

**UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS**

RENE TIO,

on behalf of himself and all others similarly
situated,

Plaintiff,

v.

**NORDVPN S.A., AND TEFINCOM S.A.
D/B/A NORDVPN,**

Defendants.

Civil Case No.:

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Rene Tio (“Plaintiff”), by his undersigned attorneys Bryson, Harris, Suci, & Demay, PLLC, and Wittels McInturff Palikovic, brings this consumer protection action in his individual capacity and on behalf of a class of Massachusetts consumers defined below against Defendants Nordvpn S.A. and Tefincom SA d/b/a NordVPN (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 challenges Nord Security’s use of deceptive and unlawful “automatic renewal” charging practices that saddle consumers with premature subscription renewal fees that are higher than previously agreed. When consumers seek timely refunds of these early and inflated autorenewal charges, Nord Security rejects their requests.

2. Nord Security offers a suite of products and services that claim to provide internet users with privacy and protection from cybersecurity threats. Those offerings include a virtual

private network (“VPN”) service called “NordVPN,”¹ a password manager called “NordPass,” and an encrypted cloud storage service called “NordLocker.” These products and services are referred to herein as the “Nord Subscriptions.”

3. This proposed class action lawsuit arises from three deceptive practices Nord Security deploys in connection with the Nord Subscriptions. **First**, the Nord Subscriptions are for a pre-set time period (i.e. one year), yet rather than waiting until that time period lapses, roughly two weeks prior Nord Security automatically renews customers and charges them for another full subscription period, without providing adequate notice of this practice.

4. **Second**, Nord Security’s premature renewal charges are significantly higher than the price consumers initially agreed to pay. Nord Security does not adequately disclose that its renewal prices are significantly higher. In both its enrollment flows and post-purchase communications, Nord Security obscures or entirely omits the material terms that reasonable consumers need to make an informed purchasing decision.

5. **Third**, Nord Security prominently advertises a “30-day money-back guarantee”—but secretly backdates that guarantee to the date of the premature renewal charge. As a result, by the time consumers discover the unauthorized, higher-priced renewal fee and try to cancel, the 30-day refund period has already expired or nearly expired.

6. The Nord Subscriptions use a “negative option” billing tactic, which the Consumer Financial Protection Bureau (“CFPB”) defines as “a term or condition under which a seller may

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 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).

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 The CFPB cautions that “[n]egative option programs can cause serious harm to consumers,” which “is most likely to occur when sellers [1] mislead consumers about terms and conditions, [2] fail to obtain consumers’ informed consent, or [3] make it difficult for consumers to cancel.”³

7. The three Nord Security subscription practices challenged in this lawsuit hit the CFPB’s warning trifecta. These practices are intentionally designed to trick consumers into paying unwanted subscription fees at higher prices than they originally agreed to, and to frustrate their efforts to avoid subscription renewal and timely get their money back.

8. That is exactly what happened here, where Plaintiff enrolled in a Nord Subscription at an agreed-upon price, only to be renewed two weeks before the end of his subscription at a rate that was essentially double the rate he had agreed to pay. Then, when that renewed subscription was coming to an end, Nord Security again charged him two weeks early and levied a fee that was 50% higher than the prior subscription rate. When Plaintiff discovered the premature charge and sought a refund within 30 days of the end of his subscription term, Nord Security refused to provide it—on the basis that the “30 day” period started not from the date of the new subscription term, but from the much earlier date when Nord Security secretly charged Plaintiff for the new term.

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.

³ *Id.* at 2.

THE UNIFORM WEB OF NORD SECURITY'S NEGATIVE OPTION SCHEME

9. Nord Security traps consumers into pricey, 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 paying premature and higher subscription fees, taken together these components work together to form an intentionally deceptive architecture that is designed to, and does, produce a predictable and unlawful outcome: saddling unwitting consumers with unwanted subscription charges.

10. Nord Security deceives consumers in at least three ways.

11. **First**, Nord Security never discloses its early-renewal practice on its Home Page, *infra* at ¶ 53, Pricing Page, *infra* at ¶ 55, Payment Page, *infra* at ¶ 57, or in its general Terms of Service.⁴ In other words, Nord Security's sign-up screens do not alert consumers that the Company will charge their payment method weeks before the stated renewal date. To the contrary, the fine print of Nord Security's own Terms of Service represent that:

Your service will be automatically renewed, and your chosen payment method will be charged ***at the end of each service period***, unless you decide to cancel your automatic payments for the Service ***before the end of the then-current subscription***.

Terms of Service at § 4 (emphasis added).

⁴ All references to Nord Security's Terms of Service, Pricing Page and Payment Page are to the versions of those in effect on June 29, 2021, Mr. Tio's original date of enrollment in a Nord Subscription.

12. In reality, however, Nord Security processes renewal charges roughly fourteen days before the end of the subscription period for annual subscribers, and roughly five days before the end of the service period for monthly subscribers, contradicting this written promise.

13. The sole evidence of this policy available to the consumer appears in an entirely separate set of terms that is not linked from the enrollment page and that directly conflicts with the Terms of Service. A reasonable consumer reviewing Nord Security's enrollment screens and the hyperlinked Terms of Service would have no reason to expect that Nord Security charges early, in contravention of its own Terms.

14. **Second**, Nord Security does not just charge premature fees; it charges more than the previously agreed subscription fee. Nord Security's Payment Page highlights a single, attractive price while withholding the fact that renewal charges are significantly higher. The Payment Page's lone reference to autorenewal prices is buried below the fold—i.e., the user must scroll down to find it—in tiny, low-contrast gray text on a gray background. Only there does Nord Security say the subscription will be “automatically renewed” at the “then-applicable renewal price,” a phrasing that conceals the key fact that the renewal price is higher, often much higher, than the advertised price. As shown below, Nord Security's Pricing Page deploys similar tactics.

15. **Third**, Nord Security prominently advertises a “30-day money-back guarantee,” signaled on the Payment Page with a bright red shield logo and statements such as “You're 100% backed by our 30-day money-back guarantee.” On its Pricing Page, Nord Security likewise promises that “[a]ll plans come with the 30-day money-back guarantee.” Nord Security's Terms of Service further promise that “[i]f you wish to claim a refund, you can do so within 30 days following your purchase of our Services.” Terms of Service § 5. Nord Security never discloses, in its Terms of Service, in any other terms, or on its Payment or Pricing pages, that for automatic

renewals the 30-day period is measured from the (premature) date Nord Security charges the consumer's payment method, rather than from the start of the renewed term. As a result, consumers seeking a refund or cancellation of the additional subscription do not have the full 30 days Nord Security promised.

16. While a given customer may not be ensnared by all aspects of Nord Security's deceptive subscription web, all Nord Security customers face the same three traps and need only be tricked by one to end up paying a premature and hefty subscription renewal fee.

17. None of this is happenstance. The gauntlet consumers must navigate is 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 and overpriced 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—over, and over, and over again—Nord Security continues to subject the consuming public to its unlawful subscription scheme and to reap significant monetary benefits from its improper conduct.

19. Only through a class action can consumers like Plaintiff 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 Massachusetts, have sufficient minimum contacts with this state, and otherwise purposely avail themselves of the privileges of conducting business in Massachusetts by marketing and selling products and services in Massachusetts. Further, the injuries to Massachusetts consumers that Plaintiff seeks to prevent through public injunctive relief arise directly from Nord Security's continuing conduct in Massachusetts, including, but not limited to, directing its subscription scheme at Massachusetts 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 Rene Tio is a citizen of Massachusetts.

25. Plaintiff 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 Massachusetts 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 Massachusetts 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."⁵

⁵ Nord Security raised another \$100M investment round, NORD SECURITY, <https://nordsecurity.com/blog/nord-security-raised-another-100m-investment-round>.

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.”⁶ Likewise, the “Corporate responsibility” page for “Nord 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,”⁷ which discusses such topics as expectations for the “Nord Security brand products, including NordVPN, NordPass, NordLocker, and NordLayer.”⁸

28. Defendant Nordvpn S.A. is a Panamanian corporation incorporated under the laws of Panama.⁹ Nordvpn S.A.’s principal place of business is in Amsterdam, the Netherlands.¹⁰ Nordvpn S.A. currently “offers” Defendants and non-Defendants NordSec Ltd. and Nord Security Inc.’s products “NordVPN, NordLocker, and NordPass.”¹¹ NordVPN is one of the products Defendants and non-Defendants NordSec Ltd. and Nord Security Inc. marketed and sold to Plaintiff in Massachusetts. Defendant Nordvpn S.A. also currently operates Defendants and non-Defendants NordSec Ltd. and Nord Security Inc.’s website, www.nordvpn.com.¹² Nordvpn S.A.’s

⁶ *Id.*

⁷ Corporate Responsibility, NORD SECURITY, <https://nordsecurity.com/corporate-responsibility>.

⁸ 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.

⁹ *Zeichner v. Nord Security Inc. et al.*, No. 24 Civ 2462 (N.D. Cal.) (“Zeichner”), Dkt. No. 39-1, ¶ 3.

¹⁰ *Id.*

¹¹ *Id.*

¹² *Id.*

corporate parents are non-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.¹³ Nordvpn S.A. shares an unnamed director with Defendant Tefincom S.A.¹⁴

29. Defendant Tefincom S.A. d/b/a NordVPN is a Panamanian corporation incorporated under the laws of Panama.¹⁵ Defendant Tefincom S.A.’s principal place of business is Panama City, Panama.¹⁶ Defendant Tefincom S.A.’s corporate parent is Stichting Raveset.¹⁷ Defendants and non-Defendants NordSec Ltd. and Nord Security Inc. admit that Defendant Tefincom S.A. was the contracting entity for Massachusetts retail consumer VPN services purchased on or before November 15, 2020.¹⁸ 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.¹⁹ NordSec Ltd. is a private limited liability company organized under the laws of England & Wales.²⁰ Defendants and non-Defendants NordSec Ltd. and Nord Security Inc. claim that NordSec Ltd. “once owned the intellectual property of the Nord brand.”²¹

¹³ *Zeichner*, Dkt. No. 37.

¹⁴ *Zeichner*, Dkt. No. 39-1, ¶ 8.

¹⁵ *Zeichner*, Dkt. No. 39-3, ¶ 3.

¹⁶ *Id.*

¹⁷ *Zeichner*, Dkt. No. 38.

¹⁸ *Zeichner*, Dkt. No. 39-3, ¶ 3.

¹⁹ *Zeichner*, Dkt. No. 39-5, ¶ 3.

²⁰ *Id.*

²¹ *Zeichner*, Dkt. No. 39, at 5.

NordSec Ltd.’s corporate parents are Cyberswift B.V., Cyberspace B.V., and Stalwart Holding B.V.²² NordSec Ltd. is also an owner of non-Defendant NordSec B.V.,²³ Defendant Nordvpn S.A.,²⁴ and Nord Security Inc.²⁵ Public records indicate that NordSec Ltd. is a prior owner of the “NordVPN” trademark.

31. Non-Defendant NordSec B.V. is an internet privacy and security company headquartered in Amsterdam, the Netherlands.²⁶ NordSec B.V. is a private limited liability company organized under the laws of the Netherlands.²⁷ Defendants and non-Defendants NordSec Ltd. and Nord Security Inc. claim that NordSec B.V. “currently owns the intellectual property of the Nord brand.”²⁸ NordSec B.V.’s corporate parents are NordSec Ltd. and two of NordSec Ltd.’s corporate parents, Cyberswift B.V. and Cyberspace B.V.²⁹ NordSec B.V. is also an owner of Defendant Nordvpn S.A.³⁰ and Nord Security Inc.³¹ Defendants and non-Defendants NordSec Ltd. and Nord Security Inc.’s website www.nordsecurity.com claims that “Nord Security trademarks,

²² *Zeichner*, Dkt. No. 35.

²³ *Zeichner*, Dkt. No. 36.

²⁴ *Zeichner*, Dkt. No. 37.

²⁵ *Zeichner*, Dkt. No. 27.

²⁶ *Zeichner*, Dkt. No. 39-2, ¶ 3.

²⁷ *Id.*

²⁸ *Zeichner*, Dkt. No. 39, at 5.

²⁹ *Zeichner*, Dkt. No. 36.

³⁰ *Zeichner*, Dkt. No. 37.

³¹ *Zeichner*, Dkt. No. 27.

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’).”³² 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.

32. Non-Defendant Nord Security Inc. is a Delaware corporation.³³ Nord Security Inc.’s corporate parents are NordSec B.V., NordSec Ltd., and Cyberswift B.V.,³⁴ which is also a corporate parent of NordSec B.V.³⁵ and NordSec Ltd.³⁶ 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 consumers like Plaintiff, instead claiming that Nord Security Inc. provides only business-to-business services.³⁷

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

³² Nord Security Trademark and Brand Guidelines, NORD SECURITY, <https://nordsecurity.com/trademark-policy>.

³³ *Zeichner*, Dkt. No. 27.

³⁴ *Id.*

³⁵ *Zeichner*, Dkt. No. 36.

³⁶ *Zeichner*, Dkt. No. 35.

³⁷ *Zeichner*, Dkt. No. 39, at 5.

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.”³⁸ 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.”³⁹ Tom Okman and Eimantas Sabaliauskas are listed as directors of NordSec Ltd., but their respective LinkedIn pages claim they are co-founders of “Nord Security.”⁴⁰

34. Upon information and belief, Defendants and non-Defendants NordSec B.V., 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 B.V., 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 B.V., 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 B.V., NordSec Ltd. and Nord Security Inc. represent is the website

³⁸ “The founders and owners of NordVPN,” NORDVPN.COM, <https://support.nordvpn.com/hc/en-us/articles/20911146148113-The-founders-and-owners-of-NordVPN>.

³⁹ *Id.*

⁴⁰ See <https://www.linkedin.com/in/tokmanas/>; see also <https://www.linkedin.com/in/eimis/>.

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 B.V., 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 B.V., 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.”⁴¹
- e. Upon information and belief, Defendants and non-Defendants NordSec B.V., NordSec Ltd., and Nord Security Inc. share employees. For example, the LinkedIn pages of many of Defendants and non-Defendants NordSec B.V., 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 (<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, the Netherlands, England, Spain, Japan, and remotely.
- f. When Defendants and non-Defendants NordSec B.V., 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 B.V., NordSec Ltd., and Nord Security Inc.

35. Both Defendants and non-Defendants NordSec B.V., NordSec Ltd., Tefincom S.A., 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 cases filed in Colorado and Illinois, Defendant Nordvpn S.A. in a case filed in North Carolina, and

⁴¹ Services, CEOCORP, <https://ceocorp.net/services/>.

Defendants Nordvpn S.A., Tefincom S.A., and non-Defendant NordSec B.V. in a case filed in New York.

36. Defendants and non-Defendants NordSec B.V., NordSec Ltd., and Nord Security Inc. do business in Massachusetts under the name “Nord Security” and interacted with Plaintiff in Massachusetts such that their claims described herein arise from Plaintiff’s contacts with Defendants and these non-Defendants in Massachusetts.

37. Any such conduct of Defendant Nordvpn S.A., Defendant Tefincom S.A. non-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.”⁴² 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. 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[.]”⁴³

⁴² See Sam Saltis, *How to Run an eCommerce Subscription Service: The Ultimate Guide*, CORE DNA, <https://www.coredna.com/blogs/ecommerce-subscription-services>.

⁴³ 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).

39. In March 2023, one source noted that “[o]ver the past 11 years, subscription-based companies[] have grown 3.7x faster than the companies in the S&P 500.”⁴⁴

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 nearly every industry is expected to last.”⁴⁵ 68% of consumers subscribed to something for the first time in 2024.⁴⁶

41. However, the subscription-based business model also has well-documented downsides. While the subscription e-commerce market has low barriers to entry, it is considerably more difficult for retailers to dominate the market due to the “highly competitive prices and broad similarities among the leading players.”⁴⁷ In particular, retailers struggle with the fact that

⁴⁴ *The Subscription Economy Index*, ZUORA (Mar. 2023), https://www.zuora.com/wp-content/uploads/2023/03/Zuora_SEI_2023_Q2.pdf<https://www.zuora.com/resources/subscription-economy-index/>.

⁴⁵ 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/>.

⁴⁶ 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>.

⁴⁷ 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>.

“[c]hurn rates are high, [] and consumers quickly cancel services that don’t deliver superior end-to-end experiences.”⁴⁸

42. 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].”⁴⁹ As these companies have realized, “[t]he real money is in the inertia.”⁵⁰ As a result, “[m]any e-commerce sites work with third-party vendors to implement more manipulative designs.”⁵¹ That is, to garner more revenue, some 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.⁵²

43. To make matters worse, once enrolled in the subscription, “[o]ne of the biggest complaints consumers have about brands/retailers is that it’s often difficult to discontinue a subscription marketing plan.”⁵³ Indeed, “the rapid growth of subscriptions has created a host of

⁴⁸ *Id.*

⁴⁹ 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.

⁵⁰ *Id.*

⁵¹ 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>.

⁵² 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>.

⁵³ Heather Long and Andrew Van Dam, *supra* note 44 (“Subscription services are a sneaky wallet

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.”⁵⁴ 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[,]”⁵⁵ widespread utilization of these misleading “dark patterns” and deliberate omissions persist.

44. 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.”⁵⁶ 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.”⁵⁷

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>.

⁵⁴ Heather Long and Andrew Van Dam, *supra* note 44.

⁵⁵ *Id.*

⁵⁶ *User Experience (UX): Process and Methodology*, UIUX TREND, <https://uiuxtrend.com/user-experience-uxprocess/>.

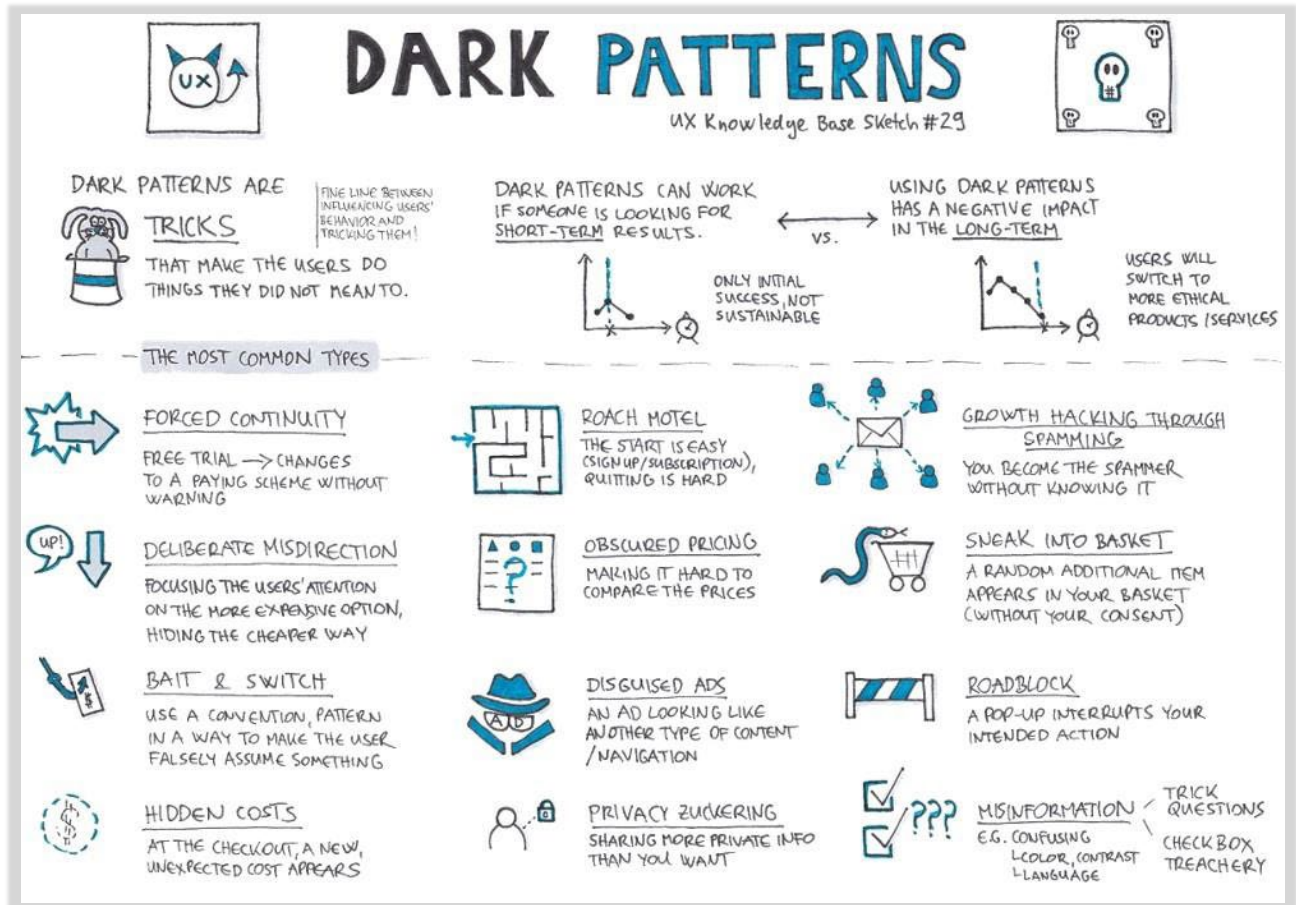
⁵⁷ Joey Ricard, *UX Dark Patterns: The Dark Side Of The UX Design*, KLIZO SOLS. PVT. LTD. (Nov. 9, 2020), <https://klizos.com/ux-dark-patterns-the-dark-side-of-the-ux-design>.

45. 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.”⁵⁸ 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.”⁵⁹ The image below provides some examples of commonly employed dark patterns:⁶⁰

⁵⁸ Harry Brignull, *Bringing Dark Patterns to Light*, MEDIUM (June 6, 2021), <https://harrybr.medium.com/bringing-dark-patterns-to-light-d86f24224ebf>.

⁵⁹ *Id.*

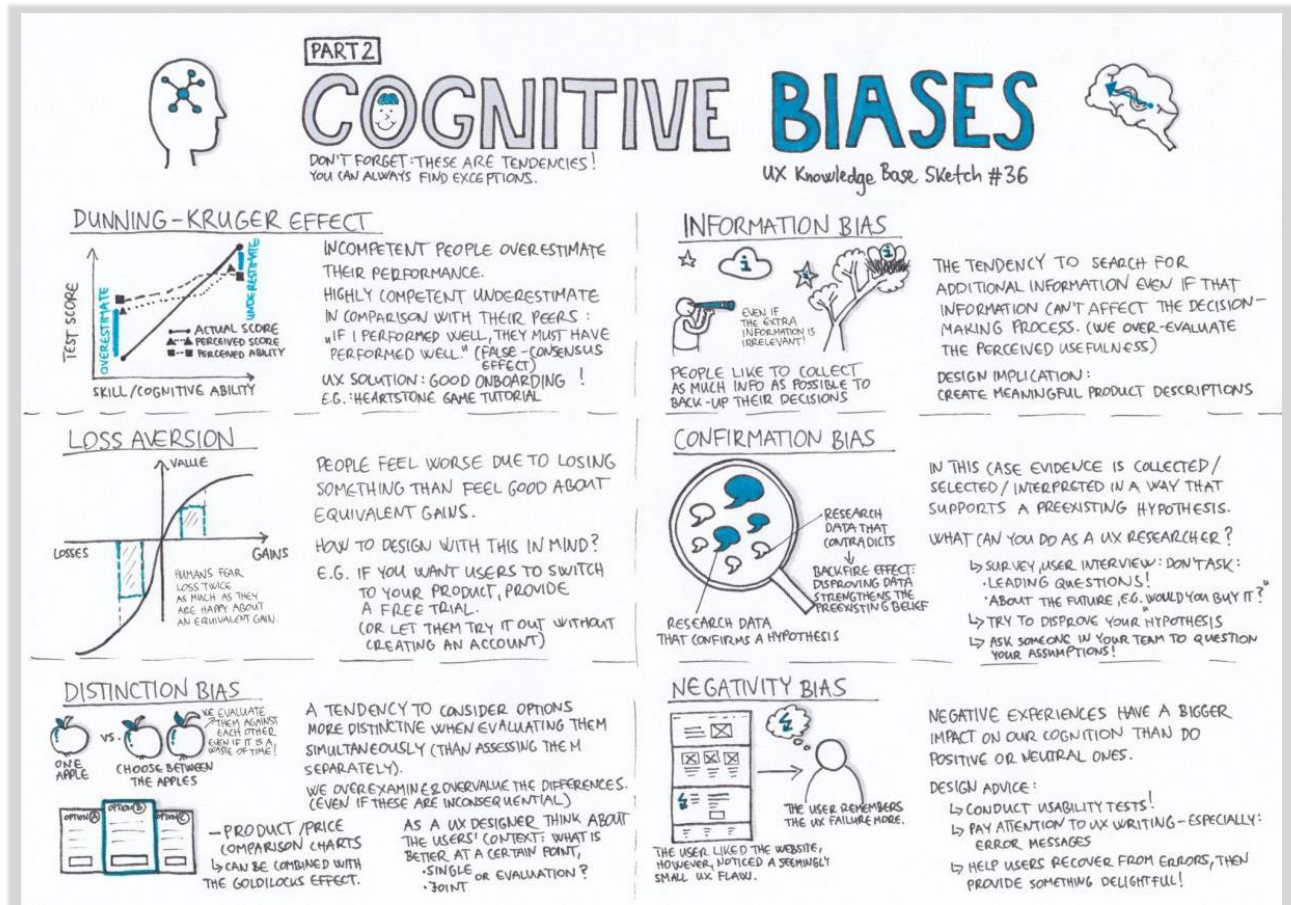
⁶⁰ Sarbashish Basu, *What is a dark pattern? How it benefits businesses- Some examples*, H2S MEDIA (Dec. 19, 2019), <https://www.how2shout.com/technology/what-is-a-dark-pattern-how-it-benefit-businesses-with-some-examples.html>.



46. The origin of dark patterns can be traced to the field of applied psychology.⁶¹ In the 1970s, behavioral science sought to understand irrational decisions and behaviors and discovered that cognitive biases guide all our thinking. The image below provides examples of cognitive biases, including some that Nord Security exploits:⁶²

⁶¹ Brignull, *supra* note 57.

⁶² Krisztina Szerovay, *Cognitive Bias — Part 2*, UX KNOWLEDGE BASE (Dec. 19, 2017), <https://uxknowledgebase.com/cognitive-bias-part-2-fab5b7717179>.



47. But while the early behavioral research focused on understanding rather than intervention, later researchers, like Cass Sunstein and Richard Thaler (authors of the noted 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.⁶³

48. 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 (version “A” and version “B”) and then measures which actions they take (or do not take) in response to each variant.⁶⁴ UX designers use this method to determine which

⁶³ 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>.

⁶⁴ UXPin, *A/B Testing in UX Design: When and Why It's Worth It*,

design or content performs best with the intended user base.⁶⁵ 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 labeled “SEARCH” versus simply identified by a magnifying glass icon.

49. 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.⁶⁶ 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.⁶⁷

50. 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.⁶⁸ Nord Security’s products and services have over 15 million users, with “[m]ost of Nord Security’s user base [] centered in the U.S.”⁶⁹

<https://www.uxpin.com/studio/blog/ab-testing-in-ux-design-when-and-why>.

⁶⁵ *Id.*

⁶⁶ Narayanan *et al.*, *supra* note 63.

⁶⁷ *Id.*

⁶⁸ Nord Security raised another \$100M investment round, NORD SECURITY, <https://nordsecurity.com/blog/nord-security-raised-another-100m-investment-round>.

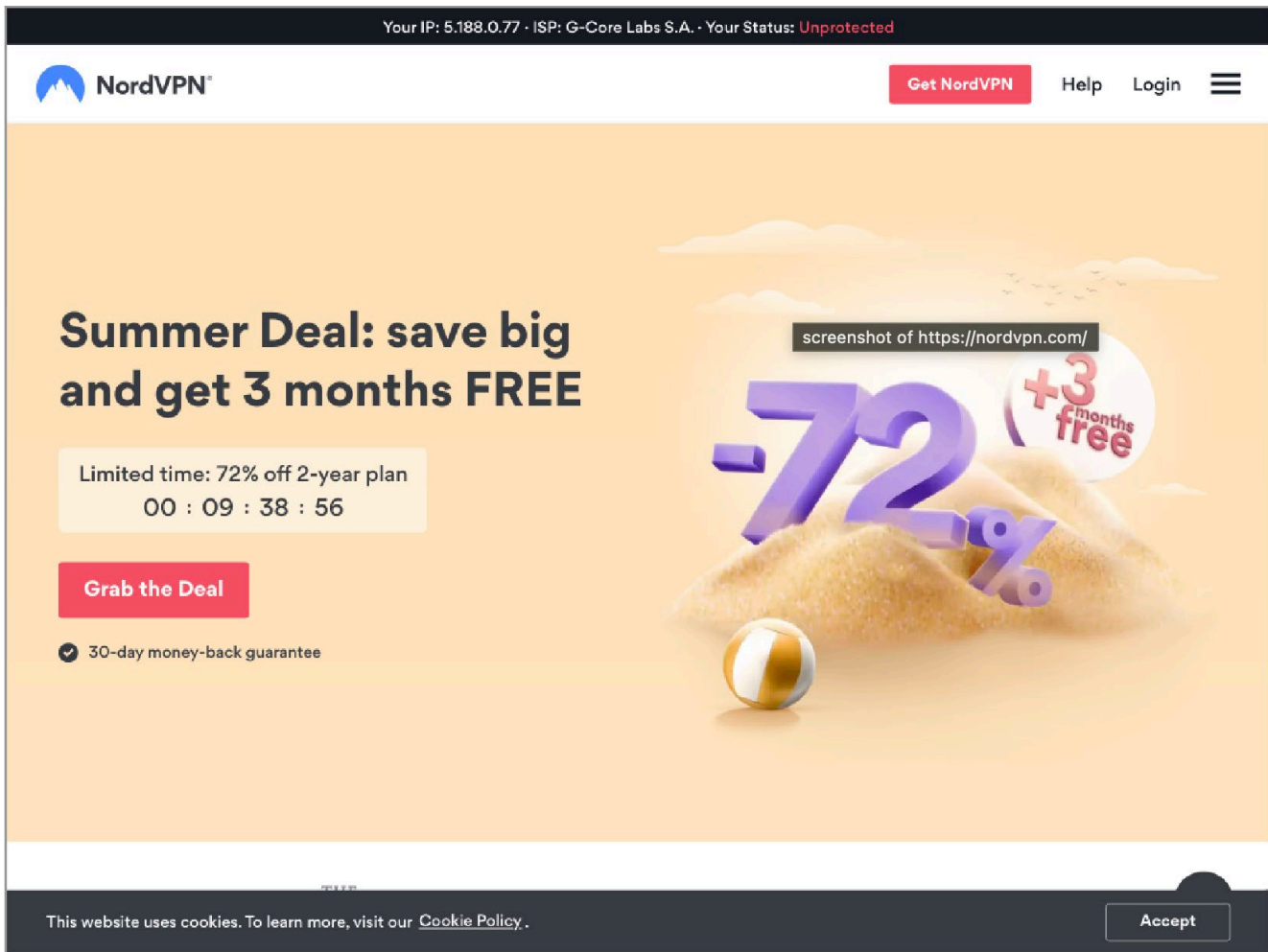
⁶⁹ Prarthana Prakash, *From bootstrapped to billions: How Nord spent ‘hundreds of millions’ minting VPN customers to become Lithuania’s tech darling*, FORTUNE (April 30, 2025), <https://fortune.com/europe/article/nord-vpn-hundreds-of-millions-minting-lithuania-tech-darling-unicorn/>.

B. Nord Security’s Material Misrepresentations and Omissions in Its Enrollment Flow

51. In its online enrollment process (“Enrollment Flow”), Nord Security presented the terms of its offer to Plaintiff in a manner that has the capacity and tendency to mislead reasonable consumers and induce reasonable consumers to act differently than they would otherwise have acted. This is a deceptive practice under the Massachusetts Consumer Protection Act, Mass. Gen. Laws ch. 93A (“Chapter 93A”). *See, e.g., Aspinall v. Philip Morris Companies, Inc.*, 442 Mass. 381, 395 (2004) (“[A]n advertisement is deceptive when it has the capacity to mislead consumers, acting reasonably under the circumstances, to act differently from the way they otherwise would have acted (i.e., to entice a reasonable consumer to purchase the product).”).

52. Nord Security’s Enrollment Flow was comprised of three webpages: a Home Page, a Pricing Page, and a Payment Page.

53. A user who navigates to Nord Security’s Home Page (the “Home Page”) will be presented with a bright logo urging the user to “Get NordVPN” and “Grab the Deal.” Below the bright red logo is a check-mark logo advising the user of Nord Security’s “30-day money-back guarantee.” The backdrop for these logos is a large, brightly colored advertisement for a then-active discount for users, available for a limited time. Upon information and belief, the Home Page used by Nord Security during the Class Period (*see infra* ¶ 93) and that Plaintiff used in June 2021 was materially similar to the Nord Security Home Page reproduced below:



54. If the user clicks “Grab the Deal” or “Get NordVPN,” they are directed to Nord Security’s Pricing Page.

55. Upon information and belief, the Pricing Page used by Nord Security during the Class Period and that Plaintiff used in June 2021 was materially similar to the Nord Security Pricing Page reproduced on the following page. This page likewise presents the user with a brightly colored call to action with the current price in large, bold font and a large, centrally located promise of a “30-day money-back guarantee.”

NordVPN [Get NordVPN](#) [Help](#) [Login](#)

Save big with our annual plans

No logs, no hidden fees. All plans come with the 30-day money-back guarantee.

Plan	Price	Savings	Original Price
2-year plan	\$4.13 per month	Save 65%	\$286.80
1-year plan	\$4.92 per month	Save 58%	\$143.40
1-month plan	\$11.95 per month	Save 0%	\$11.95

PewDiePie
109M subscribers

"I use NordVPN every single day. It's fast, it's reliable. It's safe. It helps me access epicness."

56. If a user clicks the “Get 2-Year Plan” button (or “Get 1-Year Plan” or “Get 1-Month Plan” buttons), they are taken to Nord Security’s Payment Page.

57. Upon information and belief, the Payment Page for Nord Security’s enrollment process during the Class Period and that Plaintiff used in June 2021 was materially similar to the Nord Security Payment Page reproduced below. Here, again, Nord Security floods the page with bright colors and a variety of fonts emphasizing potential savings (in bright red), potential savings (in large, bold font), and a “30 DAY MONEY-BACK 100% GUARANTEE” highlighted with a

bright red shield. A small-font, low-contrast “disclosure” is placed “below the fold”—that is, the user must scroll down to find it.

NordVPN Checkout Already have Nord Account? [Log in](#)

30 DAY MONEY-BACK GUARANTEE

Create an account

Your email address
name@example.com

If you don't want to receive marketing emails about Nord services, you can change notification settings in Nord Account.

By submitting your information and continuing to purchase, you agree to our [terms of service](#) and [privacy policy](#).

Select a payment method

Credit or debit card >

PayPal >

AmazonPay >

Google Pay >

Crypto Currencies >

Order summary

Standard plan
2-year plan (\$3.79/mo) + 3 EXTRA months \$102.33
Save 54% \$223.83

Tax country: [United States](#)
Sales tax 8.875% \$9.08

Total \$111.41*

Got a coupon?

Dedicated IP (\$3.79/mo)
Get a personal IP address that's only yours.
[See available locations](#) [Add](#)

Recommended for NordVPN users

Incogni data removal tool (\$3.69/mo)
Get your personal info off the market.
[View details and terms](#) [Add](#)

* The introductory price is valid for the first term of your subscription. Then it will be automatically renewed for an additional 1-year term annually and you'll be charged the [then-applicable renewal price](#). Savings granted by the introductory price are compared to the current renewal price, which is subject to change. But don't worry — we'll always send you a notification email prior to charging. [Learn more](#)

© 2024 Nord Security. All Rights Reserved. [support@nordvpn.com](#) [Terms of Service](#) [Cookie Preferences](#) [English](#)

58. Nord Security’s Enrollment Flow, comprised of its Home Page, Pricing Page and Payment Page, violates the Massachusetts Consumer Protection Act in the following ways.

59. **First**, the Enrollment Flow does not adequately disclose Nord Security’s practice of charging users early for subscription renewals or of the price increases it imposes at renewal.

60. On the Home Page, Nord Security makes no reference to its practice of charging early for automatic renewals, or of potential price changes at renewal.

61. On the Pricing Page, no reference whatsoever is made to Nord Security’s practice of charging early for automatic renewals. The only reference to a potential price change is obscured in low-contrast, light gray font, which says that the advertised price is “for the first [subscription period].” This disclosure is, at best, misleadingly incomplete—it does not explain

that the subscription will renew automatically, and certainly not that it will renew automatically at a higher price. Moreover, Nord Security’s design choices distract from this “disclosure” and towards the bright blue banner highlighting an “exclusive deal,” the bright red banner highlighting purported savings, and the bright blue button exhorting the user to “Get 2-Year Plan.”

62. On the Payment Page, the only reference to the timing of an autorenewal charge or of a change in the amount to be charged is placed in miniscule, low-contrast font below the fold. The text is not just small but colored light gray in low contrast against a white background. The text is not set off from the surrounding text in a manner designed to call attention to it (as opposed to, for example, the bright red “30-day” shield promoting Nord Security’s “money-back guarantee,” the enlarged, bold font highlighting the sales price, or the bright red font advertising supposed savings).

63. These intentional design choices—as to the Pricing and Payment Pages’ overall design, including the location of Nord Security’s supposed “disclosures” regarding price increases on automatic renewal, its font size, and color, *deemphasize* the notice text rather than make it **conspicuous**. Defendants’ “disclosures” are also not in visual connection with the purchase terms on the Payment Page and are instead buried at the bottom of the page.

64. The content of the hidden Payment Page “disclosure” is also inadequate and misleading. It does not make any mention of Nord Security’s practice of charging the consumer days or weeks in advance of the conclusion of the subscription period. On the contrary, it implies that charging takes place *after* the subscription term concludes:

The introductory price is valid for the first term of your subscription. ***Then it will be automatically renewed for an additional 1-year term and you’ll be charged the then-applicable renewal price.***

Payment Page (emphasis added).

65. Thus, even if a consumer managed to find this disclosure (requiring scrolling below the fold and likely zooming in on the website to make out the small print), they would have no reason to expect that Nord Security would assess renewal fees before the applicable subscription period ended.

66. Likewise, while this statement (inadequately) discloses that the user will be charged the “then-applicable” price, it does not inform the user (assuming, again, that they find the disclosure), that renewal prices are almost certain to be significantly higher than the current subscription price.

67. This is a deceptive practice under Chapter 93A, which defines an advertisement as deceptive “when it has the capacity to mislead consumers, acting reasonably under the circumstances, to act differently from the way they otherwise would have acted (i.e., to entice a reasonable consumer to purchase the product.)” *Dumont v. Reily Foods Co.*, 934 F.3d 35, 40 (1st Cir. 2019).

68. Nord Security’s design choices also violate regulations promulgated under Chapter 93A, including at least 940 C.M.R. 3.05, which provides that “[n]o claim or representation shall be made by any means concerning a product which directly, or by implication, or by failure to adequately disclose additional relevant information, has the capacity or tendency or effect of deceiving buyers or prospective buyers in any material respect.” Violation of that regulation is itself a violation of Chapter 93A. *See* 940 C.M.R. 3.16(3) (violation of Massachusetts consumer protection statutes violates Chapter 93A).

69. **Second**, if a consumer did click the “Terms of Service” (through a link provided only in miniscule font on the Payment Page) and locate, buried on the fourth paragraph of the

third page of a nine-page document, Nord Security’s description of the timing of its renewal charges, that consumer would see a demonstrably false statement:

Your service will automatically be renewed, and your chosen payment method will be charged *at the end of each service period*, unless you decide to cancel your automatic payments for service *before the end of the then-current subscription*. All prices, including recurring subscription fees, are subject to change.

Terms of Service § 4 (emphasis added).

70. This paragraph states that customers 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 paragraph above, that customers on plans lasting greater than a month will be charged in advance: “at least 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 initial plan, your subscription *will be automatically renewed*, and you will *be charged*[.]” (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.

71. *Third*, Nord Security’s Enrollment Flow does not disclose, let alone clearly and conspicuously, the conditions of its 30-day money-back guarantee—namely, that it is backdated on autorenewal to the date of Nord Security’s improper and premature charge. This not only has the tendency to mislead the consumer, in violation of Chapter 93A and its accompanying regulations, it also violates explicit disclosure requirements for guarantees under Massachusetts regulations promulgated pursuant to Chapter 93A. *See* 940 C.M.R. 3.03(2) (requiring any conditions or limitations to a guarantee to be “clearly and conspicuously disclosed”).

C. How Nord Security's Subscription Scheme Injured Plaintiff

72. Plaintiff was injured by Nord Security's unlawful and deceptive subscription scheme because Nord Security: (i) repeatedly charged Plaintiff's payment method before the conclusion of his subscription term; (ii) charged Plaintiff significantly higher subscription charges than initially agreed upon; and (iii) denied Plaintiff a refund for this premature and overpriced subscription on the basis that Nord Security's 30-day refund period had expired, even though Plaintiff sought a refund less than 30 days after the end of his subscription term.

73. On approximately June 29, 2021, Plaintiff enrolled in a two-year, \$94.56 subscription to Nord Security's NordVPN product. The two-year period began on September 29, 2021, following a three-month free period included in his enrollment. The subscription term was thus September 29, 2021 to September 29, 2023.

74. On approximately September 15, 2023—fourteen days prior to the conclusion of Plaintiff's initial subscription term—Nord Security charged Plaintiff's payment method \$105.70 for an additional one-year subscription for NordVPN. In other words, Nord Security's automatic renewal doubled the annual cost of Plaintiff's subscription. The term for the renewed subscription was September 29, 2023 to September 29, 2024. At the time, Plaintiff did not notice this premature, increased charge.

75. On approximately September 15, 2024—again fourteen days prior to the conclusion of the one-year subscription period—Nord Security charged Plaintiff's payment method \$159.25 for an additional one-year NordVPN subscription. The term for the renewed subscription was September 29, 2024 to September 29, 2025. Nord Security's charge amounted to a 51% increase in the price it charged Plaintiff the prior year.

76. On October 25, 2024, Plaintiff noticed this significant charge and sought an explanation from Nord Security. Unable to receive a satisfactory explanation, Plaintiff requested

cancellation of the subscription the next day—**October 26, 2024, or 27 days after his subscription was renewed**—to ensure the return of his payment.

77. Nord Security did not respond to Plaintiff’s cancellation request.

78. Thereafter, Plaintiff noticed that Nord Security had not provided the requested refund and he followed up with Nord Security and advised that his subscription expiration date was September 29, 2024, and that he had requested a refund within the 30-day period.

79. Nord Security refused to provide a refund, stating that, “whilst your subscription was due to expire on [September] 29th, the payment was made on September 15th, which is more than 30 days prior to October 26th. With all of this in mind, unfortunately, a refund will not be possible.”

80. Plaintiff, as any reasonable consumer would have been, was misled by Nord Security’s deceptive autorenewal practices. Plaintiff was not given adequate notice that Nord Security would continuously increase its subscription renewal rates. Plaintiff was also not given adequate notice that Nord Security would charge his payment method two weeks before the conclusion of his subscription term. Finally, Nord did not give Plaintiff adequate notice that he would not have a full thirty days following that charge to request a refund pursuant to Nord Security’s “30-day money-back guarantee.”

81. Plaintiff did not authorize or want Nord Security to charge his payment method fourteen days prior to the conclusion of his Subscription term, nor did Plaintiff authorize or want Nord Security to charge his payment method a significantly increased price for a Nord Subscription.

82. 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 enrolled in a Nord Subscription.

83. Plaintiff was further injured because he paid a premium for his Nord Subscription on the understanding that he could trust the guarantees made by Nord Security related to that subscription, including that Nord would not deploy underhanded subscription tactics.

84. 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 to process unauthorized payments in the future.

85. Given that Nord Security has engaged in a series of deceptive acts and omissions for which it billed consumers and for which consumers continue 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 no earlier than September 2024, when Nord Security last charged Plaintiff prematurely and at an increased price for a Nord Subscription renewal. Nord Security also wrongfully refused to honor its "30-day money-back guarantee" when it refused to accept Plaintiff's October 2024 refund request.

RULE 9(B) ALLEGATIONS

86. 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:

87. **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 Massachusetts through a deceptive subscription scheme by making the material misrepresentations and omissions alleged in detail above in violation of Massachusetts consumer protection statutes and the common law, including with respect to the timing of premature subscription charges, the amount of those charges, and undisclosed limitations on its “30-day money-back guarantee.”

88. WHAT:

Nord Security conducts its deceptive subscription scheme by charging consumers’ payment methods before the end of their subscription term, typically about two weeks early for annual plans (and five days early for monthly plans), without providing adequate notice of this practice in its Enrollment Flow or Terms of Service. This practice is deceptive and directly contradicts Nord Security’s representation that charges occur “at the end of each service period.”

- Nord Security conducts its deceptive subscription scheme by assessing renewal charges at prices significantly higher than those customers agreed to pay, while presenting sign-up pages that highlight a single attractive price and bury any reference to higher “then-applicable” renewal pricing in small, low-contrast text placed below the fold. These design choices are deceptive.
- Nord Security conducts its deceptive subscription scheme by advertising a “30-day money-back guarantee” in prominent, trust-inducing graphics and marketing, while secretly backdating that guarantee to the date of Nord Security’s early autorenewal charge rather than the start of the renewed term—rendering the promised 30 days illusory by the time consumers discover the unexpected, higher-priced charge.
- Nord Security conducts its deceptive subscription scheme by fragmenting and obscuring material terms across multiple documents and pages—presenting a Terms of Service that suggests end-of-term billing while locating contradictory “early charge” language in a separate set of terms—thereby creating an internally inconsistent and confusing terms of its offer.
- Nord Security conducts its deceptive subscription scheme by failing to clearly and conspicuously disclose the exact nature and extent of its “30-day money-back guarantee” before the transaction is consummated, misrepresenting that guarantee through contradictory language, and failing to perform promises made in connection with that guarantee, including by refusing timely refund requests that fall within 30 days of

the renewed term but outside 30 days of Nord Security’s undisclosed early charge.

- Nord Security conducts its deceptive subscription scheme through an enrollment flow designed to steer attention away from material terms—by emphasizing limited-time deals, large price callouts, and guarantee graphics—while relegating critical autorenewal timing and pricing information to inconspicuous locations, inaccessible font treatments, and inconsistent documents (if such information is disclosed at all). Moreover, Nord Security’s “disclosures” of this critical information are incomplete, misleading, or untrue. These practices have the capacity and tendency to mislead reasonable consumers, to induce consumers to make purchases they otherwise would not have made, and to result in payments for subscription renewals higher than consumers would have otherwise agreed to.
- Nord Security’s false guarantees—as to the timing and amount of its renewal charges, and as to its secretly backdated 30-day guarantee—also permit it to charge a premium for Nord Subscriptions above what it could otherwise charge.

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

90. 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 scheme when Plaintiff first enrolled in a Nord Subscription in June 2021, when it prematurely charged Plaintiff for automatic renewal of his subscription at increased rates in 2023 and 2024, and during Plaintiff’s unsuccessful attempt to secure a refund within 30 days of the end of his subscription term in 2024.

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

92. HOW: Nord Security conducts its deceptive and unlawful scheme by making the material misrepresentations and omissions in violation of Massachusetts consumer protection law and the common law alleged in detail above.

CLASS ACTION ALLEGATIONS

93. 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 Massachusetts (including customers of companies Nord Security acts as a successor to) from the earliest allowable date through the date of judgment (the “Class”).

94. 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.

95. 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.

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

97. 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.

98. 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.

99. 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.

100. 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.

101. 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 applicable Massachusetts consumer protection statutes;
- b. Whether Defendants' conduct violates the applicable common law doctrines;
- c. Whether Defendants were unjustly enriched as a result of their conduct;

- d. Whether Class Members have been injured by Defendants' conduct;
- e. Whether, and to what extent, equitable relief should be imposed on Defendants to prevent them from continuing their unlawful practices; and
- f. The extent of class-wide injury and the measure of damages for those injuries.

102. 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.

103. 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 applicable Massachusetts consumer protection statutes;
- b. Whether Defendants' conduct violates the applicable common law doctrines;
- c. Whether Defendants were unjustly enriched as a result of their conduct;
- d. Whether Class Members have been injured by Defendants' conduct; and
- e. Whether, and to what extent, equitable relief should be imposed on Defendants to prevent them from continuing their unlawful practices.

104. 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
MASSACHUSETTS CONSUMER PROTECTION ACT, MASS. GEN. LAWS CH. 93A,
§§1, ET SEQ.
(On Behalf of Plaintiff and the Class)

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

106. Plaintiff brings this claim under Mass. Gen. Laws Ch. 93A, §2 on his own behalf and on behalf of each member of the Class.

107. Massachusetts’ consumer protection statute prohibits “deceptive acts or practices in the conduct of any trade or commerce.” Mass. Gen. Laws. Ch. 93A, §2.

108. Because it is engaged in the “sale . . . of . . . services,” Nord Security is engaged in “commerce” under the definition established in Mass. Gen. Laws Ch. 93A, §1.

109. Defendants have engaged in, and continue to engage in, unfair methods of competition and unfair or deceptive acts or practices in violation of Mass. Gen. Laws Ch. 93A, §2, including:

- a. Misrepresenting in its Terms of Service the timing of when Nord Security will charge customers for renewals, by representing that renewal charges will occur “at the end of each service period,” when in fact Nord Security charges approximately two weeks before that date (or five days before for monthly subscriptions);
- b. Misrepresenting on its Payment Page that Nord Security will charge for autorenewal after the “term of your subscription;”
- c. Failing to disclose on its Payment Page or enrollment pages that Nord Security will charge customers well before the renewal date;
- d. Misrepresenting the price of Nord Security’s service by prominently displaying an initial subscription price while concealing, or failing to adequately disclose, that renewal charges will be assessed at higher rates;
- e. Burying Nord Security’s purported disclosure of renewal pricing (and inaccurate disclosure of the timing of renewal charges) in tiny, low-contrast gray text at the bottom of the Payment Page, below the fold;

- f. Misrepresenting in Nord Security’s Payment Page that consumers are protected by a “30-day money-back guarantee,” while failing to disclose that the 30-day period begins on the date Nord Security prematurely charges the customer’s payment method rather than on the start date of the renewed term;
- g. Misrepresenting in Nord Security’s Terms of Service that “[i]f you wish to claim a refund, you can do so within 30 days following your purchase of our Services[,]” while failing to disclose that, on renewal, the 30-day period begins on the date Nord Security prematurely charges the customer’s payment method rather than on the start date of the renewed term;
- h. Failing to present any of the foregoing material terms—early renewal charging, higher renewal pricing, and backdating of the 30-day refund period—in such a manner so that the reasonable consumer would be aware of these material terms, rather than misled into believing that any renewal charge would take place at the conclusion of the subscription term, at the price originally agreed to, and be followed by a 30-day refund period.

110. The above deceptive practices and acts by Nord Security were material omissions of existing or past facts and affirmative misrepresentations.

111. Mass Gen. Laws Ch. 93A, § 2(c) provides that “[t]he attorney general may make rules and regulations interpreting the provisions of subsection 2(a) of this chapter,” which in turn provides that “[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful.”

112. The Massachusetts Attorney General has issued such rules and regulations to protect consumers from unfair and deceptive practices like those exercised by Nord Security.

113. 940 C.M.R. 3.13 is one such regulation promulgated by the Massachusetts Attorney General, and is entitled “Pricing and Refund, Return and Cancellation Privileges.” 940 C.M.R. 3.13(4) provides that “[i]t is an unfair and deceptive trade practice (a) [t]o fail to clearly and conspicuously disclose to a buyer, prior to the consummation of a transaction, the exact nature and extent of the seller’s refund, return, or cancellation policy; (b) [t]o misrepresent the nature and terms of the seller’s refund, return, or cancellation policy; [and] (c) [t]o fail to perform any promises made to a buyer in connection with the refund, return, or cancellation privileges.”

114. Under 940 C.M.R. 3.01, “clear and conspicuous disclosure” is defined as follows:

Clear and Conspicuous Disclosure. Without limiting any other provisions of law, disclosures required by these regulations shall be of such size or color contrast and so placed as to be readily noticeable to purchasers or prospective purchasers reading advertising, sales promotional literature, or invoices containing same, or reading any representation as to content on the container in which the product is packed, or inspecting a product before installation or with a minimum of disassembly after installation. *A term is conspicuous when it is so written that a person against whom it is to operate ought to have noticed it. Language in the body of a form is “conspicuous” if it is in larger or contrasting type or color.*

Id. (emphasis added).

115. As set forth herein, Nord Security “fail[ed] to clearly and conspicuously disclose to [Plaintiff and members of the Class] the exact nature and extent of” its “30-day money-back guarantee;” “misrepresent[ed] the nature and terms of the” “30-day money-back guarantee;” and “fail[ed] to perform . . . promises made to [Plaintiff and members of the Class] in connection with the” “30-day money-back guarantee.”

116. 940 C.M.R. 3.03 is another such regulation promulgated by the Massachusetts Attorney General, and is entitled “Deceptive Advertising of Guarantees.” 940 C.M.R. 3.03(3) provides that “‘Satisfaction or your money back,’ ‘10 day free trial,’ or similar representations will be construed as a guarantee that the full purchase price will be refunded promptly at the option of the buyer. *If such guarantee is subject to any conditions or limitations whatsoever they shall be set forth as provided for in 940 C.M.R. 3.03(2).*” (emphasis added).

117. Under 940 C.M.R. 3.03(2), any conditions or limitations to a guarantee must be “clearly and conspicuously disclosed.” 940 Mass. Code Regs. 3.03(2).

118. As an example, the Massachusetts Attorney General set forth the following:

Example: A rose bush is advertised under the representation “Satisfaction or your money back.” The guarantor requires return of the product within 1

year of purchase date before he will make refund. These limitations, i.e. “return” and “time” shall be clearly and conspicuously disclosed in the ad.

940 Mass. Code Regs. 3.03(3).

119. Nord Security did not clearly and conspicuously disclose the conditions imposed on its “30-day money-back guarantee,” namely that such guarantee would be backdated to two weeks before the renewal date (or earlier), in that it did not write such a term in a manner “that a person against whom it is to operate ought to have noticed it.” Indeed, it did not disclose this condition at all.

120. Under 940 C.M.R. 3.03(6), “[a] seller or manufacturer shall not advertise or represent that a product is guaranteed when he cannot or does not promptly and scrupulously fulfill his obligations under the guarantee.”

121. Nord Security’s policy of secretly backdating its 30-day guarantee to the date of its premature charge did not “promptly and scrupulously fulfill [its] obligations under the [“30-day money-back”] guarantee.”

122. Under 940 C.M.R. 3.03(7), “[w]here guarantees are employed in such a manner as to constitute representations of material fact, the guarantor not only undertakes to perform under the terms of the guarantee, but also assumes responsibility under the law for the truth of the representations made.”

123. Nord Security did not “undertake[] to perform under the terms of the guarantee” and is now “responsib[le] under the law” for the falsity of its representations as to the 30-day money-back guarantee, namely, its failure to disclose that it backdated the 30-day refund period, such that the consumer did not have 30 days from renewal to exercise its option for a refund.

124. 940 C.M.R. 3.05 is another such regulation promulgated by the Massachusetts Attorney General, and is entitled “General Misrepresentations.” This regulation provides that “[n]o

claim or representation shall be made by any means concerning a product which directly, or by implication, or by failure to adequately disclose additional relevant information, has the capacity or tendency or effect of deceiving buyers or prospective buyers in any material respect.”

125. As outlined herein, Nord Security committed numerous misrepresentations and omissions of material facts concerning its products, which would have the capacity or tendency or effect of deceiving buyers as to: (i) the timing of autorenewal charges; (ii) the amount of autorenewal charges (and that they would increase significantly); and (iii) the backdating of Nord Security’s “30-day money-back guarantee.”

126. Nord Security’s violations of the regulations enumerated above constitute violations of Chapter 93A, Section 2(a) because regulations promulgated by the Massachusetts Attorney General under chapter 93A, Section 2(c) provide that any act or practice violates Chapter 93A, Section 2 if “[i]t fails to comply with existing statutes, rules, regulations or laws, meant for the protection of the public’s health, safety, or welfare promulgated by the Commonwealth or any political subdivision thereof intended to provide the consumers of this Commonwealth protection . . .” 940 C.M.R. 3.16(3).

127. Nord Security knew or should have known that the above unfair and deceptive practices and acts were material omissions, misrepresentations, or were otherwise deceptive or unfair.

128. Nord Security knew or should have known that the conduct outlined above has the capacity or tendency to deceive or mislead a reasonable consumer, and that the conduct outlined above has the effect of deceiving or misleading a reasonable consumer in material respects.

129. The aforementioned acts are continuing, unconscionable and deceptive and are contrary to the public policy of Massachusetts, which aims to protect consumers.

130. Nord Security's false, deceptive, and misleading statements and omissions would have been material to any potential consumer's decision to purchase a Nord Subscription.

131. Nord Security knew at the time it enrolled Plaintiff and members of the Class the nature of its "30-day money-back guarantee," the price of its offerings, and the timing of its autorenewal charges were material factors in choosing to purchase a Nord Subscription.

132. Nord Security's omissions and misrepresentations about factors were material to prospective customers, including Plaintiff and members of the Class.

133. By concealing its actual pricing strategy, refund policy, and charging policy, as described herein, Nord Security deprived customers from being able to make informed purchasing decisions.

134. Nord Security's practices are unfair, unconscionable, and outside the norm of reasonable business practices.

135. As a direct and proximate result of Nord Security's unlawful deceptive acts and practices, Plaintiff and Class Members suffered and continue to suffer an ascertainable loss of monies, including: (i) the price premium incurred paying for a product which was not the product Nord Security represented to them, in that the product was represented as being accompanied by certain guarantees (namely, a 30-day money-back guarantee, a subscription price, and a renewal charge at the end of the subscription term, rather than any earlier time) that were illusory; (ii) the full renewal price or the difference in price between the price the customer agreed to pay at enrollment and any higher price charged at renewal; and (iii) the amount of any moneys not refunded by Nord Security despite receiving a timely request for a refund within thirty (30) days of the end of a Nord Subscription Term.

136. Plaintiff and the members of the Class further seek equitable relief against Defendants. Pursuant to Mass. Gen. Laws Ch. 93A, §11, 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 return to the Plaintiff and the Class all amounts wrongfully assessed and/or collected.

137. As a result of Defendants' deceptive acts or practices, Plaintiff and Class Members suffered actual damages in an amount to be determined at trial, and are entitled to their actual damages or twenty-five dollars, whichever is greater, and costs, and reasonable attorneys' fees and all other relief available under Mass. Gen. Laws Ch. 93A, §2.

138. Because Defendants' actions were willful, Plaintiff and Class Members are further entitled at least double, and no more than treble, their actual damages. *See* Mass Gen. Laws ch. 93A, § 9(3A).

139. Pursuant to Mass. Gen. Laws Ch. 93A, §9(3), on July 9, 2025 Plaintiff served Defendants' counsel with a written demand for relief, identifying the claimant and reasonably describing the unfair or deceptive act or practice relied upon and the injury suffered.

COUNT II
CONVERSION
(On Behalf of Plaintiff and the Class)

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

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

142. 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.

143. Defendants substantially interfered with Plaintiff's 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 Subscriptions.

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

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

146. 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.

147. 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
(On Behalf of Plaintiff and the Class)

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

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

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

151. 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.

152. 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
(On Behalf of Plaintiff and the Class)

153. Plaintiff incorporates by reference all preceding and subsequent paragraphs.
154. Plaintiff brings this claim on his own behalf and on behalf of each member of the Class.
155. Defendants received moneys from Plaintiff and from each member of the Class.
156. The moneys belong to Plaintiff and each member of the Class.
157. Defendants have not fully returned the moneys.
158. 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 the Class representative, and designating Bryson, Harris, Suci, & Demay, PLLC and Wittels McInturff Palikovic 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, reasonable attorneys' fees, costs, and expenses; and
- (j) Grant all such other relief as the Court deems appropriate.

Dated: November 11, 2025

BRYSON HARRIS SUCIU & DEMAY PLLC

/s/ Scott C. Harris

Scott C. Harris, BBO #714774

900 W. Morgan Street

Raleigh, North Carolina 27603

Tel: 919-600-5000

Fax: 919-600-5035

Email: sharris@brysonpllc.com

WITTELS MCINTURFF PALIKOVIC

Daniel Kieselstein*

305 BROADWAY, 7TH FLOOR

NEW YORK, NEW YORK 10007

Tel: (914) 775-8862

Email: djk@wittelslaw.com

** Pro Hac Application Forthcoming*

Counsel for Plaintiff and the Proposed Class