthly chargeback rates for one of Reimage's accounts at Paddle—i.e., the account Reimage opened to process sales of the "Restoro" branded software program—were well above 1%. In early 2022, chargeback rates on this Reimage account climbed to over 2% in multiple consecutive months. Paddle, however, conducted no investigation to determine the root cause of Reimage's chargeback problems. Instead, Paddle substantially assisted and shielded Reimage from the acquirers' and card networks' monitoring by aggregating Reimage's consumer charges with the charges of thousands of unaffiliated sellers.

122. Paddle also assisted Reimage to mask its chargeback problems by using chargeback prevention tools (such as third-party chargeback prevention services, Ethoca and

Verifi) to artificially lower Reimage's actual cardholder dispute rates and issue immediate refunds.

123. In July 2022, Paddle's risk team prepared an internal report showing Paddle's clients with "high fraud rate" and "ones we can offboard." The report showed that chargeback rates on one of Reimage's accounts at Paddle averaged over 3% from January 2022 to June 2022, and that Reimage was one of the top sellers causing chargeback problems for Paddle's merchant accounts. Paddle's account manager reached out to Reimage to inquire about the high chargeback rates but received no explanation. Paddle did not probe further. Instead, Paddle assured Reimage that Paddle is working on "how we can manage chargebacks in a better way for you."

124. Indeed, Paddle informed Reimage that Paddle would be using "chargeback prevention" tools to keep Reimage's chargeback rates at a low rate to avoid detection by the card networks. As Paddle told Reimage, "[w]e utilize third-party tools to issue warnings when a transaction has a high risk of turning into a chargeback before the dispute actually happens. In the event we receive an alert, we automatically refund the transaction to the original card, to avoid receiving a chargeback…. This will not affect your chargeback ratio and helps keep your account's dispute ratio within an acceptable threshold."

125. The credit card network rules require merchants that exceed a certain annual sales threshold to sign a "direct merchant agreement" with an acquirer. Currently, Visa's volume threshold is $1 million in annual sales volume for merchants that process through Visa. The acquirer must also have a contract with the specific payfac sponsoring the high-volume merchant. The purpose of these requirements is to ensure that the merchant's transactions are more closely monitored by the acquirer. Even before onboarding Reimage, Paddle expected the

annual revenues for Reimage to exceed the card networks' annual sales volume thresholds. At the time Paddle onboarded Reimage in 2020, these volume thresholds were set at $100,000 in annual sales for Visa and $1 million in annual Mastercard charges for Mastercard.

126. By early 2021, Reimage was already generating over $1 million a month in sales through Paddle alone. Paddle's account management team also saw that Reimage was processing substantial sales volume through other payment processors. Moreover, Reimage had not signed a direct merchant agreement with any acquirer that had a contract with Paddle. Thus, even if Paddle had registered and were authorized to operate as a payfac by the card networks, it still would not have been permitted to "sponsor" and process payments for Reimage.

127. The card network rules also require payfacs to contract only with a sponsored merchant located in the same country as the acquirer. Paddle knew that Reimage was registered as an Isle of Man entity, and later re-domiciled in Cyprus, with employees in Israel and a call center in the Philippines. Paddle also knew that a large segment of Reimage's customers were in the U.S. By standing in as the "merchant of record" and opening merchant accounts with registered payfacs based in the U.S., Paddle gave Reimage unfettered access to the card networks and ability to charge consumers in the U.S.

128. In sum, Paddle knew that Reimage was engaged in deceptive marketing practices, including deceptive telemarketing. Despite this knowledge, Paddle continued to process consumer charges for Reimage. Further, by submitting and aggregating Reimage's charges with thousands of unaffiliated sellers through Paddle's own merchant account, Paddle substantially assisted Reimage to evade scrutiny and monitoring by acquirers and the card networks. Additionally, Paddle's aggressive use of chargeback prevention companies, while disregarding

the consistent stream of consumer complaints and other signs of Reimage's deception, helped to further hide Reimage's true chargeback rates from the card networks and acquirers.

Paddle Received Numerous Warnings About Processing for Tech Support and Other High Risk or Prohibited Sellers

129. Some of the registered payfacs that Paddle has contracted with, such as Stripe and Adyen, and acquirers, such as Wells Fargo Bank, N.A. ("Wells Fargo"), have had policies either restricting or prohibiting their clients from processing charges for transactions involving certain goods or services, such as remote technical support services, "counterfeit goods," or goods sold through negative option marketing (especially with poorly disclosed terms) or through telemarketing. Both PC Vark and Reimage fall into those categories.

130. Despite its knowledge of these restrictive policies, Paddle has used its merchant accounts to process charges for such restricted or prohibited transactions through the registered payfacs and Wells Fargo, while also helping the sellers involved in those transactions avoid scrutiny and detection by the card networks. Also, while many of the tech support sellers onboarded by Paddle are not based in the U.S., Paddle has allowed these sellers to use Paddle's services to facilitate cross-border transactions with U.S.-based consumers for years.

131. Even when confronted with evidence from the card networks or payment processors that several of its clients were engaged in fraud or deceptive conduct, Paddle often did not immediately halt processing charges for these sellers.

132. In or around November 2017, for example, Microsoft and the International AntiCounterfeiting Coalition ("IACC") informed a registered payfac that contracted with Paddle that one of Paddle's clients was selling counterfeit software to consumers. IACC is a non-profit organization with a stated mission to combat product counterfeiting and piracy. When this report was brought to Paddle's attention, Paddle's founder and CEO at the time told the payfac that

Paddle did not find any concerns when the seller's website was initially "audited" but that Paddle would be terminating the seller to respond to the payfac's concerns.

133. Internally, Paddle's executives at the time referred to this seller as a "fake Microsoft reseller" and noted that this was a "wake up call as the current system of checks and balances … had fallen down." Despite these alarms, Paddle re-activated this same seller's account about a year later and continued to receive complaints about its sales practices. One Paddle risk analyst remarked internally that the seller was a "nuisance" but "considering the high [transaction volume] they're bringing to the company, we've had no other choice but to re-activate the account but monitor closely."

134. Separately, in November 2017, Paddle learned that Visa's chargeback monitoring program was identifying transactions based on individual merchant billing descriptors. In effect, Visa at this time was flagging Paddle's merchant billing descriptors associated with various tech support sellers due to excessive chargeback disputes. In response, Paddle changed its billing descriptors so that Visa would identify only Paddle as the merchant associated with the chargebacks being generated and thus "aggregate all of [Paddle's] disputes and sales within a given month," instead of by individual sellers. In so doing, Paddle was able to mask the chargeback rates for all of Paddle's clients (including PC Vark at this time) from Visa and make it difficult for Visa to detect the chargebacks associated with those sellers.

135. Paddle has known for years that the tech support sellers it has onboarded pose a substantial risk of fraud and excessive chargebacks. During an internal board meeting held in July 2018, Paddle executives noted that sellers "using CPC [cost per click advertising, e.g., pop-up ads] to sell anti-virus software or those offering system benefits" are responsible for causing excessive chargeback rates on Paddle's merchant accounts, and that the main reason for their

high chargeback rates was "aggressive marketing tactics." Paddle's internal risk management team created a special label for problematic sellers that Paddle continues to do business with, called "dodgy dealers." Paddle's risk team described these sellers as "the pain in the ass, good for nothing, scum of the earth dodgy vendors who take up our time." In October 2022, Paddle's executives again remarked: "Our customer base exposes us to a relatively high volume of chargebacks, a significant proportion of which is fraud."

136. In early 2020, Paddle received warnings from payfac Adyen, which processed one of Paddle's merchant accounts, that another one of Paddle's tech support sellers was found to be impersonating Microsoft in marketing their services and using "fake false positives in order to convince customers to purchase the [paid] version of their [software] programs." Adyen warned Paddle that Visa deemed this to be a "scam" and a violation of its rules, and further noted that "[a]side from the IP infringement and the scam this vendor has a very dubious reputation, as we discovered ourselves via quick Google searches." Paddle tried to assure Adyen that Paddle's internal "investigation" did not reveal any issues with the seller and insisted that the seller was "legitimate." Paddle claimed that it was the seller's affiliates who were using "misleading practices to drive traffic to the Seller's website." Adyen conducted its own investigation and reported to Paddle that, contrary to Paddle's claim, the seller itself was using deceptive affiliate marketers to lure consumers to its website.

137. In June 2020, Adyen contacted Paddle again to report that Visa and the acquirer Wells Fargo had been reviewing Paddle's business model and "have reason to believe that Paddle is acting as a[n] [unauthorized] Payment Facilitator." Visa and Wells Fargo rejected Paddle's claim that it was a "reseller" and the "merchant of record," because consumers' orders

were being fulfilled by the software providers that Paddle was processing charges for, and all product support questions were routed to the software provider and not to Paddle.

138. Adyen also expressed concerns about whether "Paddle was reselling for entities that are unqualified or utilize deceptive practices that are not supported" by the acquirer and the card network rules. Ultimately, Adyen decided to terminate Paddle's merchant account as Adyen continued to find additional problematic sellers in Paddle's client portfolio, including those suspected of trafficking illegal pharmaceuticals under the guise of selling software. Adyen told Paddle that the termination was due to ongoing failures by Paddle to effectively screen and monitor its clients, and that "unfortunately the volume and extent of the violations notified by Visa leaves us no other choice."

139. When Paddle learned of Adyen's decision to terminate Paddle's merchant account, Paddle quickly sought out other payfacs—such as Checkout.com and Worldpay—through which to continue its payment aggregation practices. In its applications to open merchant accounts with these payfacs, Paddle continued to falsely claim that it was a "reseller," that Paddle did not remit consumer payments to the software providers, and that Paddle was ultimately responsible for the delivery and fulfillment of the software products and services.

140. In September 2020, Paddle was warned by an outside consultant that if Paddle were in fact a software reseller and the actual "merchant of record," that "leaves [Paddle] with 100% of all risk and ultimate compliance obligations." The consultant also warned Paddle's executives that "'best efforts' are not normally good enough as any simple standalone merchant would have full knowledge and control over what they sell and as Merchant of Record, you should know the same." Paddle's executives acknowledged that as the "merchant of record," "we need to have knowledge and control over everything that we are selling." However, Paddle

made no changes to its business. Instead, Paddle continued to operate as a payment aggregator, while, in its interactions with consumers, continuing to disclaim responsibility for those sellers' products and deferring product-related questions to the sellers.

141. Throughout 2022, Paddle received numerous warnings from payfac Stripe that its merchant accounts had been put on the card network's fraud and chargeback monitoring programs. Despite Paddle's use of an aggregated merchant account to mask and dilute certain sellers' high chargeback rates with thousands of other sellers whose payments were also processed through that account, the overall chargeback rates from the account grew so high that Paddle's merchant account had again exceeded the credit card networks' chargeback monitoring thresholds.

142. In May 2022, for example, Stripe notified Paddle that its merchant account was placed on Mastercard's Excessive Fraud Merchant Program due to excessive chargebacks over the prior three months. When Stripe asked Paddle to look into the sellers driving up the monthly chargeback rates—which included Reimage—and provide a remediation plan to avoid fines by the card networks, Paddle responded by promising to lean more heavily on chargeback prevention vendors to help stave off chargeback disputes.

143. In September 2022, Stripe notified Paddle that its merchant account was again flagged, this time placed on Visa's Fraud Monitoring Program, due to fraud disputes initiated by cardholders and asked Paddle to provide "root cause/remediation insights" for the account in question. Reimage, again, was one of the merchants responsible for driving up Paddle's collective chargeback rate. Paddle responded by assuring Stripe that Paddle had changed its chargeback prevention alert settings to enable Paddle to more expediently "refund the transactions before a chargeback hits" and that Paddle was exploring other tools to improve its

early detection of cardholder disputes. Stripe's repeated warnings did not cause Paddle to audit or terminate any of the high-volume sellers responsible for Paddle's consistently high chargeback rates, such as Reimage.

144. In September 2022, the FTC issued a Civil Investigative Demand to Paddle, notifying Paddle that the FTC is investigating Paddle for violations of the FTC Act and the TSR in connection with its payment processing practices.

Paddle's Representations Regarding Its Merchant of Record or Reseller Services

145. Paddle is a business that collects money from consumers on behalf of Paddle's clients under the Paddle name. When tech support products or services are purchased by consumers through Paddle, consumers receive an invoice from Paddle confirming the purchase, as illustrated in Figure 8 below. The charges on consumers' credit card statements include the name Paddle or Paddle.net.

146. In their communications with Paddle's clients, consumers, card networks, banks and payment processors, Paddle claims that it is the "merchant of record" or "reseller" in the sales transaction with consumers. According to Paddle, "[w]hen the transaction is complete, it's the merchant of record that is the principal in the transaction and it is their name that appears on the customer's credit card statement and to whom the cardholder has recourse in case of any dispute. This is how and why the merchant of record becomes the liable party." Thus, according to Paddle, Paddle is liable for the sales conducted when it undertakes to process transactions as the "merchant of record" or "reseller."

147. Indeed, Paddle has represented to payment processors that, as the "merchant of record" or "reseller," Paddle takes "full responsibility and risk for the sale," that Paddle has "primary obligation to [consumers] to provide the product and remains liable to [consumers] for

the products that it sells," and that all consumers "have direct and full recourse against Paddle for any issues with the products…."

Paddle's Negative Option Billing Practices

148. From at least April 2020 to July 2023, consumers who purchased software from Reimage through Paddle's online checkout process were enrolled in a subscription plan with a recurring annual charge. Many consumers were unaware of these annual charges when they purchased the software.

149. The purchase of the "Restoro" and "Reimage" branded software programs typically began at the merchant's website, where the consumer was presented with an option to select a "Basic – One time use" plan for $27, a "Premium – 1 License, Unlimited Use 1 Year" plan for $41, or an "Extended – 3 Licenses, Unlimited Use 1 Year" plan for $58. As shown below, none of these selections disclosed that the consumer would be enrolled in an auto-renewing subscription plan with annual fees.

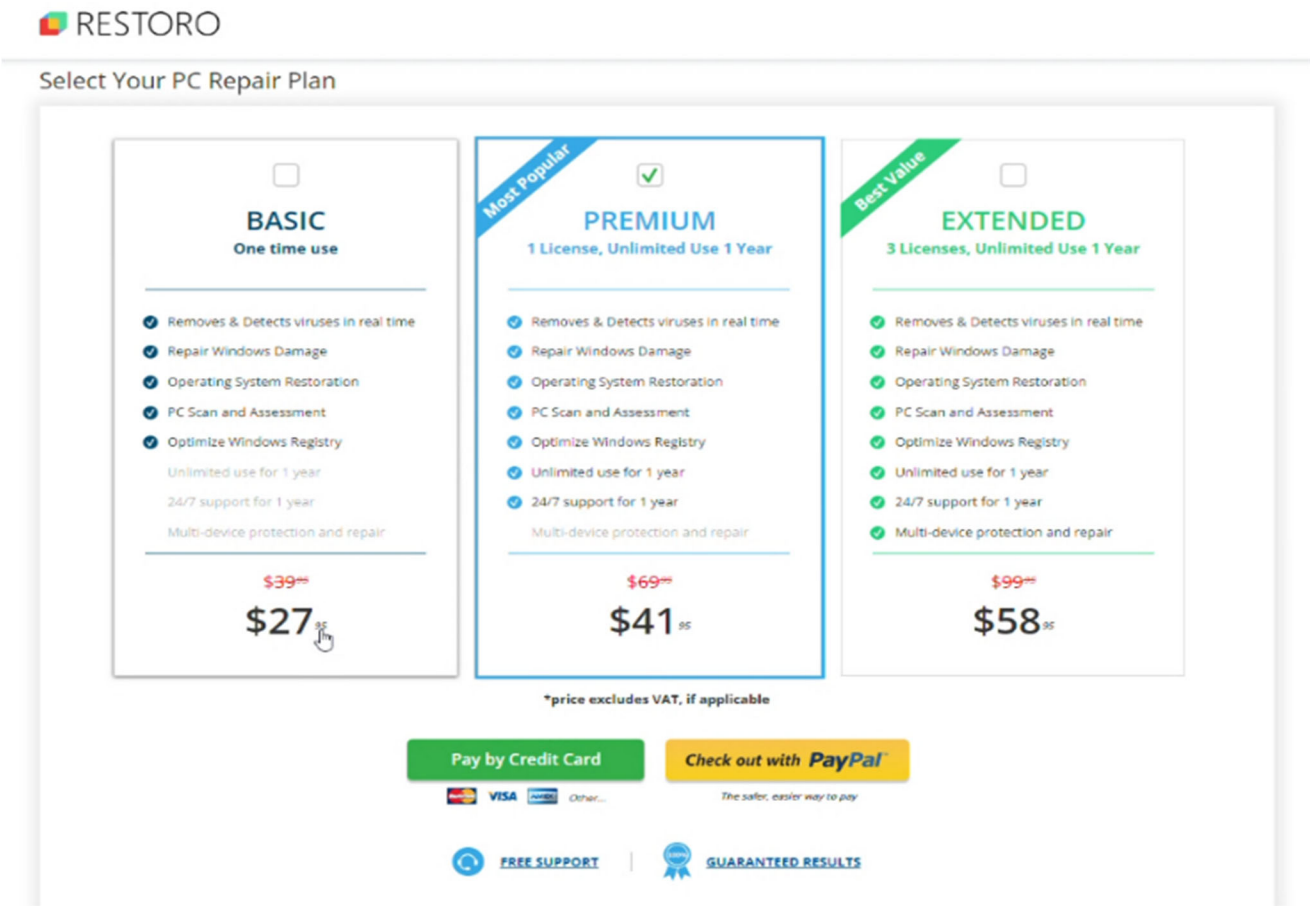

Figure 3: Reimage's product plan selection page (www.restoro.com/pricing)

150. At the very bottom of Reimage's initial product plan page was an inconspicuous "Terms of Use" hyperlink. That hyperlink, if clicked, led to a webpage with a lengthy recital. In the middle was a section titled "Auto-Renewals," which stated: "Some of our packages include yearly recurring payments." Not only was this disclaimer buried in fine print and hard to find, it also did not specify what products or packages were subject to auto-renewals, or the prices or amount of any renewal charges.

151. Once the consumer selected a plan and the option to pay by credit card or PayPal, the product was added to the consumer's virtual shopping cart and the consumer was routed to a series of checkout pages created and controlled by Paddle.

152. In the first step of the checkout process, Paddle displayed a pop-up box stating

"Purchase **Restoro 1 Year**" on the top and an option to click a box to receive product updates by email, as shown in the image below. The pop-up did not explicitly require the consumer to affirmatively authorize an auto-renewing subscription plan. At the bottom, the pop-up stated, "Your total is $41.95" and, below that in a smaller font, "Then $41.95 per/year." The pop-up provided no explanation of the terms of the subscription plan.

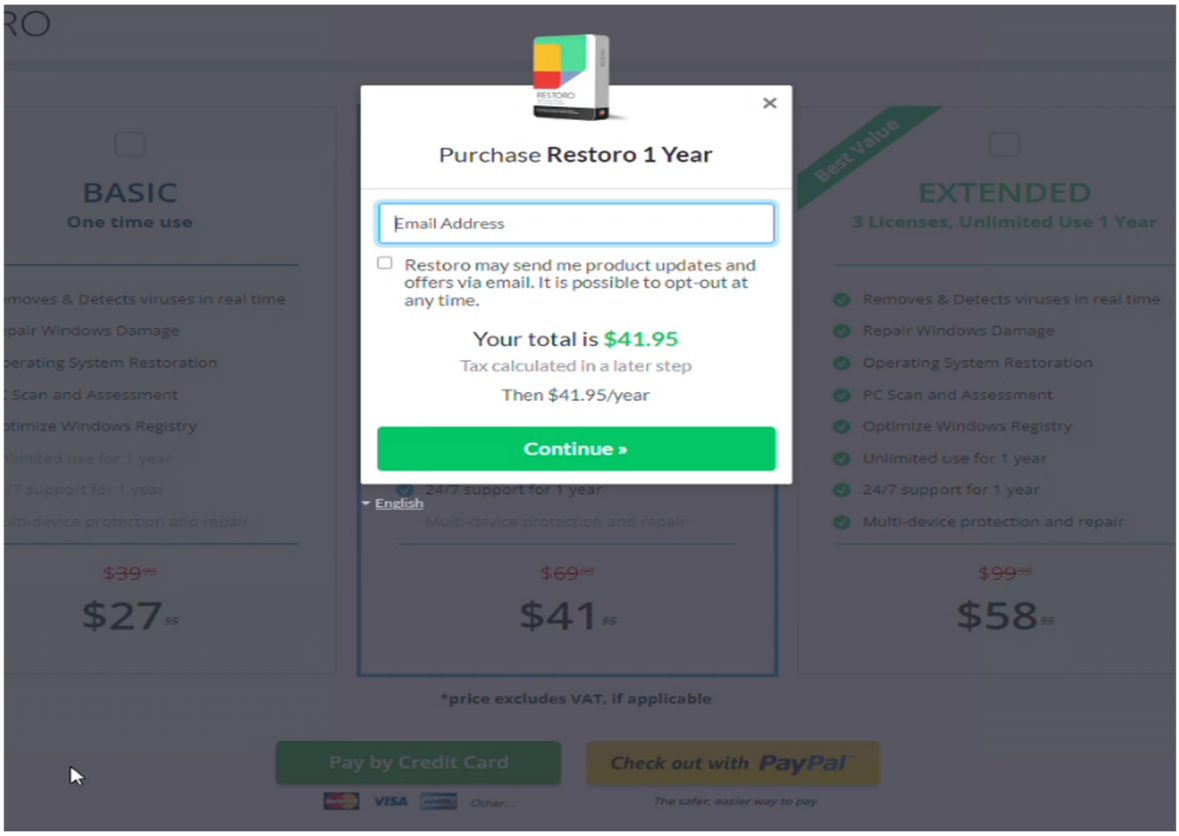

Figure 4: Close-up view of Paddle checkout window #1

153. Clicking the "Continue" box on the pop-up led consumers to another pop-up that prompted consumers to enter their zip code. Here too, there was no mention of any renewal charge or enrollment in a negative option plan.

154. Clicking the "Continue" box on that second pop-up directed consumers to a third pop-up, as shown in the image below, which stated, "Purchase Restoro 1 Year" and provided a calculation of the total purchase after tax.

155. At the bottom of the pop-up, in smaller font, it stated "Then $44.47/year." Here too, consumers were not given an option or box to click to affirmatively enroll in an auto-renewing subscription plan and were not provided with the terms of the plan. The pop-up directed consumers to pay by credit card or by PayPal.

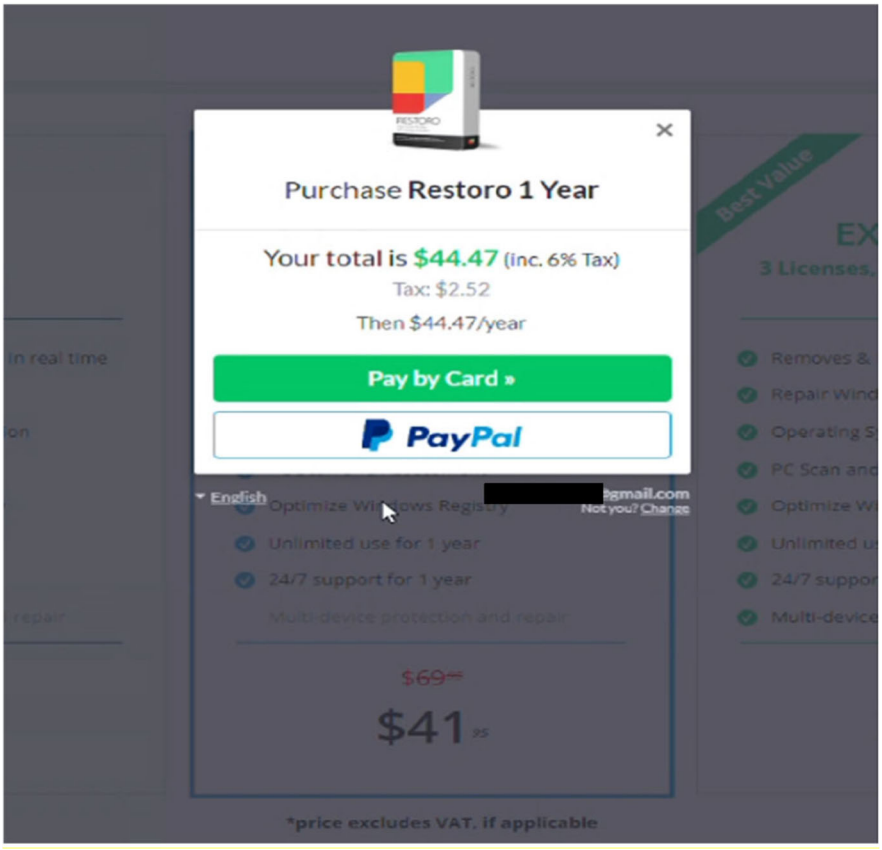

Figure 5: Close-up view of Paddle checkout window #2 (email address redacted)

156. Once consumers selected the method of payment, they were directed to enter their payment information, as shown in Figure 6 below. Once consumers selected "Subscribe Now," Paddle charged the consumers for the software purchase (in this example, the $44.47 for the Premium Plan). Unbeknownst to many consumers, in clicking the "Subscribe Now" button, the consumers were enrolled in a negative option plan for Reimage with an annual recurring charge.

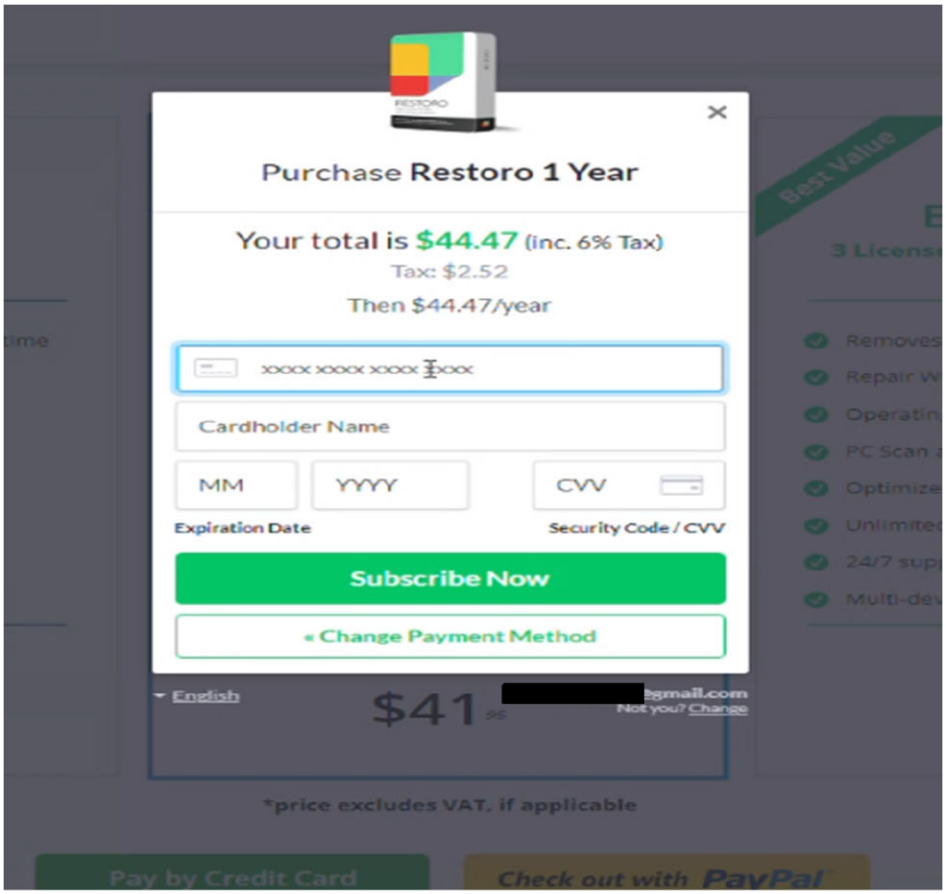

Figure 6: Close-up view of Paddle checkout window #3 (email address redacted)

157. In the final step of the checkout process, consumers were directed to a payment confirmation page. The payment confirmation page at Figure 2, above, directed the consumer to call a toll-free telephone number to "activate" the software. This confirmation page also did not disclose the terms of the negative option billing plan.

158. At the bottom left corner of Paddle's checkout window, the Paddle logo appears along with the statement, in small print, that "This order process is conducted by our online reseller & Merchant of Record, Paddle.com, who also handle [sic] order related inquiries and returns. Your data will be shared with Restoro for product fulfilment," as appears in the image below.

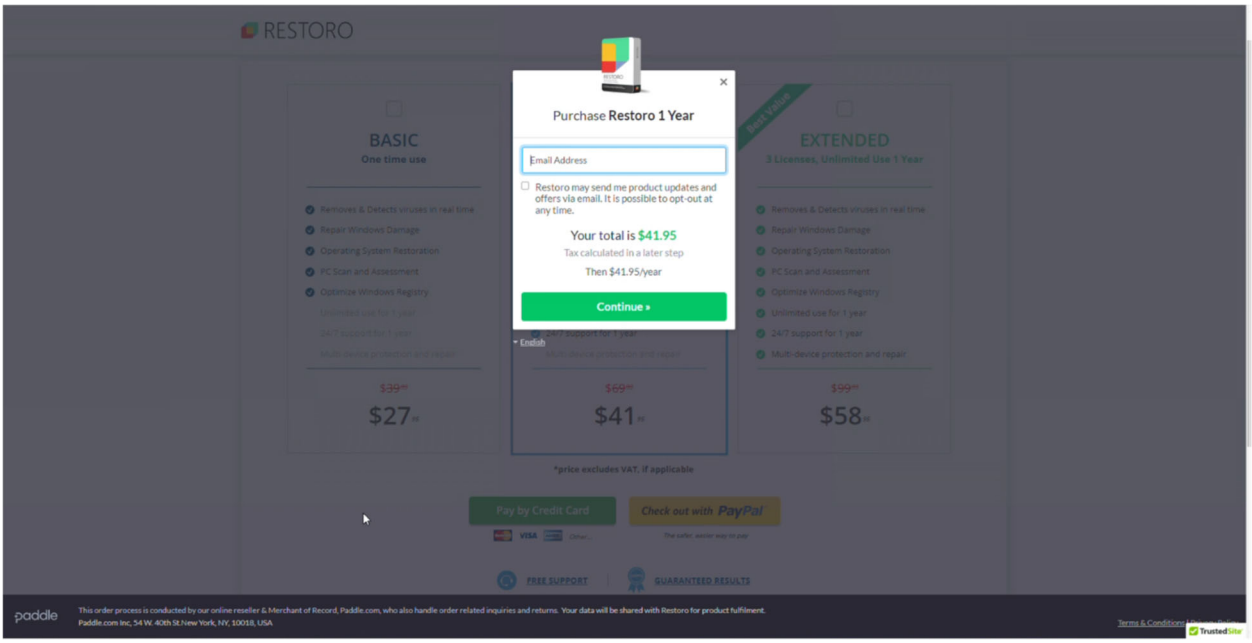

Figure 7: Paddle checkout window #1 (www.restoro.com/pricing)

159. At the far bottom right of the Paddle checkout window, was a small hyperlink to Paddle's own terms and conditions page. If a consumer clicked on that link, they would be directed to another lengthy recital of disclaimers, and buried in the middle of this lengthy recital is the statement: "Paid Subscriptions automatically renew until cancelled…. If you wish to cancel your subscription, please contact us here [i.e., hyperlink to paddle.net/contact] at least 48 hours before the end of the current billing period." Consumers who clicked on the link were directed to Paddle's Kino "bot" that purported to assist the consumer with order lookups and process common requests.

160. Paddle's checkout process for the purchase of the "Reimage" branded software program was substantially similar to the process discussed above.

161. After the purchase of the "Restoro" or "Reimage" branded software program, Paddle did not promptly notify consumers that they were enrolled in a subscription with automatic annual charges. Paddle often sent consumers a purchase receipt by email, but that receipt did not disclose the automatic annual charges. Instead, as shown in the image below, the

receipt conveyed the impression that the term of the purchase was for one year, as it stated "Restoro 1 Year."

paddle

Receipt PAID

Receipt to

Receipt from

Paddle.com Inc
3811 Ditmars Blvd #1071
New York, 11105-1803
Astoria
United States

Your order

USA 85260
Order Number / Receipt: #38009574-48025796
Billing date: Jun 10, 2022

Payment method: Visa card ending [redacted]
Currency: USD

	Billing period	Quantity	Price
Restoro 1 Year	Jun 10, 2022 - Jun 9, 2023	1	US$41.95
Sales Tax (8.05%)			US$3.38
YOUR ORDER			US$45.33

The US$45.33 payment will appear on your bank/card statement as:
PADDLE.NET* RESTORO

If you have a problem with your order (e.g. don't recognise the charge, suspect a fraudulent transaction), please visit paddle.net.

paddle

Figure 8: Electronic receipt of "Restoro 1 Year" purchase in June 2022 (card number redacted)

162. At times, Paddle sent consumers a renewal "reminder" email approximately two weeks before the annual renewal date. For many consumers, that was the first time they were made aware of the automatic annual charges and that they had been enrolled in a negative option billing plan. However, many other consumers, not expecting such charges, overlooked these "reminder" emails and failed to cancel their subscription before the charges posted.

163. When a consumer purchased a "Restoro" or "Reimage" branded software program and entered their billing information, as illustrated above, that information was collected and retained by Paddle. Paddle collected and stored this confidential customer information so that Paddle could post renewal charges to the consumer's account. Paddle also exercised control over the cancellation process and issuing refunds and directed consumers to contact Paddle directly to resolve any fraudulent and unauthorized charges and other billing issues.

164. Paddle routinely received complaints from consumers and knew that consumers constantly complained about incurring unwanted and unauthorized renewal charges. Starting in 2021, when the annual recurring charges for the "Restoro" and "Reimage" software purchases began to appear on consumers' credit card statements, Paddle began receiving an influx of complaints and demands for cancellations and refunds. For example, one consumer wrote in 2021: "At the time (maybe 12 months ago) I believed I was agreeing to a one-off charge in order to evaluate the service. Evidently the Restoro's App did not present the user with clear payment options in this regard. Was this Restoro's poor presentation or was it intentional trickery?" Another consumer wrote in January 2023: "I had no idea this was a subscription that would auto renew as I cannot accept these, we have to have approval for every spend I make – and nothing was requested or approved for this renewal."

165. In July 2022, a Paddle account manager informed Reimage that Paddle's internal risk and compliance team "have been approached" about the issue where buyers believed they were making a one-time purchase, instead of being enrolled in an annual subscription. He noted that this negative option billing practice was making certain employees at Paddle "nervous" and "might be confusing to consumers when purchasing."

166. Paddle received complaints from consumers about its failure to provide a simple online cancellation mechanism for the "Restoro" or "Reimage" software subscriptions, and that consumers' cancellation requests were being ignored. As one consumer told Paddle in 2022, "you advised that the unwanted and non requested one year subscription was cancelled. On the same date you billed me via American Express $107.46. I did not sign up nor approve for this extended service and request that you promptly reimburse or cancel this charge."

167. In 2022, Paddle conducted an annual revenue performance review of Reimage's accounts and found that there were over 80,000 customer support tickets opened in 2021 for these accounts. Of these support tickets, customer cancellations accounted for about 46% of all tickets (about 37,300 tickets) and refunds accounted for nearly 22% of all tickets (17,800 tickets). In October 2022, Paddle's founder and CEO at the time circulated an internal report to the Paddle board noting that for Paddle's merchants generally, "about 50 to 60% of fraud comes from recurring payments (merchant initiated subscriptions, rather than customer-present card transactions)."

168. Despite numerous customer complaints and high rates of cancellations and refund demands, Paddle did not change the checkout process for the "Restoro" and "Reimage" software purchases. Instead, Paddle employed tactics to increase the chance that subscriptions would be renewed. For example, Paddle used an "automatic credit card updater"—a workaround for a bank's potential rejection of expired credit cards of Reimage's customers by obtaining updated credit card details directly from the banks—rather than requesting the customers to update their own card information, before the recurring charges are posted.

169. Moreover, Paddle has known since at least 2020 that consumers who were asked to update their card information for autorenewals generally opted to cancel rather than update

their card information. An account manager at Paddle even advised a Paddle client in August 2020 not to send notification emails to consumers about their expired cards.

170. Paddle continues to charge consumers using negative option billing plans without clearly and conspicuously disclosing the terms and conditions of the plans, such as the terms and duration of the billing plan or how to cancel the plan, and without obtaining consumers' informed express consent.

* * *

171. 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 of, among other things, Defendants' history of processing consumer payments for deceptive tech support merchants, Defendants' continued involvement in the business of payment processing, Defendants' continued payment aggregation practices despite knowledge of the consumer harm Paddle has caused, Defendants' participation in unlawful subscription billing practices, and the ease with which Defendants can engage in similar conduct.

VIOLATIONS OF SECTION 5 OF THE FTC ACT

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

173. 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 Practices

174. In numerous instances, Defendants have (a) opened and maintained payment processing accounts for merchants engaged in deceptive practices, (b) processed transactions to consumers' accounts for merchants engaged in deceptive practices, (c) disregarded evidence of deceptive activity on merchant accounts that Defendants opened or maintained, often taking steps to shield deceptive merchants from further scrutiny, or (d) used their merchant accounts to process payments for unaffiliated merchants or entities engaged in deceptive practices.

175. 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.

176. Therefore, Defendants' practices as described in Paragraph 174 constitute unfair acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. §§ 45(a) and 45(n).

COUNT II

Misrepresentations to Consumers (Pled in the Alternative)

177. Defendants have submitted credit card charges for tech support products through merchant accounts held in Defendants' name, identifying themselves to payment processors, acquiring banks, consumers, and the card networks, as the "reseller" or "merchant of record" and taking full ownership of the charges processed through Defendants' merchant accounts. Defendants also entered into agreements with PC Vark, Reimage and other tech support software providers, and claim to being the reseller or merchant of record in the transactions with consumers.

178. In numerous instances in connection with the offering for sale of tech support

products or services, Defendants have represented, directly or indirectly through PC Vark, Reimage and other tech support providers, expressly or by implication, that they have identified significant performance or security problems on consumers' computers, including that consumers' computers are infected with a virus, and that the tech support provider is associated with legitimate companies, such as Microsoft or McAfee.

179. In truth and in fact, in numerous instances in which Defendants, directly or indirectly, have made the representations set forth in Paragraph 178, Defendants have not detected significant performance problems, security problems, or viruses on consumers' computers and the tech support providers were not associated with legitimate companies, such as Microsoft or McAfee.

180. Therefore, Defendants' practices as described in Paragraph 178 constitute deceptive practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(a).

VIOLATIONS OF THE TELEMARKETING SALES RULE

181. 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.

182. PC Vark and Reimage are sellers or telemarketers under the TSR. A "seller" means any person who, in connection with a telemarketing transaction, provides, offers to provide, or arranges for others to provide goods or services to the customer in exchange for consideration. 16 C.F.R. § 310.2(dd). A "telemarketer" means any person who, in connection with telemarketing, initiates or receives telephone calls to or from a customer or donor. 16 C.F.R. § 310.2(ff).

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

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

185. 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 III

Assisting and Facilitating Deceptive Telemarketing

186. 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.

187. Therefore, Defendants' acts or practices as set forth in Paragraph 186 violate the TSR, 16 C.F.R. § 310.3(b).

VIOLATIONS OF THE RESTORE ONLINE SHOPPERS' CONFIDENCE ACT

188. In 2010, Congress passed the Restore Online Shoppers' Confidence Act, 15 U.S.C. §§ 8401–05, which became effective on December 29, 2010. Congress passed ROSCA because "[c]onsumer confidence is essential to the growth of online commerce. To continue its

development as a marketplace, the Internet must provide consumers with clear, accurate information and give sellers an opportunity to fairly compete with one another for consumers' business." Section 2 of ROSCA, 15 U.S.C. § 8401.

189. Section 4 of ROSCA, 15 U.S.C. § 8403, states: "It shall be unlawful for any person to charge or attempt to charge any consumer for any goods or services sold in a transaction effected on the Internet through a negative option feature (as defined in the Federal Trade Commission's Telemarketing Sales Rule in part 310 of title 16, Code of Federal Regulations), unless the person … (1) provides text that clearly and conspicuously discloses all material terms of the transaction before obtaining the consumer's billing information; (b) obtains a consumer's express informed consent before charging the consumer's credit card, debit card, bank account, or other financial account for products or services through such transaction; and (c) provides simple mechanisms for a consumer to stop recurring charges from being placed on the consumer's credit card, debit card, bank account, or other financial account."

190. The TSR defines a negative option feature as: "in an offer or agreement to sell or provide any goods or services, a provision under which the consumer's silence or failure to take an affirmative action to reject goods or services or to cancel the agreement is interpreted by the seller as acceptance of the offer." 16 C.F.R. § 310.2(u). Defendants enroll and charge consumers through a negative option feature as defined by the TSR.

191. Pursuant to Section 5 of ROSCA, 15 U.S.C. § 8404, and Section 18(d)(3) of the FTC Act, 15 U.S.C. § 57a(d)(3), a violation of ROSCA constitutes a violation of a rule under section 18 of the FTC Act, 15 U.S.C. § 57a, and constitutes an unfair or deceptive act or practice in or affecting commerce, in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

COUNT IV

Illegal Negative Option Billing

192. In numerous instances, Defendants have charged consumers for tech support products or services sold online through a negative option feature while (a) failing to disclose, clearly and conspicuously, all material terms of the transaction before obtaining the consumer's billing information, (b) failing to obtain the consumer's express informed consent before making the charge, or (c) failing to provide a simple mechanism to stop recurring charges.

193. Defendants' acts or practices as set forth in Paragraph 192 are deceptive acts or practices that violate Section 4 of ROSCA, 15 U.S.C. § 8403.

CONSUMER INJURY

194. Consumers have suffered and will continue to suffer substantial injury as a result of Defendants' violations of the FTC Act, the TSR and ROSCA. Consumers are injured both by Defendants' initial charges and recurring charges. 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, the TSR, and ROSCA;

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: June 16, 2025

Sung Kim

Sung W. Kim
Russell Deitch

Federal Trade Commission
600 Pennsylvania Ave. NW
Washington, D.C. 20580
Tel. (202) 326-2211; Email: skim6@ftc.gov
Tel. (202) 326-2585; Email: rdeitch@ftc.gov

Attorneys for Plaintiff
FEDERAL TRADE COMMISSION