UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

LANZY KANDEH,

On Behalf of Himself and All Others Similarly Situated,

Plaintiff,

v.

Nordvpn S.A., Tefincom SA d/b/a NordVPN, and Nordsec B.V.,

Defendants.

Case No.: 25 Civ. 2571

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Lanzy Kandeh ("Plaintiff"), by his undersigned attorneys Wittels McInturff Palikovic and Milberg Coleman Bryson Phillips Grossman, PLLC, brings this consumer protection action in his individual capacity and on behalf of a class of New York consumers defined below against Defendants Nordvpn S.A., Tefincom SA d/b/a NordVPN, and Nordsec B.V. (hereinafter, "Nord Security," "Defendants," or the "Company") and hereby alleges the following with knowledge as to his own acts and upon information and belief as to all other acts:

INTRODUCTION

1. This proposed class action lawsuit challenging Nord Security's use of deceptive and illegal "automatic renewal" tactics to trick consumers into paying for unwanted, pricey subscriptions for Internet privacy and security products ("Nord Subscription"). Nord Security intentionally misleads consumers into thinking they can subscribe to privacy product offerings for a discrete period of time. The truth is, however, that Defendants' Nord Subscriptions automatically renew and the Company's "disclosures" regarding this feature are hidden from consumers both before and after purchase and fall far short of the legal requirements for such subscriptions. Further, Nord Security intentionally makes Nord Subscriptions difficult to cancel and fails to provide adequate notice of material changes to those subscriptions.

2. Nord Security offers a suite of products and services to consumers that claim to provide internet users with privacy and protection from cybersecurity threats. Those offerings include the data removal tool Incogni, which claims to "erase" consumers' personal data from "commercial databases" and "people search sites," a virtual private network ("VPN") service called "NordVPN,"[1] and a password manager called "NordPass."

[1] A VPN service is one that purports to protect a user's internet connection and online privacy. These services typically route a user's internet traffic through an encrypted tunnel to a server in

3. Potential customers are directed to Nord Security's website through online searches or the Company's advertising. Nord Security advertises widely: online, on numerous podcasts, in commercials, through influencer sponsorship and affiliate marketing on platforms such as YouTube, and through email marketing to existing or former customers. This advertising touts the benefits that Nord Security allegedly offers: for example, the Company describes the Incogni product as allowing consumers to "[p]revent scammers from finding your info in commercial databases," "[c]urb identity thieves," and "[e]njoy better protection against online stalking."

4. But while consumers enroll in Defendants' Nord Subscriptions for privacy and security, Nord Security is actually collecting their payments and payment information via deceptive and unlawful subscription practices designed to entrap consumers into paying unknown and/or unwanted recurring subscription fees. Indeed, that is exactly what happened here, where Plaintiff Kandeh enrolled in a Nord Subscription that he did not know would automatically renew and was then charged $119.08 for another year of that subscription that he did not want.

5. Nord Security's product offerings have a "negative option" feature, which the Consumer Financial Protection Bureau ("CFPB") defines as "a term or condition under which a seller may interpret a consumer's silence, failure to take an affirmative action to reject a product or service, or failure to cancel an agreement as acceptance or continued acceptance of the offer."[2] As the CFPB cautions, "[n]egative option programs can cause serious harm to consumers," which

---

another location, masking the user's location and protecting the user's data from interception along the way. Uses for VPNs range from casual entertainment (*i.e.*, using a VPN while abroad to watch a show that is only available in the U.S.) to the distribution of politically significant information (*i.e.*, masking journalistic sources within a totalitarian regime).

[2] Consumer Financial Protection Circular 2023-01, Unlawful negative option marketing practices (Jan. 19, 2023), https://files.consumerfinance.gov/f/documents/cfpb_unlawful-negative-option-marketing-practices-circular_2023-01.pdf.

"is most likely to occur when sellers mislead consumers about terms and conditions, fail to obtain consumers' informed consent, or make it difficult for consumers to cancel."[3]

6. Nord Security's subscription scheme hits the CFPB's warning trifecta. Due to the Company's deceptive and unlawful negative option practices, many consumers who sign up for Nord product offerings including NordVPN and Incogni ultimately end up paying for Nord Subscriptions that they do not want.

7. In order to prevent consumers from being deceived by negative option practices into paying for automatically renew subscriptions they do not want, in 2020 New York enacted its Automatic Renewal Law, G.B.L. §§ 527–527a, to "end the practice of ongoing charging" of consumer payment accounts "without the consumers' explicit consent." NY LEGIS 267 (2020), 2020 Sess. Law News of N.Y. Ch. 267 (S. 1475-A). As described below, Nord Security violated that law in multiple ways.

THE UNIFORM WEB OF NORD SECURITY'S NEGATIVE OPTION SCHEME

8. Nord Security traps consumers into unintended purchases with a web of deceptive online design features that exploit well-known shortcomings in consumer decision-making. The paragraphs below describe the various deceptive strategies Nord Security employs in the structure of its offerings. While each of the deceptive strategies is independently sufficient to trick consumers into making inadvertent purchases, taken together these components reveal an intentionally deceptive process that is designed to, and does, result in an unlawful outcome: saddling unwitting consumers with unwanted subscriptions.

9. Nord Security deceives consumers in at least six ways.

[3] *Id*. at 2.

10. First, during the enrollment process, Nord Security misleads consumers regarding the fact that its Nord Subscriptions automatically renew, the terms of any such automatic renewal, and the cancellation policy that applies to the offer. For example, instead of clearly explaining to the consumer what they are actually getting into, Nord Security offers consumers what appear to be time-limited plans and withholds the relevant (and inadequate) fine print that reveals otherwise until a customer reaches the payment step, where this "disclosure" is buried in a drop-down feature customers do not see unless they click on it. Nor does Nord Security obtain consumers' affirmative consent to the automatic renewal offer prior to charging consumers' payment cards or third-party payment accounts.

11. Second, Nord Security's scheme continues post-sign up. The post-purchase receipt email Defendants send to consumers after enrollment in a Nord Security subscription continues the deception began during enrollment and does not contain the automatic renewal offer terms that apply to the consumers' purchase. In fact, this email omits all information whatsoever on the need to cancel a Nord Security subscription to avoid additional charges (let alone information on how to do so), further misleading consumers into believing they have made a one-time purchase.

12. Third, Nord Security employs a highly unconventional charging practice. Rather than automatically renew consumers by charging their stored payment methods at the beginning of a new subscription period if they do not cancel before the prior subscription is over, Nord Security extracts its charges 14 days ***before the customer's current subscription period even ends***. By doing so, Nord Security locks consumers into another yearlong subscription well before any reasonable consumer would expect such a subscription to renew, allowing Nord Security to collect and keep payment from consumers who do not wish to remain Nord Security customers.

13. Fourth, Nord Security makes canceling exceedingly difficult and requires customers to figure out—with no help from the Company—that, to Nord Security, cancelling means the entirely unorthodox process of navigating Nord Security's account settings to find a buried feature labelled "turn off automatic renewal." If users manage to find this link and click it, they must navigate additional windows and click a minimum of two additional buttons and provide a reason for their decision and then navigate past large, colorful offers for promotional pricing or customer service assistance before Nord Security will process a cancellation. Upon information and belief, during the time that Plaintiff was a Nord Security customer, the Company's complicated cancellation process also included the message "Be sure to make a payment before [the end of this subscription period] to keep your account active"—falsely implying that automatic renewal had already been turned off, when the consumer actually had to complete an additional step in order for Nord Security to process the cancellation.

14. Fifth, Nord Security fails to provide sufficient notice under New York law that the customer's subscription will automatically renew at least 15 days, but no more than 45 days before the subscription automatically renews, because Nord Security's "notice" email fails to: (1) "include instructions on how to cancel" the automatic renewal contract; and (2) provide a "cost-effective, timely, and easy-to-use" cancellation mechanism, which Nord Security does not have.

15. Sixth, Nord Security fails to clearly and conspicuously disclose material changes to its customers' automatic renewal terms, and further fails to provide any information whatsoever about how to cancel a subscription in connection in material change communication, let alone information concerning a "cost-effective, timely, and easy-to-use" cancellation mechanism, which Nord Security does not have.

16. While a given customer may not be ensnared by each and every aspect of Nord Security's deceptive subscription web, all Nord Security customers face the same traps and need only be tricked by one of them to end up paying a hefty subscription fee for a year (or more) of internet security and privacy services they do not want.

17. These outcomes are not only unsurprising, but are in fact the result of Nord Security's intentional and bad-faith design choices. Nord Security is well aware that its scheme is tricking customers, as complaints about Nord Security are legion, with hundreds of consumers complaining directly to Nord Security or via sites like Trustpilot, SiteJabber, and Reddit. Upon information and belief, Nord Security experiences a high rate of chargebacks when consumers, frustrated by Nord Security's subscription scheme, initiate disputes through their credit card companies or other payment processors over unwanted Nord Security transactions. Upon information and belief, Nord Security has developed customer service protocols for dealing with customers complaining about unwanted subscription charges.

18. Nevertheless, despite the clear messages Nord Security's customers are sending, Nord Security continues to subject the consuming public to its unlawful subscription scheme and to reap significant monetary benefits from its unlawful conduct.

19. Only through a class action can consumers like Plaintiff Kandeh remedy Nord Security's unlawful practices. Because the monetary damages suffered by each customer are small in comparison to the much higher cost a single customer would incur in trying to challenge Nord Security's improper conduct, it makes no financial sense for an individual customer to bring his or her own lawsuit. Furthermore, many customers do not realize they are victims of Nord Security's unlawful acts and continue to be charged to this day. With this class action, Plaintiff

and the Class seek to level the playing field, enjoin Nord Security's unlawful business practices, and recover the charges Nord Security has imposed on them in violation of the law.

JURISDICTION AND VENUE

20. This Court has personal jurisdiction over Defendants because they conduct substantial business in New York, have sufficient minimum contacts with this state, and otherwise purposely avail themselves of the privileges of conducting business in New York by marketing and selling products and services in New York. Further, the injuries to New York consumers that Plaintiff seeks to prevent through public injunctive relief arise directly from Nord Security's continuing conduct in New York, including, but not limited to, directing its subscription scheme at New York consumers.

21. This Court has jurisdiction over the claims asserted in this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), because the aggregate claims of the Class exceed the sum or value of $5,000,000, the Class has more than 100 members, and diversity of citizenship exists between at least one member of the Class and Nord Security.

22. This Court has original subject matter jurisdiction over all claims in this action pursuant to the Class Action Fairness Act. However, if the Court determines that it lacks original jurisdiction over any claim in this action, it may exercise supplemental jurisdiction over Plaintiff's claims under 28 U.S.C. § 1367 because all of the claims arise from a common nucleus of operative facts and are such that Plaintiff ordinarily would expect to try them in one judicial proceeding.

23. Venue is proper in this District pursuant to 28 U.S.C. § 1391(c)(3). Each Defendant is a foreign corporation and may be sued in any judicial district in the United States. *Id*.

PARTIES

24. Plaintiff Lanzy Kandeh is a citizen of New York.

25. Plaintiff Kandeh is a consumer who was victimized by Nord Security's unlawful subscription scheme, suffered ascertainable injury in fact, and lost money because of Nord Security's violations of New York consumer protection statutes and the common law.

26. Upon information and belief, with respect to all actions and decisions relevant to this action, Defendants along with non-Defendants NordSec Ltd. and Nord Security Inc. have operated as a single company called "Nord Security." Yet unbeknownst to the ordinary consumer, "Nord Security" is a brand and not a formal corporate entity.

27. Defendants, along with non-Defendants NordSec Ltd. and Nord Security Inc., hold themselves out to the public, including Plaintiff, as if a single fictitious entity called "Nord Security" sells the services consumers in New York and the rest of the United States purchase. For example, when a consumer visits www.nordsecurity.com they see a typical company website with the "Nord Security" logo that features "our products" (including one of the products purchased by Plaintiff), "our story," "our team" and "our values." Similarly, when top U.S. venture capital firm Warburg Pincus and others invested $100 million in Defendants and non-Defendants NordSec Ltd. and Nord Security Inc., "Nord Security" issued a press release describing the funding as an investment in "Nord Security, a global leader in internet privacy and security solutions."[4] This same press release states that NordVPN is "the biggest and most popular VPN service in the world" and that "Nord Security was founded in Lithuania in 2012 by co-founders and co-CEOs Tom Okman and Eimantas Sabaliauskas."[5] Likewise, the "Corporate responsibility" page for "Nord

[4] Nord Security raised another $100M investment round, NORD SECURITY, https://nordsecurity.com/blog/nord-security-raised-another-100m-investment-round.

[5] *Id.*

Security" shows pictures of the founders, explains "our mission," and contains links to Nord Security's "corporate responsibility reports" and Nord Security's "Code of Conduct,"[6] which discusses such topics as expectations for the "Nord Security brand products, including NordVPN, NordPass, NordLocker, and NordLayer."[7]

28. Defendant Nordvpn S.A. is a Panamanian corporation incorporated under the laws of Panama.[8] Nordvpn S.A.'s principal place of business is in Amsterdam, the Netherlands.[9] Nordvpn S.A. currently "offers" Defendants and non-Defendants NordSec Ltd. and Nord Security Inc.'s products "NordVPN, NordLocker, and NordPass."[10] NordVPN is one of the products Defendants and non-Defendants NordSec Ltd. and Nord Security Inc. marketed and sold to Plaintiff in New York. Defendant Nordvpn S.A. also currently operates Defendants and non-Defendants NordSec Ltd. and Nord Security Inc.'s website, www.nordvpn.com.[11] Nordvpn S.A.'s corporate parents are Defendant NordSec B.V., non-Defendant NordSec Ltd., and Cyberswift B.V., which is also one of the corporate parents of non-Defendant NordSec Ltd.[12] Nordvpn S.A. shares an unnamed director with Defendant Tefincom S.A.[13]

---

[6] Corporate Responsibility, NORD SECURITY, https://nordsecurity.com/corporate-responsibility

[7] Code of Conduct, NORD SECURITY, https://res.cloudinary.com/nordsec/image/upload/v1712078877/nord-security-web/corporate/code%20of%20conduct/Nord_Security_Code_of_Conduct.pdf.

[8] *Zeichner v. Nord Security Inc. et al.*, No. 24 Civ 2462 (N.D. Cal.) ("Zeichner"), Dkt. No. 39-1, ¶ 3.

[9] *Id.*

[10] *Id.*

[11] *Id.*

[12] *Zeichner*, Dkt. No. 37.

[13] *Zeichner*, Dkt. No. 39-1, ¶ 8.

29. Defendant Tefincom S.A. d/b/a NordVPN is a Panamanian corporation incorporated under the laws of Panama.[14] Defendant Tefincom S.A.'s principal place of business is Panama City, Panama.[15] Defendant Tefincom S.A.'s corporate parent is Stitching Raveset.[16] Defendants and non-Defendants NordSec Ltd. and Nord Security Inc. admit that Defendant Tefincom S.A. was the contracting entity for New York retail consumer VPN services purchased on or before November 15, 2020.[17] Defendant Tefincom S.A. was the original owner of the trademark for "NordVPN."

30. Non-Defendant NordSec Ltd. is an internet privacy and security company headquartered in London, England.[18] NordSec Ltd. is a private limited liability company organized under the laws of England & Wales.[19] Defendants and non-Defendants NordSec Ltd. and Nord Security Inc. claim that NordSec Ltd. "once owned the intellectual property of the Nord brand."[20] NordSec Ltd.'s corporate parents are Cyberswift B.V., Cyberspace B.V., and Stalwart Holding B.V.[21] NordSec Ltd. is also an owner of Defendant NordSec B.V.,[22] Defendant Nordvpn S.A.,[23] and Nord Security Inc.[24] Public records indicate that NordSec Ltd. is a prior owner of the "NordVPN" trademark.

---

[14] *Zeichner*, Dkt. No. 39-3, ¶ 3.

[15] *Id.*

[16] *Zeichner*, Dkt. No. 38.

[17] *Zeichner*, Dkt. No. 39-3, ¶ 3.

[18] *Zeichner*, Dkt. No. 39-5, ¶ 3.

[19] *Id.*

[20] *Zeichner*, Dkt. No. 39, at 5.

[21] *Zeichner*, Dkt. No. 35.

[22] *Zeichner*, Dkt. No. 36.

[23] *Zeichner*, Dkt. No. 37.

[24] *Zeichner*, Dkt. No. 27.

31. Defendant NordSec B.V. is an internet privacy and security company headquartered in Amsterdam, the Netherlands.[25] NordSec B.V. is a private limited liability company organized under the laws of the Netherlands.[26] Defendants and non-Defendants NordSec Ltd. and Nord Security Inc. claim that NordSec B.V. "currently owns the intellectual property of the Nord brand."[27] NordSec B.V.'s corporate parents are NordSec Ltd. and two of NordSec Ltd.'s corporate parents, Cyberswift B.V. and Cyberspace B.V.[28] NordSec B.V. is also an owner of Defendant Nordvpn S.A.[29] and Nord Security Inc.[30] Defendants and non-Defendants NordSec Ltd. and Nord Security Inc.'s website www.nordsecurity.com claims that "Nord Security trademarks, trade names, company names, logos," whether registered or not, "as well as other Nord Brand features (such as Nord Security websites, applications and creative works embodied therein), are the exclusive property of NordSec B.V. ('Nord Security')."[31] NordSec B.V.'s marks include the marks "Nord Security," "NordVPN," "Nord," "NordSec," NordLocker," and "NordPass." Upon information and belief, the website Plaintiff used to enroll with Nord Security was the website owned by NordSec B.V. and one of the Nord Subscriptions he purchased bore the "Nord Security," "NordVPN," "Nord," and "NordSec" marks owned by NordSec B.V. NordSec B.V. processed the payment for Plaintiff's Nord Subscription to the Incogni product.

[25] *Zeichner*, Dkt. No. 39-2, ¶ 3.

[26] *Id.*

[27] *Zeichner*, Dkt. No. 39, at 5.

[28] *Zeichner*, Dkt. No. 36.

[29] *Zeichner*, Dkt. No. 37.

[30] *Zeichner*, Dkt. No. 27.

[31] Nord Security Trademark and Brand Guidelines, NORD SECURITY, https://nordsecurity.com/trademark-policy.

32. Non-Defendant Nord Security Inc. is a Delaware corporation.[32] Nord Security Inc.'s corporate parents are NordSec B.V., NordSec Ltd., and Cyberswift B.V., [33] which is also a corporate parent of NordSec B.V.[34] and NordSec Ltd.[35] Defendants and non-Defendants NordSec Ltd. and Nord Security Inc. claim in a separate litigation that Nord Security Inc. is not the "Nord Security" that offers services to New York consumers, instead claiming that Nord Security Inc. provides only business-to-business services.[36]

33. Upon information and belief, at all times pertinent to this action, the finances, policies, and business practices of Defendants and non-Defendants NordSec Ltd. and Nord Security Inc. are and were dominated and controlled by one another in such a manner that each individual Defendant and each of non-Defendants NordSec Ltd. and Nord Security Inc. has no separate mind, will, identity, or existence of its own and instead operated as mere instrumentalities and alter egos of one another. For example, even though public records and fine print on the www.nordsecurity.com website indicate that NordSec B.V. owns the "NordVPN" trademark, the www.nordvpn.com website states that "NordVPN is owned and operated by nordvpn S.A."[37] Similarly, that same website also states that "[b]ack in 2012, two best friends sought to create a tool for a safer and more accessible internet. Driven by the idea of internet freedom, Tom Okman and Eimantas Sabaliauskas created NordVPN."[38] Tom Okman and Eimantas Sabaliauskas are

[32] *Zeichner*, Dkt. No. 27.

[33] *Id.*

[34] *Zeichner*, Dkt. No. 36.

[35] *Zeichner*, Dkt. No. 35.

[36] *Zeichner*, Dkt. No. 39, at 5.

[37] "The founders and owners of NordVPN," NORDVPN.COM, https://support.nordvpn.com/hc/en-us/articles/20911146148113-The-founders-and-owners-of-NordVPN.

[38] *Id.*

listed as directors of NordSec Ltd., but their respective LinkedIn pages claim they are co-founders of "Nord Security."[39]

34. Upon information and belief, Defendants and non-Defendants NordSec Ltd. and Nord Security Inc. are so closely related in ownership and management, and each works closely in concert with the others, such that each has become the alter ego of the others, in that, among other things:

a. Defendants and non-Defendants NordSec Ltd. and Nord Security Inc. operate and hold themselves out to the public as a single, fictitious entity, Nord Security.

b. Defendants and non-Defendants NordSec Ltd. and Nord Security Inc. operate and hold themselves out to the public in such a way that members of the public would be unable to identify and distinguish between one entity and another. For example, a consumer searching the internet for "NordVPN" would find www.nordvpn.com, which is owned and operated by Defendant Nordvpn S.A. but which Defendants and non-Defendants NordSec Ltd. and Nord Security Inc. represent is the website of the non-existent entity "Nord Security." "Nord Security" is a trademark owned by NordSec B.V. The www.nordsecurity.com website, which Defendants and non-Defendants NordSec Ltd. and Nord Security Inc. also represent is owned by the brand "Nord Security" similarly lists the various "Nord Security" products, including NordVPN.

c. Defendants and non-Defendants NordSec Ltd. and Nord Security Inc. do not market themselves independently.

d. Olga Sinkeviciene, a director of NordSec Ltd., and Ruta Gorelcionkiene, a director of NordSec B.V., are both employees of CEOcorp, a company that "specializes in the incorporation of entities and implementation of corporate structures across diverse jurisdictions."[40]

e. Upon information and belief, Defendants and non-Defendants NordSec Ltd. and Nord Security Inc. share employees. For example, the LinkedIn pages of many of Defendants and non-Defendants NordSec Ltd. and Nord Security Inc.'s employees state that these employees work at "Nord Security," even though no such entity exists. When a prospective employee visits Defendant Nordvpn S.A.'s website, www.nordvpn.com, they are redirected to the "careers" subpage of www.nordsecurity.com

[39] *See* https://www.linkedin.com/in/tokmanas/; *see also* https://www.linkedin.com/in/eimis/.
[40] Services, CEOCORP, https://ceocorp.net/services/.

(https://nordsecurity.com/careers). That page contains various claims and a video about what it is like to work at "Nord Security." Job applicants can apply for "Nord Security" positions available in Lithuania, Germany, Poland, and remotely.

f. When Defendants and non-Defendants NordSec Ltd. and Nord Security Inc. issue press releases, they do so under the name "Nord Security" without identifying or distinguishing between corporate entities.

g. On information and belief, there is a unified executive team that controls all operational and financial aspects of Defendants and non-Defendants NordSec Ltd., and Nord Security Inc.

35. Both Defendants and non-Defendants NordSec Ltd. and Nord Security Inc. have been represented by the same counsel in cases filed in North Carolina and California, where non-Defendants NordSec Ltd. and Nord Security Inc. were also named as defendants. This same counsel also represents Defendants Nordvpn S.A. and Tefincom S.A. in a case filed in Colorado and Defendant Nordvpn S.A. in a case filed in North Carolina.

36. Defendants and non-Defendants NordSec Ltd. and Nord Security Inc. do business in New York under the name "Nord Security" and interacted with Plaintiff in New York such that his claims described herein arise from Plaintiff's contacts with Defendants and these non-Defendants in New York.

37. Any such conduct of Defendant Nordvpn S.A., Defendant Tefincom S.A. Defendant NordSec B.V., non-Defendant NordSec Ltd., and non-Defendant Nord Security Inc. should be imputed to each other.

FACTUAL ALLEGATIONS

A. Background on the Subscription e-Commerce Industry

38. The e-commerce subscription model is a business model in which retailers provide ongoing goods or services "in exchange for regular payments from the customer."[41] Subscription e-commerce services target a wide range of customers and cater to a variety of specific interests. Given the prevalence of online and e-commerce retailers, the popularity of subscription e-commerce has grown rapidly in recent years. Indeed, as of 2022 the "subscription economy ha[d] grown more than 400% over the last 8.5 years as consumers have demonstrated a growing preference for access to subscription services[.]"[42]

39. The production, sale, and distribution of subscription-based products and services is a booming industry that has exploded over the past few years. "Over the past 11 years, subscription-based companies[] have grown 3.7x faster than the companies in the S&P 500."[43]

40. The expansion of the subscription e-commerce market shows no signs of slowing. According to The Washington Post, "[s]ubscriptions boomed during the coronavirus pandemic as Americans largely stuck in shutdown mode flocked to digital entertainment[.] . . . The subscription economy was on the rise before the pandemic, but its wider and deeper reach in

---

[41] *See* Sam Saltis, *How to Run an eCommerce Subscription Service: The Ultimate Guide*, CORE DNA, https://www.coredna.com/blogs/ecommerce-subscription-services.

[42] Mary Mesienzahl, *Taco Bell's taco subscription is rolling out nationwide — here's how to get it*, BUSINESS INSIDER (Jan. 6, 2022), https://www.businessinsider.com/taco-bell-subscription-launching-across-the-country-2022-1 (internal quotation marks omitted).

[43] *The Subscription Economy Index*, ZUORA (Mar. 2023), https://www.zuora.com/wp-content/uploads/2023/03/Zuora_SEI_2023_Q2.pdfhttps://www.zuora.com/resources/subscription-economy-index/.

nearly every industry is expected to last."[44] 68% of consumers subscribed to something for the first time in 2024.[45]

41. However, there are well-documented downsides associated with the subscription-based business model. While the subscription e-commerce market has low barriers and is thus easy to enter, it is considerably more difficult for retailers to dominate the market due to the "highly competitive prices and broad similarities among the leading players."[46] In particular, retailers struggle with the fact that "[c]hurn rates are high, [] and consumers quickly cancel services that don't deliver superior end-to-end experiences."[47] Yet, retailers have also recognized that, where the recurring nature of the service, billing practices, or cancellation process is unclear or complicated, "consumers may lose interest but be too harried to take the extra step of canceling their membership[s]."[48] As these companies have realized, "[t]he real money is in the inertia."[49] As a result, "[m]any e-commerce sites work with third-party vendors to implement more

---

[44] Heather Long and Andrew Van Dam, *Everything's becoming a subscription, and the pandemic is partly to blame*, WASHINGTON POST (June 1, 2021), https://www.washingtonpost.com/business/2021/06/01/subscription-boom-pandemic/.

[45] Tien Tzuo, *They said subscriptions were doomed. The market said otherwise.*, ZUORA (Mar. 6, 2025), https://www.zuora.com/subscribed/they-said-subscriptions-were-doomed-the-market-said-otherwise.

[46] Tony Chen, *et al*., *Thinking inside the subscription box: New research on e-commerce consumers*, MCKINSEY & COMPANY (Feb. 9, 2018), https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/thinking-inside-the-subscription-box-new-research-on-ecommerce-consumers#0.

[47] *Id.*

[48] Amrita Jayakumar, *Little-box retailing: Subscription services offer new possibilities to consumers, major outlets*, WASHINGTON POST (Apr. 7, 2014), https://www.washingtonpost.com/business/economy/tktktktk/2014/04/07/f68135b6-a92b-11e3-8d62-419db477a0e6_story.html.

[49] *Id.*

manipulative designs."[50] That is, to facilitate consumer inertia, some subscription e-commerce companies, including Nord Security, "are now taking advantage of subscriptions in order to trick users into signing up for expensive and recurring plans. They do this by intentionally confusing users with their app's design and flow, . . . and other misleading tactics[,]" such as failure to fully disclose the terms of its automatic-renewal programs.[51]

42. To make matters worse, once enrolled in the subscription, "[o]ne of the biggest complaints consumers have about brand/retailers is that it's often difficult to discontinue a subscription marketing plan."[52] Indeed, "the rapid growth of subscriptions has created a host of challenges for the economy, far outpacing the government's ability to combat aggressive marketing practices and ensure that consumers are being treated fairly, consumer advocates say."[53] Thus, although "Federal Trade Commission regulators are looking at ways to make it harder for companies to trap consumers into monthly subscriptions that drain their bank accounts, [and are] attempting to respond to a proliferation of abuses by some companies over the past few years[,]"[54] widespread utilization of these misleading "dark patterns" and deliberate omissions persist.

---

[50] Zoe Schiffer, *A new study from Princeton reveals how shopping websites use 'dark patterns' to trick you into buying things you didn't actually want*, BUSINESS INSIDER (June 25, 2019), https://www.businessinsider.com/dark-patterns-online- shopping-princeton-2019-6.

[51] Sarah Perez, *Sneaky subscriptions are plaguing the App Store*, TECHCRUNCH (Oct. 15, 2018), https://techcrunch.com/2018/10/15/sneaky-subscriptions-are-plaguing-the-app-store.

[52] Heather Long and Andrew Van Dam, *supra* note 44 ("'Subscription services are a sneaky wallet drain,' said Angela Myers, 29, of Pittsburgh. 'You keep signing up for things and they make it really hard to cancel.'"); *see also The problem with subscription marketing*, NEW MEDIA AND MARKETING (Mar. 17, 2019), https://www.newmediaandmarketing.com/the-problem-with-subscription-marketing.

[53] Heather Long and Andrew Van Dam, *supra* note 44.

[54] *Id.*

43. The term "dark patterns" used herein is not a science fiction reference, but a term of art from the field of user experience ("UX"). The International Organization for Standardization defines UX as a "person's perceptions and responses that result from the use or anticipated use of a product, system or service."[55] Dark patterns in UX are "carefully designed misleading interfaces by UX design experts that trick the users into choosing paths that they didn't probably want to take, thus fulfilling the business objectives, completely ignoring the requirements and ethics of users."[56]

44. The term "dark patterns" was first coined by cognitive scientist Harry Brignull, who borrowed from existing UX terminology. In UX, designers refer to common, re-usable solutions to a problem as a "design pattern," and conversely to common mistakes to solutions as "anti-patterns."[57] The term "dark patterns" was intended to "communicate the unscrupulous nature" of the design "and also the fact that it can be shadowy and hard to pin down."[58] The image on the next page provides some examples of commonly employed dark patterns:[59]

---

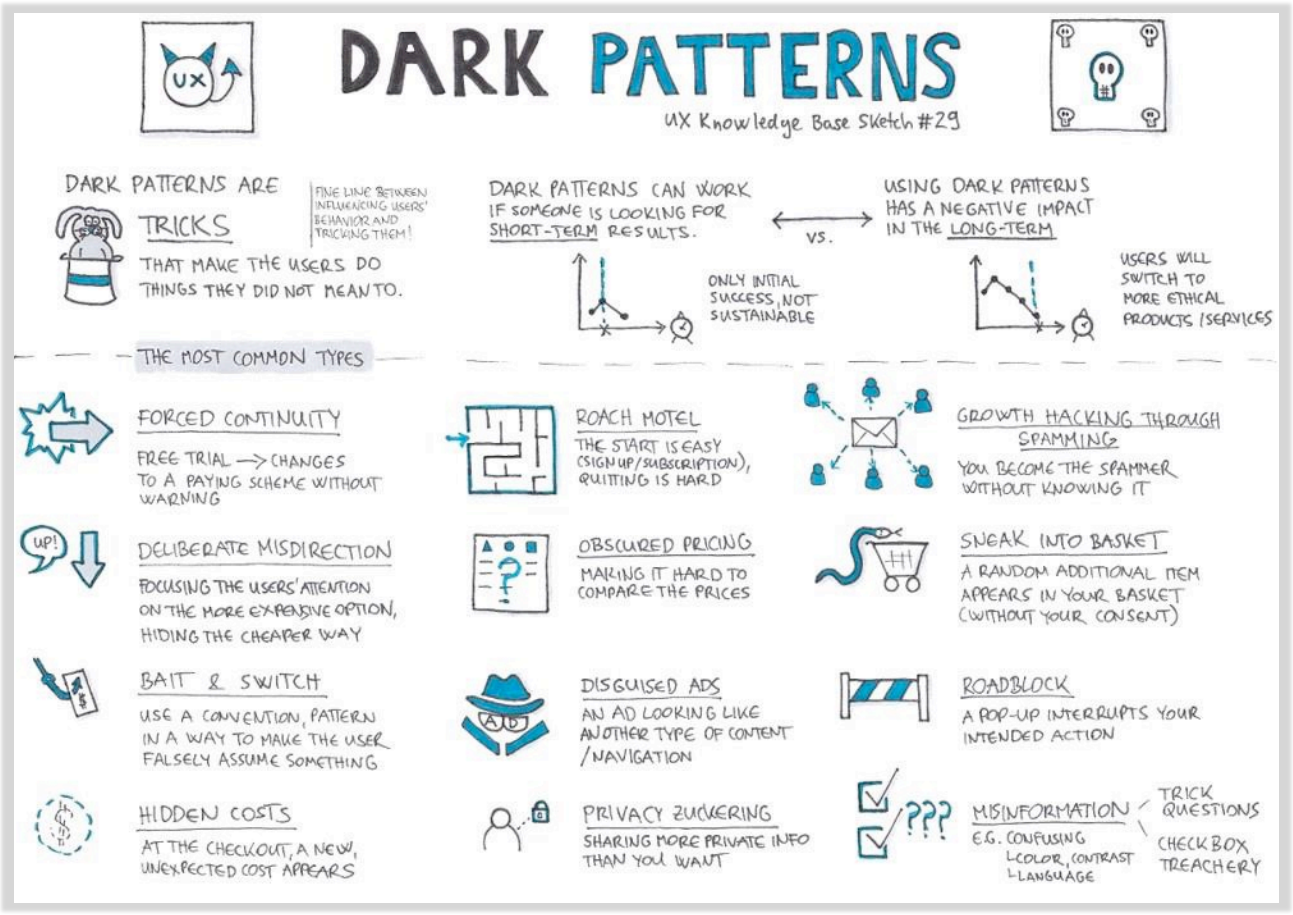
[55] *User Experience (UX): Process and Methodology*, UIUX TREND, https://uiuxtrend.com/user-experience-uxprocess/.

[56] Joey Ricard, *UX Dark Patterns: The Dark Side Of The UX Design*, KLIZO SOLS. PVT. LTD. (Nov. 9, 2020), https://klizos.com/ux-dark-patterns-the-dark-side-of-the-ux-design.

[57] Harry Brignull, *Bringing Dark Patterns to Light*, MEDIUM (June 6, 2021), https://harrybr.medium.com/bringing-dark-patterns-to-light-d86f24224ebf.

[58] *Id.*

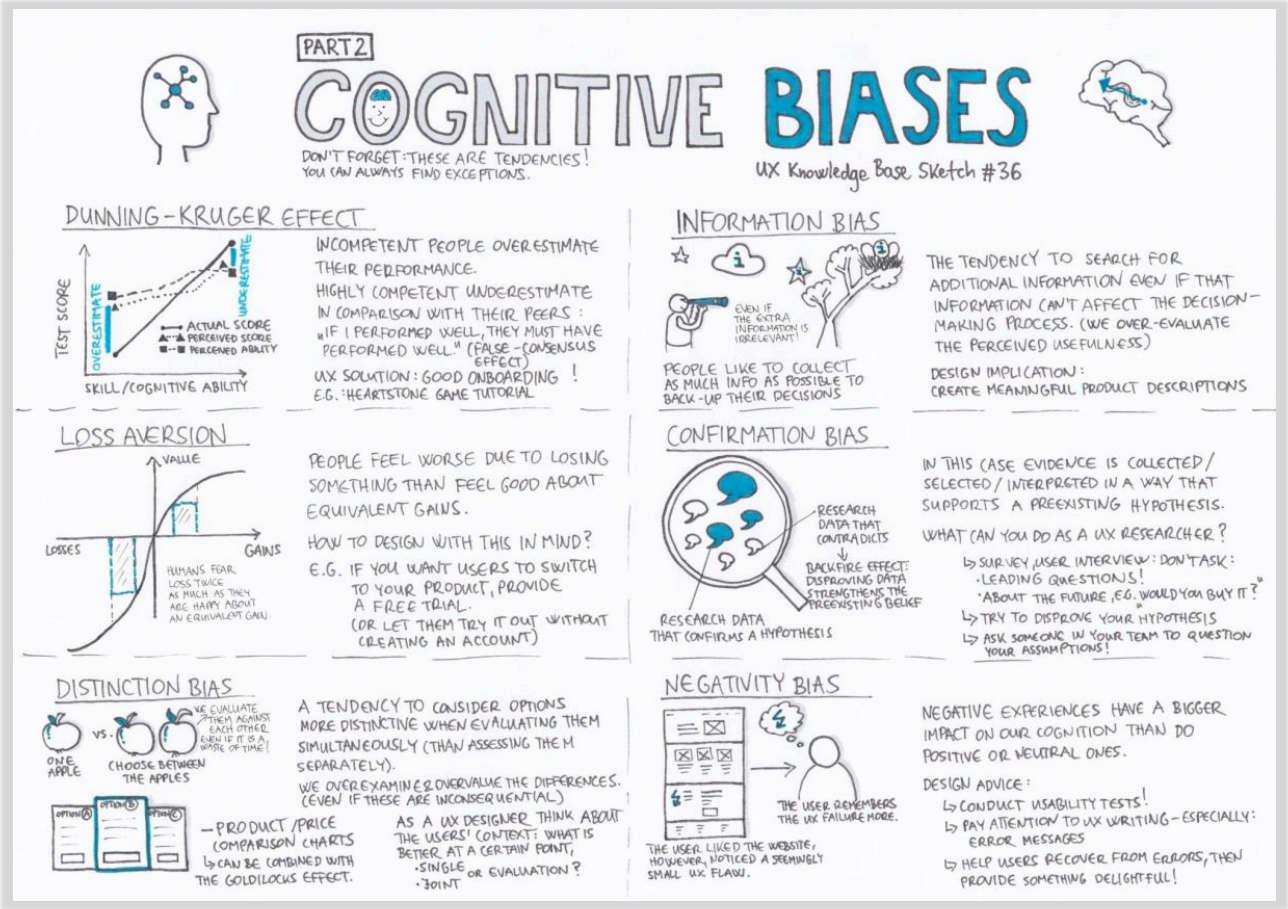
[59] Sarbashish Basu, *What is a dark pattern? How it benefits businesses- Some examples*, H2S MEDIA (Dec. 19, 2019), https://www.how2shout.com/technology/what-is-a-dark-pattern-how-it-benefit-businesses-with-some-examples.html.



45. The origin of dark patterns can be traced to the use of applied psychology and A/B testing in UX.[60] In the 1970s, behavioral science sought to understand irrational decisions and behaviors and discovered that cognitive biases guide all our thinking. The image on the next page provides examples of cognitive biases, including some that Nord Security employs in its cancellation process:[61]

[60] Brignull, *supra* note 57.

[61] Krisztina Szerovay, *Cognitive Bias — Part 2*, UX KNOWLEDGE BASE (Dec. 19, 2017), https://uxknowledgebase.com/cognitive-bias-part-2-fab5b7717179.



46. But while the early behavioral research focused on understanding rather than intervention, later researchers, like Cass Sunstein and Richard Thaler (authors of the book *Nudge*) shifted focus and made the policy argument that institutions should engineer "choice architectures" in a way that uses behavioral science for the benefit of those whom they serve.[62]

47. Another step in the development and application of such research is the use of A/B testing in UX. A/B testing is a quantitative research method that presents an audience with two variations of a design and then measures which actions they take (or do not take) in response to each variant.[63] UX designers use this method to determine which design or content performs best

[62] Arvind Narayanan *et al.*, *Dark Patterns: Past, Present, and Future. The evolution of tricky user interfaces*, 18 ACM QUEUE 67-91 (2002), https://queue.acm.org/detail.cfm?id=3400901.

[63] UXPin, *A/B Testing in UX Design: When and Why It's Worth It*, https://www.uxpin.com/studio/blog/ab-testing-in-ux-design-when-and-why.

with the intended user base.[64] For example, a large health care provider might A/B test whether a website visitor is more or less likely to conduct a search of its doctors if the website's search function is labelled "SEARCH" versus simply identified by a magnifying glass icon.

48. Unscrupulous UX designers have subverted the intent of the researchers who discovered cognitive biases by using these principles in ways that undermine consumers' autonomy and informed choice, and they used A/B testing to turn behavioral insights into strikingly "effective" user interfaces that deceive consumers in ways that are more profitable to the company applying them.[65] For example, dark patterns can be used to increase a company's ability to extract revenue from its users by nudging or tricking consumers to spend more money than they otherwise would, hand over more personal information, or see more ads.[66]

49. Nord Security has engaged in these unlawful subscription practices with great success. In 2023, Nord Security raised $100 million from investors, with the company valued at $1.6 billion.[67] Nord Security's products and services have over 15 million users.

B. Nord Security's Enrollment and Acknowledgment Processes Contain Numerous Material Misrepresentations and Omissions.

50. In order to purchase in a Nord product offering, a consumer must visit Defendants' website, select the product, and complete the transaction on the website. Consumers cannot purchase a Nord product offering through Nord Security's mobile or desktop app.

51. During the Class period (*see infra* ¶ 123) to the present, Nord Security presents its subscription plans to consumers considering a purchase as if they were time-limited, rather than

---

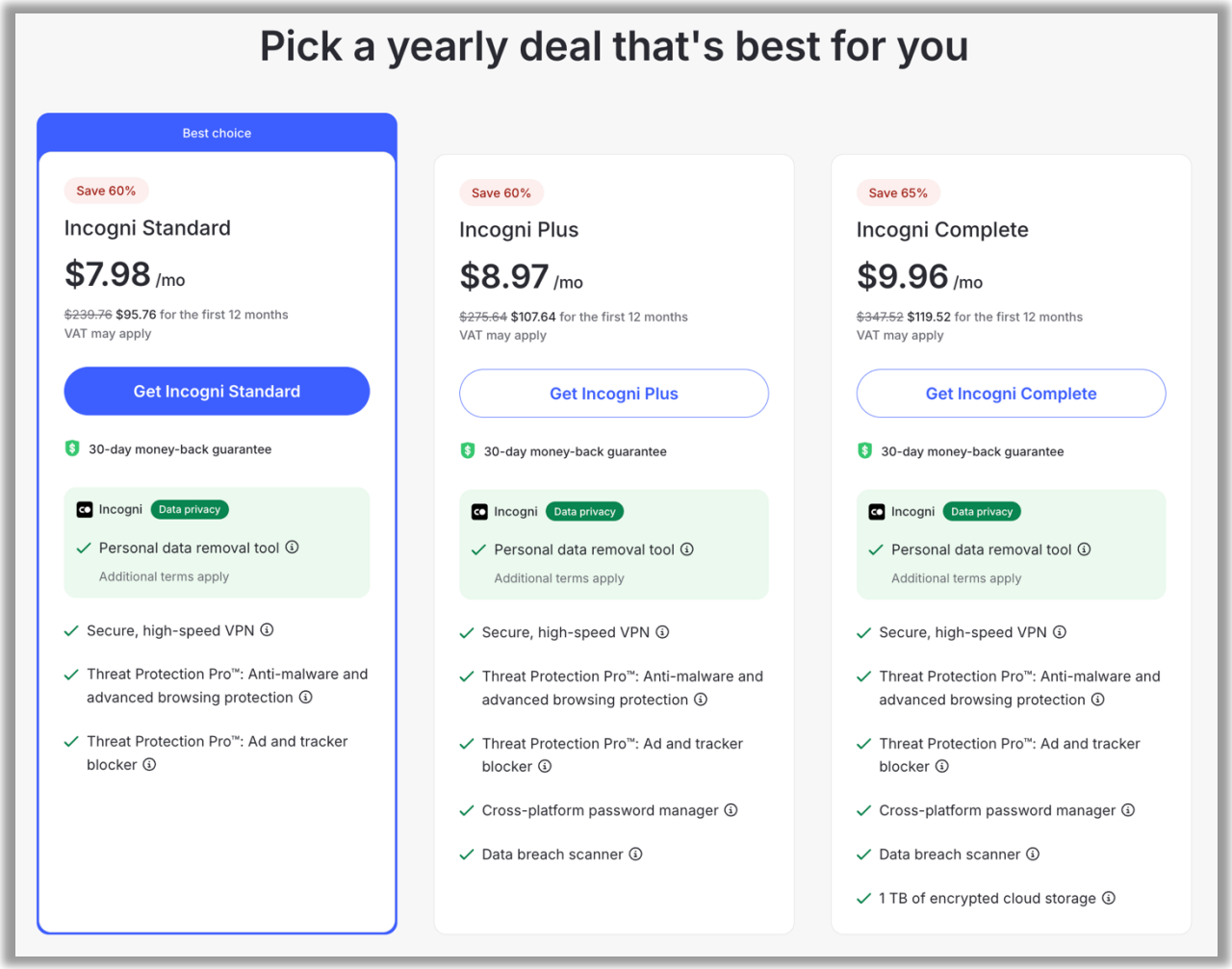
[64] *Id.*

[65] Narayanan *et al.*, *supra* note 62.

[66] *Id.*

[67] Nord Security raised another $100M investment round, NORD SECURITY, https://nordsecurity.com/blog/nord-security-raised-another-100m-investment-round.

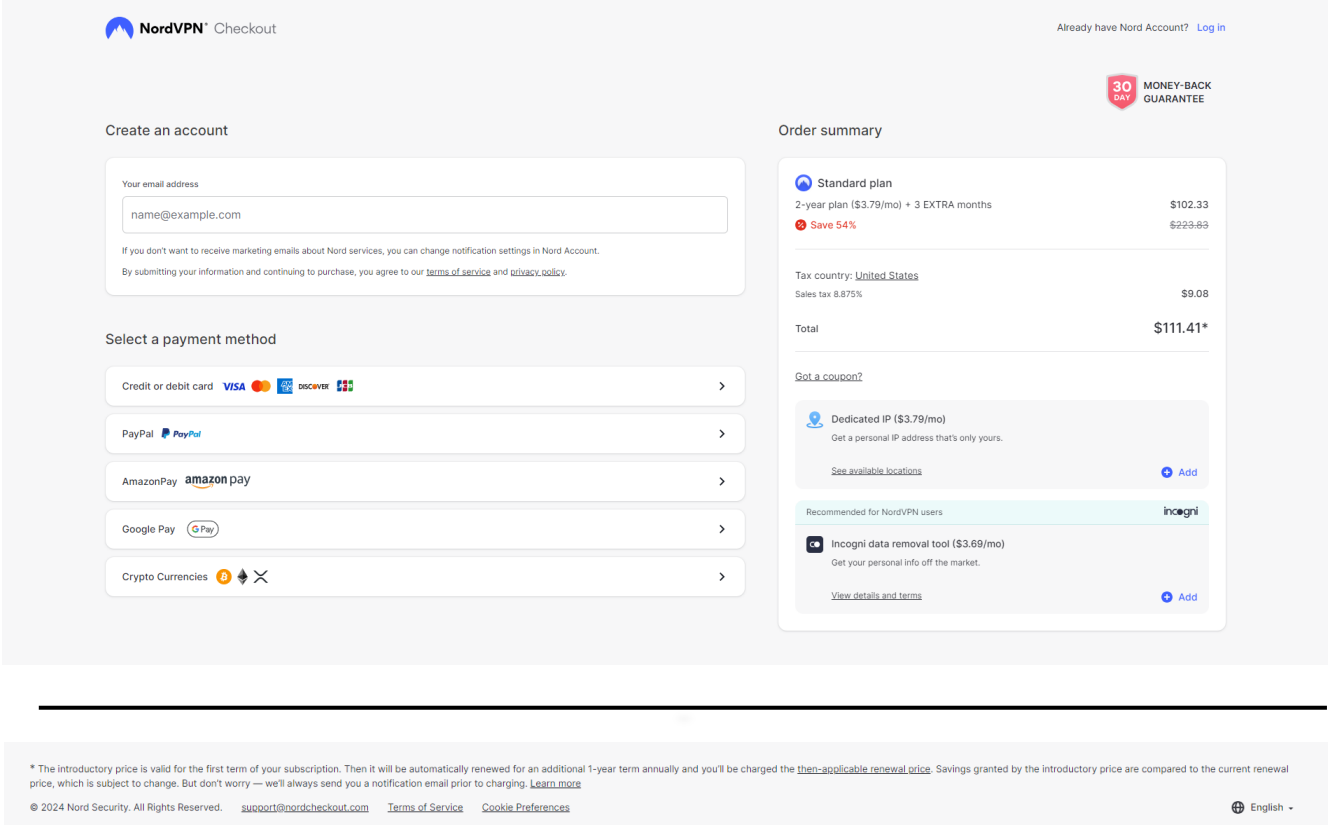
autorenewing. For example, a reasonable consumer choosing between three tiers of a Nord Subscription to the Incogni product in March 2025 would understand Nord to be offering a time-limited one year plan of its "Standard" tier for the heavily discounted price of $95.76, billed at $7.98 per month:



52. In reality, a consumer who purchased the "Incogni Standard" plan selected in the image above would pay $95.76 up front for a year of access to Incogni and would be autorenewed year-to-year indefinitely at some undisclosed future renewal price, unless he or she cancelled.

53. After selecting a product tier, the consumer is taken to Nord Security's checkout page. Upon information and belief, the payment page for Nord Security's enrollment process that

Plaintiff used in December 2023 to purchase the Incogni product was materially similar to the Nord Security payment page for Nord Security's NordVPN product reproduced below:



54. On the checkout page, Nord Security continues to deceive consumers about the autorenewing nature of its product offerings. Indeed, not only are the terms and conditions of Nord Security's automatic renewal offer are not presented to consumers in a "clear and conspicuous" manner, as required by New York's Automatic Renewal Law, G.B.L. §§ 527, 527-a ("ARL"), they are actively obscured by Nord Security's web design.

55. The fine print that includes Nord Security's (inadequate) "disclosures" about its automatic renewal offer (shown below the solid black line above) is on Nord Security's payment screen but is not visible unless the consumer scrolls down to view it. The automatic renewal language is also not in larger type than the surrounding font. Instead, it is colored light gray rather

than a more conspicuous color and is not set off from the surrounding text of the same size by symbols or other marks in a manner that clearly calls attention to the language. All of the aforementioned intentional design choices made by Defendants violate the ARL, *see* G.B.L. § 527-a(1)(a) (requiring companies like Nord Security to "present the automatic renewal offer terms . . . in a clear and conspicuous manner"), and deceived consumers into thinking they are purchasing a time-limited access to the Nord product offering.

56. Instead, the payment page's overall design, including the location of Defendants' supposed "disclosure," its font size, and color, ***deemphasize*** the notice text rather than make it ***conspicuous***. Defendants' automatic renewal terms are not in visual connection with the purchase terms and are instead buried at the bottom of the page. This makes it unlikely reasonable consumers will even see the "disclosures" because they must scroll down to view them, they are presented in a light grey font against a lighter gray background, and are in a single-spaced format, which makes the "disclosures" difficult to read.

57. Further, because consumers must scroll down to view the automatic renewal terms, Nord Security's automatic renewal offer is not "in visual proximity" to its request for consumers to consent to the offer, an additional violation of the ARL. *Id*. § 527-a(1)(a)

58. Defendants' fine print also intentionally omit key details about Nord Security's subscription practices, including the cancellation policy and information on how to cancel.

59. Moreover, any supposed "disclosures" on the Nord Security payment page are far overshadowed by the page's other components in a clear demonstration of the "Misinformation" dark pattern. Defendants' payment page uses at least 12 different colors, presents information in differently sized fonts and in various boxes, and includes hyperlinks, drop-down menus styled as hyperlinks, two call-outs for add-on products, and 13 different logos. In contrast, the automatic

renewal terms are hidden at the bottom of the page, difficult to discern, and easy to miss, especially since consumers must scroll down on the screen to view them.

60. Nord Security's "Order Summary" box likewise does not sufficiently present the terms and conditions of its automatic renewal offer to consumers, nor does it present the consumer with an easily accessible disclosure of the methods that the consumer may use to cancel the subscription. Nord Security's intentional omissions in the section of the checkout page "summarizing" the order contribute to the reasonable consumer's impression that they are purchasing time-limited access to Nord Security's product offerings.

61. When a consumer selects a payment method on the checkout page (*e.g.*, credit card, Paypal, etc. in the image *supra* ¶ 53), the payment method box expands, again failing to disclose Nord Security's autorenewal terms, let alone in a clear and conspicuous manner. The expanded payment boxes also do not present the consumer with any disclosure of the cancellation policy or the methods that may be used to cancel the subscription, let alone a method that is easily accessible.

62. The Nord Security payment page fails to obtain consumers' affirmative consent to the automatic renewal terms and contains no mechanism for affirmatively consenting to the automatic renewal terms. For example, there is no checkbox that consumers must click to indicate that they accept those terms. *See id.* § 527-a(1)(b) (it is unlawful to charge consumers for an automatic renewal "without first obtaining the consumer's affirmative consent to the agreement containing the automatic renewal offer terms").

63. Nowhere on the payment page does Nord Security disclose critical information regarding cancellation, such as how to cancel and how to turn off autorenewal, and certainly does not clearly and conspicuously disclose how to do so in a manner that is capable of being retained

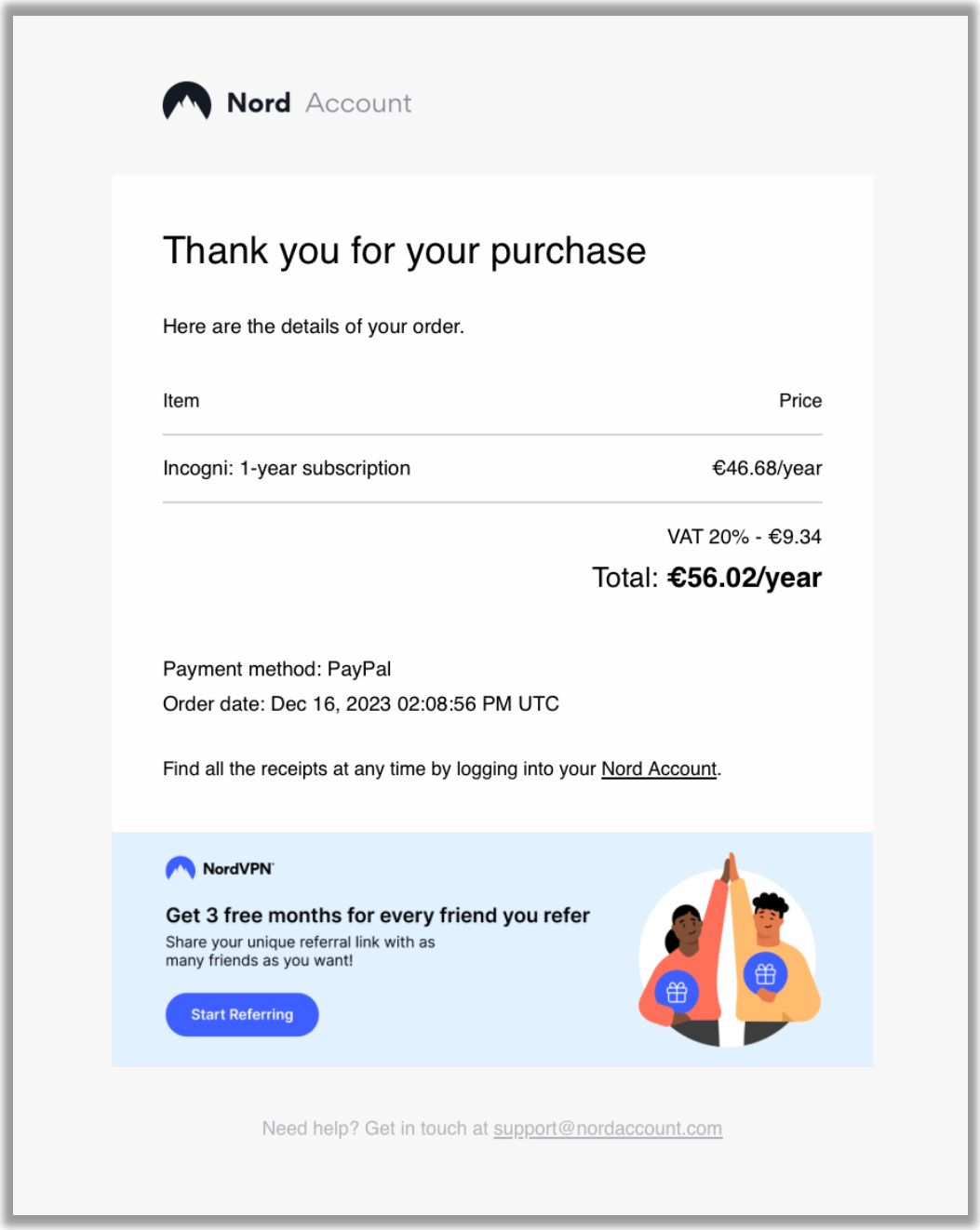
by the consumer. *See id*. § 527-a(1)(a) (it is unlawful to fail to provide automatic renewal offer terms "in a clear and conspicuous manner before the subscription or purchasing agreement is fulfilled and in visual proximity . . . to the request for consent to the offer"); G.B.L. § 527(2)(b) (defining "automatic renewal offer terms" to include "the description of the cancellation policy that applies to the offer").

64. Instead, Nord Security intentionally provides tiny, inconspicuous hyperlinks to "terms of service" and "terms" which themselves do not clearly and conspicuously explain the nature of Nord Security's automatic renewal offer or cancellation mechanism. *See infra* ¶¶ 80–82.

65. In sum, Nord Security's enrollment process is misleading in that it suggests that consumers are purchasing time-limited access to Nord Security's product offerings, laying a trap through which Nord Security can later (and indefinitely) autorenew the consumer into additional, pricey subscriptions periods without their consent.

C. Nord Security's Misrepresentations Continue Even After a Customer Has Purchased a Nord Subscription

66. After Plaintiff enrolled in Incogni, Nord Security sent Plaintiff an email with the subject line "Order receipt from Dec 16, 2023." A representative version of the acknowledgement email sent to Plaintiff and other consumers is shown on the next page:



67. The post-purchase receipt email Defendants send after consumers complete a purchase on Nord Security's website is deceptive in several ways

68. First, the term "Order receipt" in the email's subject line is deceptive because it implies that the consumer has completed a one-time financial transaction in exchange for the time-limited subscription to a Nord product offering, when in fact the consumer has unwittingly entered an indefinite, autorenewing subscription.

69. Second, that impression is only confirmed by the email itself which thanks the consumer "for your purchase" and lists the "Item" purchased as a time-limited subscription to the product offering for a set "Price" (in the email above, "Incogni: 1-year subscription").

70. Third, the receipt email fails to disclose critical aspects of Nord Security's subscription scheme, including that it is autorenewing, that a consumer must cancel before a certain date in order to avoid being charged, that the price charged may be different than the price shown in the receipt, and that the date by which the consumer must cancel is ***not*** at or after the end of the subscription term purchased (i.e., one year), but is instead 14 days earlier, as discussed in greater detail *infra* ¶¶ 79–82. It also fails to provide any cancellation instructions or a means of cancelling.

71. Nor does Nord Security's receipt email meet the post purchase requirements that the ARL imposes on an automatically renewing product or service. It does not provide "the automatic renewal offer terms . . . , cancellation policy, and information regarding how to cancel" for Nord Subscriptions, *id*. § 527-a(1)(c), nor disclose "how to cancel" the renewal "before the consumer pays" for a Nord Subscription, *id*., nor "allow the consumer to cancel" before they pay for a Nord Subscription, *id*. In fact, the email does not include any disclosure whatsoever about how to cancel a Nord Subscription.

72. Moreover, Defendants' receipt email does not include other automatic renewal offer terms beyond cancellation policy that the ARL requires be included in a post-purchase acknowledgment email, *id*., including "clear and conspicuous" disclosure "that the subscription or purchasing agreement will continue until the consumer cancels," G.B.L. § 527(2)(a), that the amount of any recurring charge and that the amount may change, *id*. § 527(2)(c), or the length of the automatic renewal term, *id.* § 527(2)(d).

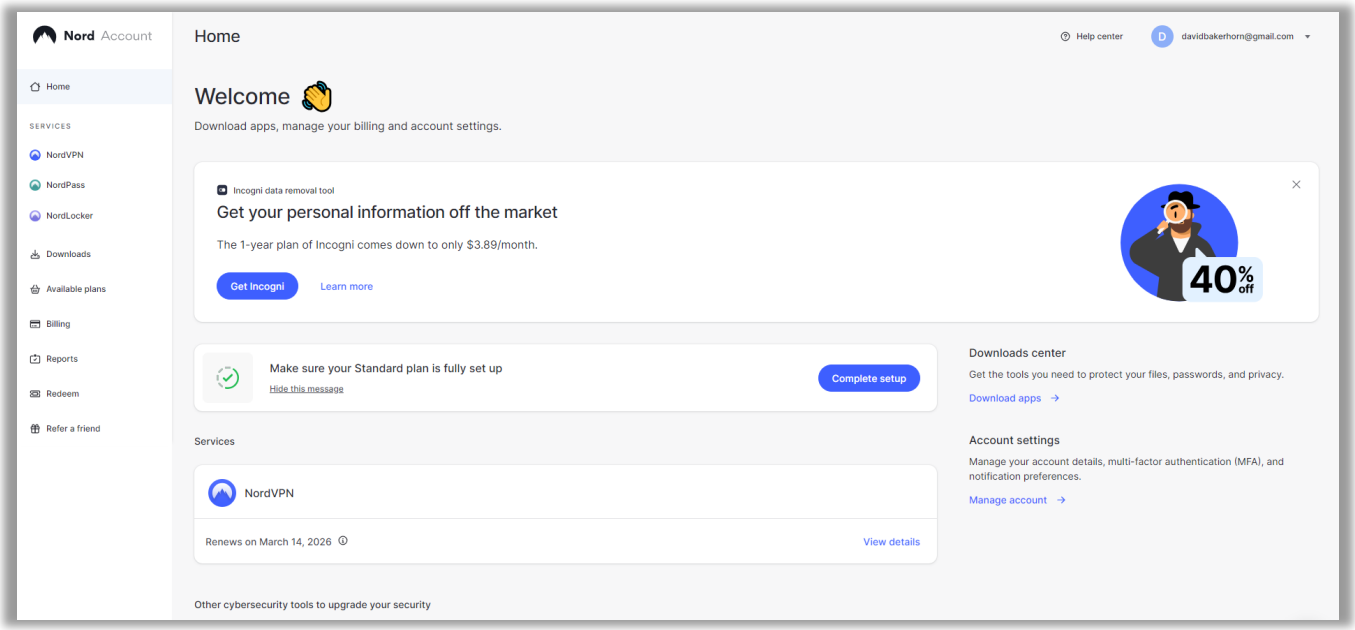
73. Nord Security's failure to comply with the ARL's protections injured Plaintiff and Class Members.

D. Nord Security's Material Misrepresentations and Omissions Regarding Cancellation Process Violates the ARL.

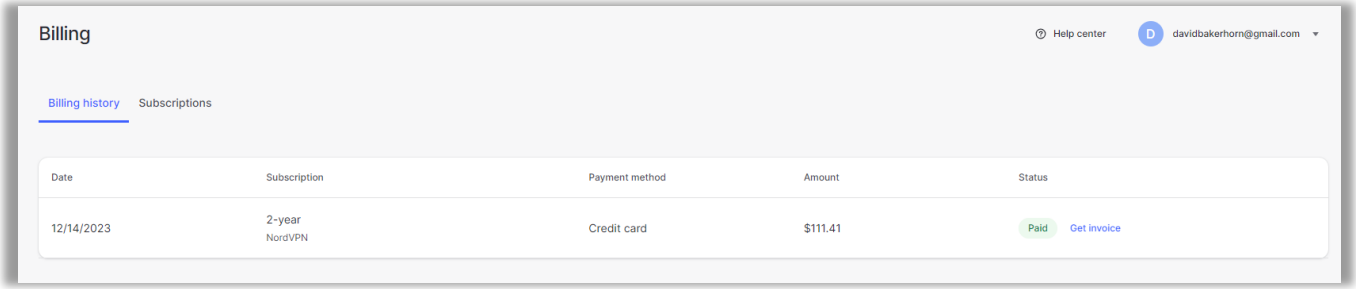
74. Nord Security's cancellation process is not cost-effective, timely, nor easy-to-use. G.B.L. § 527-a(2). Instead, Nord Security employs the "roach motel" dark pattern strategy: it is easy to sign up for Nord Security products and services, but hard to get out.

75. Nord Security buries its cancellation mechanism four layers deep in its customer account portal, with no clear path evident to the consumer for how to get there. Canceling a Nord Security subscription first requires consumers to (1) log into their customer account, and (2) select "Billing" from a list of at least nine options. Once "Billing" is selected, the default view on the "Billing" page does not mention anything about cancellation, and instead shows the consumer's "Billing history." Upon information and belief, Nord Security's "Home" and "Billing" pages available to Plaintiff in December 2023 when he enrolled in Incogni were materially similar to the Home and Billing pages copied below and on the next page:

Home:

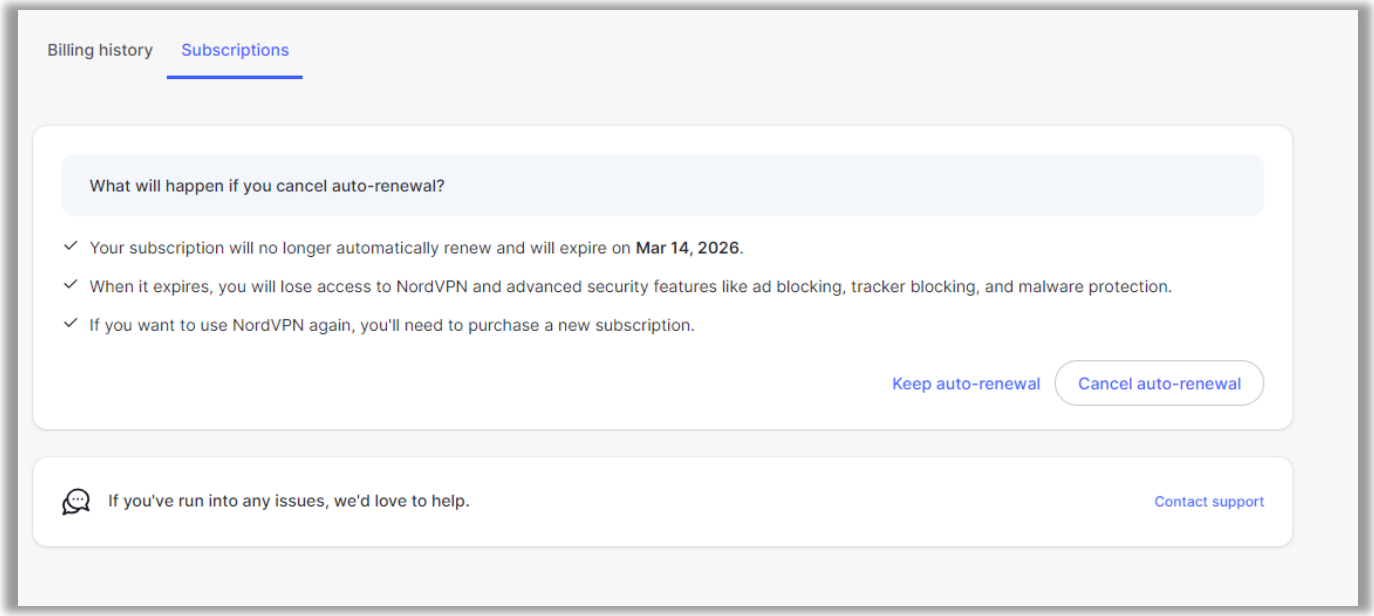


Billing:

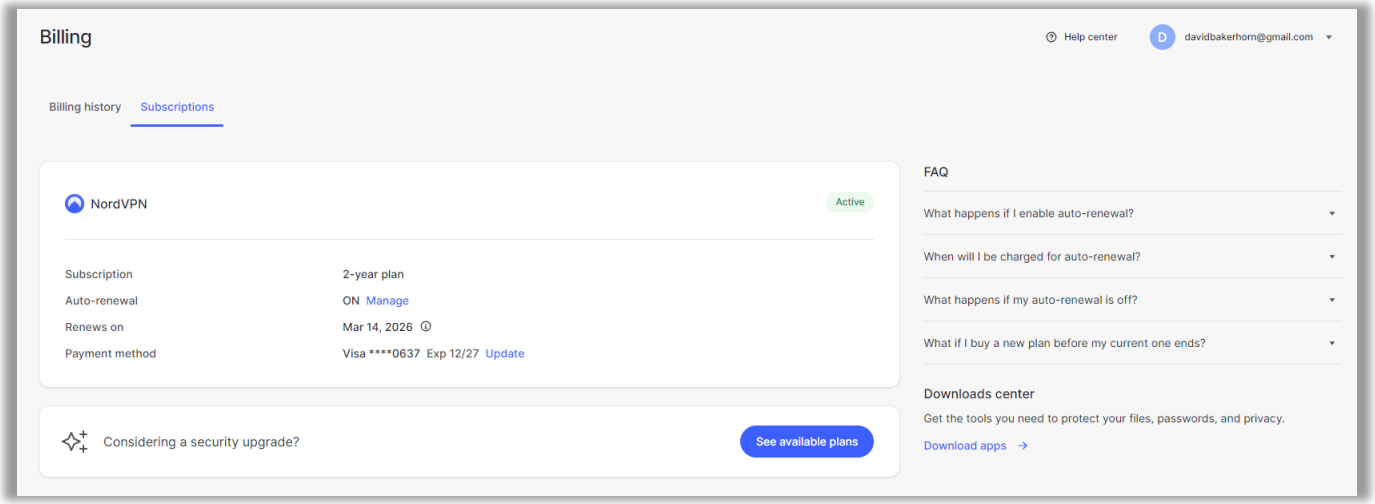


76. After navigating to Nord Security's "Billing page," consumers wishing to cancel must then (3) figure out how to navigate to the "Subscriptions" tab on the "Billing" page. Once customers access the "Subscriptions" tab, they are still not presented with a "Cancel" option. Instead, consumers must then (4) understand that they need to click on "Manage" on a line pertaining to "Auto-renewal" to finally access a page where they can cancel their account. Upon information and belief, Nord Security's "Subscriptions" tab available to Plaintiff in or around December 2023 was materially similar to the image below, as well as the page consumers view when they click "Manage" next to "Auto-renewal," in the image on the following page:

Subscriptions Tab:



After Clicking "Manage:"



77. For consumers who manage to find and click "Cancel auto-renewal," the autorenewal is finally canceled. But Nord Security's multi-step cancellation process is specifically and intentionally designed to thwart cancellation—a "roach motel" dark pattern—that prevents consumers from finding and canceling autorenewal. This violates the ARL because it is not cost-effective, timely, or easy-to-use. G.B.L § 527-a(2). Nor does Nord Security provide a toll-free telephone number or electronic mail address consumers may contact to cancel the automatic renewal. *Id.*

78. For those consumers who use Nord Security's desktop and mobile applications there is no way in which to cancel autorenewal within those apps. This too violates the ARL. *Id.*

E. Nord Security's Material Misrepresentations and Omissions Regarding Its Billing Practices Deceive Consumers and Violate the ARL.

79. Compounding its subscription scheme, Nord Security employs an unorthodox billing practice: rather than billing consumers for its autorenewing Nord Subscriptions when the consumers' current subscriptions ***end***, Nord Security instead bills them ***14 days beforehand***. Nord has intentionally adopted this billing practice to pad its bottom line.

80. Worse still, Nord Security obscures information about its unorthodox billing practices by deliberately scattering confusing, inconsistent, and inaccurate provisions addressing its automatic renewal offer across multiple sections of its "terms" and "terms of service" document" (which total more than 9,500 words), burying them inconspicuously in dense surrounding text.

81. For example, upon information and belief the then-most recent version of Nord Security's "terms of service" at the time Plaintiff enrolled in his Nord Subscription for the Incongi product contained a paragraph labeled "Auto-Renewal," which reads as follows:

> 3.2 **Auto-Renewal**. After the end of your Service period, your Subscription will automatically renew for the successive defined Service periods at the renewal dates, unless you decide to cancel the Subscription renewal before the day of the charge. If you do not cancel the Subscription in such due course, your chosen payment method will be charged the then-current renewal price for the upcoming defined Service period.

82. This "Auto-Renewal" paragraph gives reasonable consumers the impression that they will be charged only ***after*** the original subscription ends. Meanwhile, a separate Nord Security "terms" document reveals, in a paragraph not cross referenced in the "Auto-Renewal" paragraph above, that customers on plans lasting greater than a month will be charged in advance: "at least fourteen (14) days before" the scheduled auto-renewal. This provision is itself in conflict with another provision in the same "terms" document, which provides that "***[a]fter the end*** of your first Subscription period, your Subscription ***will be automatically renewed*** for an additional term . . . . You will ***be charged*** the ***then-current price*** . . . valid ***at the time of your renewal***." (emphasis added). In other words, this paragraph in the "terms" document expressly states that the consumer will ***not*** be charged until "after" the subscription period ends, not "at least fourteen days" before.

F. Nord Security's Insufficient Autorenewal "Notice" Violates the ARL

83. Nord Security offers subscriptions with an initial plan term of one year or longer that later automatically renew for paid terms of six months or longer. For customers with such subscriptions, under the ARL Nord Security must provide notice of the upcoming automatic renewal "at least 15 days before, but not more than forty-five days before, the cancellation deadline[.]" GBL § 527-a(3)(b). That notice must inform the consumer of the upcoming charge to his or her account and "shall include instructions on how to cancel such renewal charge" before the deadline by which the consumer must do so to avoid additional charges. *Id*.

84. During the Class period (*see infra* ¶ 123) and upon information and belief, Nord Security violated the ARL's requirement that it provide statutorily-compliant advanced notice of the autorenewal by misleading consumers as to the date and/or time by which they must cancel the autorenewal to avoid an additional charge.

85. For example, and upon information and belief, Nord Security sent New York customers a notice email that listed the date on which the recipient's subscription period expires (for example, "December 1st"). Nord Security's email intentionally misled consumers into thinking that they could avoid an autorenewal charge if they cancel by the subscription expiration date, when in reality Nord Security employs the unorthodox billing practice of charging customers 14 days ***before*** the subscription expiration date.

86. Moreover, upon information and belief the notice email Nord Security sent New York customers during the Class period also omitted the ***time*** a consumer must cancel their subscription in order to avoid future charges, suggesting to reasonable consumers that they had up to and through 11:59 PM on a particular date when in fact that would be charged at an undisclosed time on that date.

87. Moreover, upon information and belief, notice emails Nord Security sent during the Class Period did not "include instructions on how to cancel such renewal charge," GBL § 527-a(3)(b), and instead simply stated that the customer must "cancel" to avoid a charge with no information whatsoever on how to do so.

88. Upon information and belief, the notice email that Nord Security sent New York customers during the Class period prior to automatic renewal contrasted starkly with the receipt email Nord Security sent ***after*** a consumer was charged for automatic renewal—and when it was too late to cancel and avoid the charge. Upon information and belief, that email at least attempted to provide consumers with clues on how to cancel, including stating that the consumer "can manage [their] subscription here" where "here" was a hyperlink to a login page for Nord Security's account dashboard. It also advised that the consumer could "cancel a recurring subscription from your Nord Account."

G. Nord Security Violates the ARL's Requirements with Respect to Material Changes to Consumers' Automatic Renewal Terms

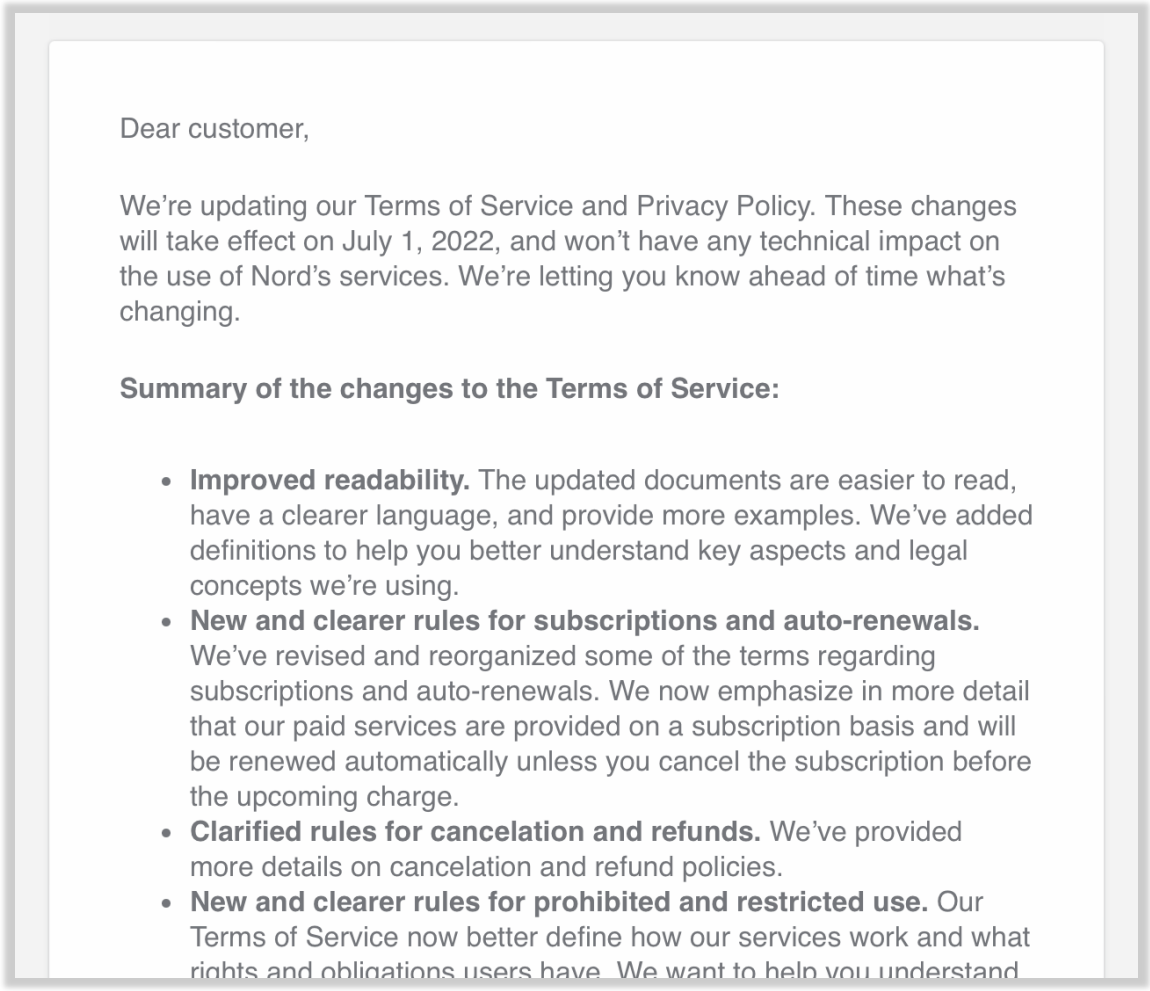
89. During the Class period (*see infra* ¶ 123), Nord Security violated the ARL's requirement that it provide customers with a clear and conspicuous notice of material changes to the automatic renewal terms applicable their accounts.

90. For example, and upon information and belief, on June 15, 2022, Nord Security sent New York consumers an email regarding updates to Nord Security's "Terms of Service" effective July 1, 2022. In relevant part, the email states that Nord Security made the following changes:

- "**New and clearer rules for subscriptions and auto-renewals.** We've revised and reorganized some of the terms regarding subscriptions and auto-renewals. We now emphasize in more detail that our paid services are provided on a subscription basis and will be renewed automatically unless you cancel the subscription before the upcoming charge."

- "**Clarified rules for cancelation and refunds.** We've provided more details on cancelation and refund policies."

91. An excerpt of the June 15, 2022 email sent is reproduced below:



Dear customer,

We're updating our Terms of Service and Privacy Policy. These changes will take effect on July 1, 2022, and won't have any technical impact on the use of Nord's services. We're letting you know ahead of time what's changing.

Summary of the changes to the Terms of Service:

- **Improved readability.** The updated documents are easier to read, have a clearer language, and provide more examples. We've added definitions to help you better understand key aspects and legal concepts we're using.
- **New and clearer rules for subscriptions and auto-renewals.** We've revised and reorganized some of the terms regarding subscriptions and auto-renewals. We now emphasize in more detail that our paid services are provided on a subscription basis and will be renewed automatically unless you cancel the subscription before the upcoming charge.
- **Clarified rules for cancelation and refunds.** We've provided more details on cancelation and refund policies.
- **New and clearer rules for prohibited and restricted use.** Our Terms of Service now better define how our services work and what rights and obligations users have. We want to help you understand

92. The June 15, 2022 email fails to comply with the ARL's material change provision because it does not provide clear and conspicuous notice of the changes that would be made to consumers' existing autorenewal terms on July 1, 2022. G.B.L. § 527-a(4). Instead, the email offers only vague statements that changes will be made and makes no distinction as to the format for the material changes to customers' automatic renewal terms and all other changes to Nord Security's "Terms of Service" more broadly (bullet point with bolded clause followed by unbolded sentence(s)).

93. The June 15, 2022 email also fails to comply with the ARL's material change provision because it does not "include instructions on how to cancel." *Id*.

94. The changes Nord Security made to its automatic renewal terms on July 1, 2022 were material. For example, the June 15, 2022 email states that the Terms of Service will be changed to provide "more details on cancelation and refund polices." A "description of the cancellation policy that applies" is one of the automatic renewal offer terms that must be disclosed to consumers under the ARL, G.B.L. § 527-a(2)(b), and thus notice of any material changes to that policy must be made in a manner that complies with G.B.L. § 527(4), which Nord Security's June 15, 2022 email fails to do.

95. During the Class period and upon information and belief, Nord Security's "notice" emails sent before a customer's subscription is automatically renewed, as described above at ¶¶ 83–88, likewise contained material changes to automatic renewal terms, including the length of the subscription term and the price. Those emails also failed to comply with the ARL's material change provision because they did not "include instructions on how to cancel." G.B.L. § 527(4).

H. How Nord Security's Subscription Scheme Injured Plaintiff

96. Plaintiff was injured by Nord Security's unlawful and deceptive subscription scheme because had Plaintiff known that he was enrolling in an automatically renewing Nord Subscription when he purchased Defendants' NordVPN and Incogni product offerings in 2023, he would not have purchased them.

97. On or about October 19, 2023, Plaintiff enrolled in a two-year subscription to Nord Security's NordVPN product offering for $87.89.

98. Nord Security deceived Plaintiff into believing that once his two-year plan period was over, he would no longer be subscribed to NordVPN.

99. After Plaintiff purchased NordVPN, Nord Security advertised its Incogni product to Plaintiff.

100. Plaintiff thereafter decided to purchase Incogni.

101. On or about December 16, 2023, Plaintiff enrolled in a one-year subscription to Nord Security's Incogni product offering.

102. On December 16, 2023, Plaintiff received a receipt from Nord Security for 56.02 Euros for the Incogni product offering. This receipt reflected Plaintiff's payment for one year of Incogni using PayPal, which converted the price to $64.21 (US).

103. Nord Security deceived Plaintiff into believing that once his one-year plan period was over, he would no longer be subscribed to Incogni.

104. As a result of Defendants' material misrepresentations and omissions, including their NY ARL violations, Plaintiff never expected to pay Nord Security anything for Incogni beyond what he had already paid in December 2023. Nord Security did not adequately disclose to Plaintiff that it would begin charging non-refundable recurring Incogni fees on a yearly basis.

105. Nonetheless, on or about December 2, 2024, Plaintiff discovered that Nord Security had charged his PayPal account 107.86 Euros for a one-year Incogni subscription, which PayPal converted to a purchase price of $119.08 (US).

106. After seeing Nord Security's charges Plaintiff tried to cancel his NordVPN and Incogni subscriptions but was unable to figure out how to do so.

107. Because he never authorized Nord Security to charge him for additional years of Incongi, Plaintiff then cancelled autorenewal of his Nord Subscriptions to both Incogni and NordVPN with the assistance of his counsel.

108. Nord Security did not provide "clear and conspicuous" disclosures to Plaintiff that it would automatically renew his two Nord Subscriptions. This information is not clearly and conspicuously provided in the contract offers made on Nord Security's website, in any hyperlinked terms on the website, or in any post-purchase acknowledgement or receipt email.

109. Similarly, Nord Security did not provide "clear and conspicuous" disclosures to Plaintiff about how he could cancel his Nord Security subscriptions. This information is not clearly and conspicuously provided in the contract offers made on Nord Security's website, in any hyperlinked terms on the website, or in any post-purchase acknowledgement or receipt email.

110. Plaintiff did not authorize or want his Nord Subscriptions to renew.

111. Plaintiff was injured in December 2024 when Nord Security charged his PayPal account 107.86 Euros ($119.08 (US)) for a one-year subscription to Incogni he did not want and did not want to pay for.

112. After requesting a refund via PayPal, Plaintiff received a refund of 107.86 Euros from Defendant Nordsec B.V. on or around December 19, 2024.

113. Plaintiff was further injured by Nord Security's subscription scheme because had he known the truth about Nord Security's intentionally misleading subscription practices, he would not have purchased either Nord VPN or Incogni.

114. Plaintiff intends to purchase products and services in the future for himself from internet security companies, including Nord Security, as long as he can gain some confidence in Nord Security's representations about its products and services and subscription practices, including autorenewal and cancellation. Moreover, Nord Security still has Plaintiff's payment information and could use it process unauthorized payments in the future.

115. Given that Nord Security has engaged in a series of deceptive acts and omissions for which it billed consumers and consumers continued to pay, the continuing violation doctrine applies, effectively tolling the limitations period until the date of Nord Security's last wrongful act against Plaintiff, which was in December 2024, when Nord Security last charged Plaintiff for an automatically renewing subscription he did not want and did not want to pay for.

RULE 9(B) ALLEGATIONS

116. To the extent necessary, as detailed in the paragraphs above and below, Plaintiff has satisfied the requirements of Rule 9(b) by establishing the following elements with sufficient particularity:

117. **WHO**: Defendants and their instrumentalities and alter egos, through a single fictitious entity called Nord Security by which they collectively hold themselves out to the public, sell services to consumers in New York through a deceptive subscription scheme by making the material misrepresentations and omissions alleged in detail above in violation of New York consumer protection statutes and the common law, including with respect to automatic renewal and cancellation, leaving many consumers who sign up for a Nord Security product offering paying for subscriptions that they do not want.

118. **WHAT**:

- Nord Security conducts its deceptive subscription scheme by failing to clearly and conspicuously disclose the Company's terms and conditions to customers, including how to cancel a subscription. For example, instead of clearly explaining to the consumer what they are actually getting into, Nord Security requires customers to scroll to find the relevant (and inadequate) fine print on its payment page and buries the key provisions in confusing, inconsistent, and inaccurate terms scattered across multiple sections of at least two fine print documents.

- Nord Security conducts its deceptive subscription scheme by subjecting Nord Security customers to an exceedingly difficult cancellation process that requires consumers to figure out—with no help from the Company—the entirely unorthodox process of navigating Nord

Security's account settings to find a buried feature labelled "Auto-renewal" and turning it to "OFF" (rather than, for example, by clicking a button clearly and prominently labelled, "CANCEL SUBSCRIPTION"). And for those consumers who contact the Company directly prior to the end of their subscription period to cancel, Nord Security refuses to cancel any upcoming payments and instead only turns off autorenewal for later payments. Nord Security's cancellation process is intentionally difficult to navigate and complete in order to trap consumers into paying for recurring Nord Security subscriptions that they do not want.

- Nord Security conducts its deceptive subscription scheme by failing to meet the post purchase requirements that the ARL imposes on an automatically renewing product or service. Nord Security does not provide "an acknowledgment that includes the automatic renewal or continuous service offer terms, cancellation policy, and information regarding how to cancel in a manner that is capable of being retained by the consumer," G.B.L. § 527-a(1)(c). In fact, Nord Security's receipt email does not include any disclosure whatsoever about how to cancel a Nord Security subscription.

- Nord Security conducts its deceptive subscription scheme by employing a highly unconventional charging practice. Rather than automatically renew consumers by charging their stored payment methods at the beginning of a new subscription period if they do not cancel before the prior subscription is over, Nord Security extracts its charges 14 days ***before the customer's current subscription period even ends***. By doing so, Nord Security locks consumers into another yearlong subscription well before any reasonable consumer would expect to be auto-renewed, allowing Nord Security to collect and keep payment from consumers who do not wish to remain Nord Security customers.

- Nord Security conducts its deceptive subscription scheme by failing to meet the requirements to notify customers about forthcoming automatic subscription renewals, including by failing to: (1) "include instructions on how to cancel such renewal charge;" and (2) utilize a cancellation mechanism that is "cost-effective, timely, and easy-to-use." G.B.L. § 527-a(2). Nord Security also actively misleads consumers in supposed "notice" emails that provide the subscription end date without making clear that to avoid a future charge the customer must cancel at least 14 days before that date.

- Nord Security conducts its deceptive and unlawful subscription scheme by failing to provide clear and conspicuous notice of material changes to customers' existing autorenewal terms and failing to provide information regarding how to cancel in a manner that may be retained by consumers in connection with those material changes.

119. **WHERE**: Nord Security's deceptive and unlawful subscription scheme is conducted through its website, mobile/tablet/desktop applications, and electronic communications with customers.

120. **WHEN**: Nord Security has been engaging in its deceptive and unlawful subscription scheme for years, and the scheme is ongoing. For specific examples, Nord Security used its deceptive and unlawful subscription practices scheme when Plaintiff first enrolled in a Nord Security subscription in October 2023 and again in December 2023 and through Nord Security's receipt emails sent to Plaintiff, Nord Security's "terms of service" and "terms" hyperlinks, and Plaintiff's unsuccessful attempt to cancel his account after learning that Nord Security had charged him for an unwanted automatic renewal. Nord Security uses the same or substantially similar deceptive and unlawful subscription practices scheme for all of its customers.

121. **WHY**: Nord Security uses its deceptive and unlawful subscription scheme in order to trap Nord Security customers into paying for Nord Security subscriptions that they do not want. As a direct result of this scheme, Defendants have successfully reaped tens of millions in unlawful charges at the expense of unsuspecting customers.

122. **HOW**: Nord Security conducts its deceptive and unlawful practices scheme by making the material misrepresentations and omissions alleged in detail above in violation of New York consumer protection law and the common law.

CLASS ACTION ALLEGATIONS

123. Plaintiff brings this action on his own behalf and additionally, pursuant to Rule 23(b)(2) and (3) of the Federal Rules of Civil Procedure, on behalf of a class that is preliminarily defined as all Nord Security customers in New York (including customers of companies Nord Security acts as a successor to) who were automatically enrolled into and charged

for at least one month of Nord Security membership by Defendants at any time from the applicable statute of limitations period to the date of judgment (the "Class").

124. As alleged throughout this Complaint, the Class's claims all derive directly from a single course of conduct by Defendants. Defendants have engaged in uniform and standardized conduct toward the Class and this case is about the responsibility of Defendants, at law and in equity, for their knowledge and conduct in deceiving their customers. Defendants' conduct did not meaningfully differ among individual Class Members in their degree of care or candor, their actions or inactions, or in their false and misleading statements or omissions. The objective facts on these subjects are the same for all Class Members.

125. Excluded from the Class are Defendants; any parent, subsidiary, or affiliate of Defendants; any entity in which Defendants have or had a controlling interest, or which Defendants otherwise control or controlled; and any officer, director, employee, legal representative, predecessor, successor, or assignee of Defendants. Also excluded are federal, state and local government entities; and any judge, justice, or judicial officer presiding over this action and the members of their immediate families and judicial staff.

126. Plaintiff reserves the right, as might be necessary or appropriate, to modify or amend the definition of the Class and/or add Subclasses, when Plaintiff files his motion for class certification.

127. Plaintiff does not know the exact size of the Class since such information is in the exclusive control of Defendants. Plaintiff believes, however, that the Class encompasses thousands of consumers whose identities can be readily ascertained from Nord Security's records. Accordingly, the members of the Class are so numerous that joinder of all such persons is impracticable.

128. The Class is ascertainable because its members can be readily identified using data and information kept by Defendants in the usual course of business and within their control. Plaintiff anticipates providing appropriate notice to each Class Member in compliance with all applicable federal rules.

129. Plaintiff is an adequate class representative. Plaintiff's claims are typical of the claims of the Class and do not conflict with the interests of any other members of the Class. Plaintiff and the other members of the Class were subject to the same or similar conduct engineered by Defendants. Further, Plaintiff and members of the Class sustained substantially the same injuries and damages arising out of Defendants' conduct.

130. Plaintiff will fairly and adequately protect the interests of all Class Members. Plaintiff has retained competent and experienced class action attorneys to represent his interests and those of the Class.

131. Questions of law and fact are common to the Class and predominate over any questions affecting only individual Class members, and a class action will generate common answers to the questions below, which are apt to drive the resolution of this action:

a. Whether Defendants' conduct violates the New York ARL;

b. Whether Defendants' conduct violates New York G.B.L. § 349;

c. Whether Defendants' conduct violates the applicable common law doctrines;

d. Whether Defendants were unjustly enriched as a result of their conduct;

e. Whether Class Members have been injured by Defendants' conduct;

f. Whether, and to what extent, equitable relief should be imposed on Defendants to prevent them from continuing their unlawful practices; and

g. The extent of class-wide injury and the measure of damages for those injuries.

132. A class action is superior to all other available methods for resolving this controversy because: (1) the prosecution of separate actions by Class Members will create a risk of adjudications with respect to individual Class Members that will, as a practical matter, be dispositive of the interests of the other Class Members not parties to this action, or substantially impair or impede their ability to protect their interests; (2) the prosecution of separate actions by Class Members will create a risk of inconsistent or varying adjudications with respect to individual Class Members, which will establish incompatible standards for Defendants' conduct; (3) Defendants have acted or refused to act on grounds generally applicable to all Class Members; and (4) questions of law and fact common to the Class predominate over any questions affecting only individual Class Members.

133. Further, the following issues are also appropriately resolved on a class-wide basis under Federal Rule of Civil Procedure 23(c)(4):

a. Whether Defendants' conduct violates the ARL;

b. Whether Defendants' conduct violates New York G.B.L. § 349;

c. Whether Defendants' conduct violates the applicable common law doctrines;

d. Whether Defendants were unjustly enriched as a result of their conduct;

e. Whether Class Members have been injured by Defendants' conduct;

f. Whether, and to what extent, equitable relief should be imposed on Defendants to prevent them from continuing their unlawful practices.

134. Accordingly, this action satisfies the requirements set forth under Rules 23(a), (b)(2), (b)(3), and (c)(4) of the Federal Rules of Civil Procedure.

COUNT I

NEW YORK GENERAL BUSINESS LAW § 349

135. Plaintiff incorporates by reference all preceding and subsequent paragraphs.

136. Plaintiff brings this claim under GBL § 349 on his own behalf and on behalf of each member of the Class.

137. New York's consumer fraud statute prohibits "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state." G.B.L. § 349.

138. Defendants' subscription scheme and its associated practices are consumer-oriented in that they are directed at members of the consuming public.

139. By engineering and implementing materially misleading subscription scheme alleged in this complaint, Defendants engaged in, and continue to engage in, deceptive acts and practices in violation of New York's G.B.L. § 349.

140. Through their deceptive subscription scheme as alleged throughout this Complaint, Defendants engaged in deceptive acts or practices that violated G.B.L. § 349 by making the material misrepresentations and omissions including with respect to automatic renewal and cancellation, leaving many consumers who sign up for a Nord Security service paying for subscriptions that they do not want. Defendants systematically misrepresented, concealed, suppressed, and omitted material facts relating to the automatic renewal and cancellation of Nord Security products and services in the course of their business.

141. By violating New York's ARL as alleged throughout this Complaint, Defendants are liable to Plaintiff and the Class for committing a deceptive act.

142. The aforementioned acts are unfair, unconscionable and deceptive and are contrary to the public policy of New York, which aims to protect consumers.

143. Defendants knew or should have known that their conduct violated G.B.L. §§ 349, 527, and 527-a.

144. As a direct and proximate result of Defendants' unlawful and deceptive subscription scheme and associated practices, Plaintiff and the Class has suffered injury and monetary damages in an amount to be determined at the trial of this action and upon information and belief, believed to exceed $50 million.

145. Plaintiffs and the members of the Class further seek equitable relief against Defendants. Defendants' violations present a continuing risk to Plaintiff and Class Members, as well as to the general public. Defendants' unlawful acts and practices complained of herein affect the public interest. Defendants' unfair and deceptive acts or practices occurred repeatedly in Defendants' trade or business and significant impacts a substantial portion of the purchasing public as actual or potential customers of Defendants. Pursuant to G.B.L. § 349, this Court has the power to award such relief, including but not limited to, an order declaring Defendants' practices to be unlawful, an order enjoining Defendants from engaging in any further unlawful conduct, and an order directing Defendants to refund to Plaintiff and the Class all fees wrongfully assessed and/or collected.

COUNT II

CONVERSION

146. Plaintiff incorporates by reference all preceding and subsequent paragraphs.

147. Plaintiff brings this claim on his own behalf and on behalf of each member of the Class.

148. Plaintiff and the Class own and have a right to possess the money that is in their respective bank accounts, internet payment accounts, and/or credit cards.

149. Defendants substantially interfered with Plaintiff and the Class's possession of this money by knowingly and intentionally making unauthorized charges to their bank accounts, internet payment accounts, and/or credit cards for Nord Security subscriptions.

150. Plaintiff and the Class never consented to Defendants taking of this money from their bank accounts, internet payment accounts, and/or credit cards.

151. Defendants wrongfully retained dominion over this monetary property and/or the time-value of the monetary property.

152. Plaintiff and the Class have been damaged by Defendants' wrongful taking and/or possession of such money from their bank accounts, internet payment accounts, and/or credit cards in an amount that is capable of identification through Defendants' records.

153. By reason of the foregoing, Defendants are liable to Plaintiff and the Class for conversion in an amount to be proved at trial.

COUNT III

UNJUST ENRICHMENT

154. Plaintiff incorporates by reference all preceding and subsequent paragraphs.

155. Plaintiff brings this claim on his own behalf and on behalf of each member of the Class.

156. As a result of Defendants' violations of the NY ARL, "any goods, wares, merchandise, or products" delivered to Plaintiff and the Class are "deemed an unconditional gift to the consumer . . . without any obligation whatsoever on the consumers part." G.B.L. § 527-a(6). Any contract between Plaintiff and Defendants is therefore void and unenforceable.

157. By reason of Defendants' wrongful conduct, Defendants have benefited from receipt and maintenance of improper funds, and under principles of equity and good conscience, Defendants should not be permitted to keep this money.

158. As a result of their unjust conduct, Defendants have been unjustly enriched.

159. As a result of Defendants' conduct it would be unjust and/or inequitable for Defendants to retain the benefits of its conduct without restitution to Plaintiff and the Class. Accordingly, Defendants must account to Plaintiff and the Class for their unjust enrichment.

COUNT IV

MONEYS HAD AND RECEIVED

160. Plaintiff incorporates by reference all preceding and subsequent paragraphs.

161. Plaintiff brings this claim on his own behalf and on behalf of each member of the Class.

162. Defendants received moneys from Plaintiff and from each member of the Class.

163. As a result of Defendants' violations of the NY ARL, "any goods, wares, merchandise, or products" delivered to Plaintiff and the Class are "deemed an unconditional gift to the consumer . . . without any obligation whatsoever on the consumers part." G.B.L. § 527-a(6). Any contract between Plaintiff and Defendants is therefore void and unenforceable.

164. The moneys belong to Plaintiff and each member of the Class.

165. Defendants have not returned the moneys.

166. Plaintiff, on behalf of himself and the members of the Class, seeks the return of the moneys in an amount to be proved at trial.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that the Court:

(a) Issue an order certifying the Class defined above, appointing the Plaintiff as Class representative, and designating Wittels McInturff Palikovic and Milberg Coleman Bryson Phillips Grossman, PLLC as Class Counsel;

(b) Find that Defendants have committed the violations of law alleged herein;

(c) Determine that Defendants have been unjustly enriched as a result of their wrongful conduct, and enter an appropriate order awarding restitution and monetary damages to the Class;

(d) Enter an order granting all appropriate relief including injunctive relief on behalf of the Class under the applicable laws;

(e) Render an award of compensatory damages of at least $50,000,000, the exact amount of which is to be determined at trial;

(f) Issue an injunction or other appropriate equitable relief requiring Defendants to refrain from engaging in the deceptive practices alleged herein;

(g) Declare that Defendants have committed the violations of law alleged herein;

(h) Render an award of punitive damages;

(i) Enter judgment including interest, costs, reasonable attorneys' fees, costs, and expenses; and

(j) Grant all such other relief as the Court deems appropriate.

Dated: March 28, 2025

WITTELS MCINTURFF PALIKOVIC
/s/ J. Burkett McInturff
J. Burkett McInturff
305 BROADWAY, 7TH FLOOR
NEW YORK, NEW YORK 10007
Tel: (914) 775-8862
jbm@wittelslaw.com

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
Scott C. Harris*
900 W. MORGAN STREET
RALEIGH, NORTH CAROLINA 27603
Tel: 919-600-5000
sharris@milberg.com

* *Pro Hac Application Forthcoming*

Co-Counsel for Plaintiff and the Proposed Class