

WITTELS MCINTURFF PALIKOVIC

J. Burkett McInturff
Ethan D. Roman
Daniel J. Brenner
305 BROADWAY, 7TH FLOOR
NEW YORK, NEW YORK 10007
Tel: (914) 775-8862
jbm@wittelslaw.com
edr@wittelslaw.com
djb@wittelslaw.com

**MILBERG COLEMAN BRYSON PHILLIPS
GROSSMAN, PLLC**

Scott C. Harris
J. Hunter Bryson
900 W. MORGAN STREET
RALEIGH, NORTH CAROLINA 27603
Tel: 919-600-5000
sharris@milberg.com
hbryson@milberg.com

**UNITED STATES DISTRICT COURT
DISTRICT OF COLORADO**

TIM PETERSON,

on Behalf of Himself and All Others Similarly
Situated,

Plaintiff,

v.

**NORDVPN S.A. and TEFINCOM S.A. d/b/a
NordVPN,**

Defendants.

Case No.: 24 Civ. 3218

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Tim Peterson (“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 Colorado consumers defined below against Defendants Nordvpn S.A. and Tefincom S.A. d/b/a NordVPN (hereafter, “Defendants,” “Nord Security,” 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 is a 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 security services. Nord Security intentionally misleads consumers into thinking they can subscribe to Nord Security’s virtual private network and other services for a discrete period of time. The truth is, however, that Nord Security’s subscriptions automatically renew and Nord Security’s “disclosures” regarding this feature of its subscriptions 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 those subscriptions difficult to cancel.

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 a virtual private network (“VPN”) service called “NordVPN,”¹ a password manager called “NordPass,” and an encrypted cloud storage service called “NordLocker.”

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).

3. Potential customers are directed to Nord Security's various sales websites through online searches, its sponsorship of influencers, or by advertising for the Company's VPN and/or other services. Nord Security advertises widely online and on dozens of podcasts. Nord Security's advertising touts the benefits that its services allegedly offer the prudent consumer; for example, the Company claims that its VPN service provides consumers "safe and private access to the internet" and that it is "trusted by tech experts and users."

4. When consumers enroll in Nord Security's privacy and security products and services, unbeknownst to these consumers Nord Security is actually collecting consumers' payments and payment information via deceptive and unlawful subscription practices designed to entrap consumers into paying unknown and/or unwanted recurring subscription fees.

5. Nord Security's products are offered with 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 notes, "[n]egative option programs can cause serious harm to consumers," which "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 Nord Security's deceptive and unlawful negative option practices, many consumers who sign up for a Nord Security service ultimately end up paying for subscriptions that they do not want.

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

7. 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 service offerings. While Nord Security's deceptive web has several components that can independently trip up consumers and lead to inadvertent purchases, taken together these components make up a larger deceptive process that leads to a common and predictable outcome: saddling consumers with unwanted recurring subscriptions.

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

9. First, during the enrollment process, Nord Security fails to clearly and conspicuously present the terms of the automatic renewal offer, including a description of 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 requires customers to scroll to find the relevant (and inadequate) fine print on its payment page and buries its key autorenewal provisions in confusing, inconsistent, and inaccurate terms scattered across multiple sections of at least two fine print documents. Nor does Nord Security obtain consumers' affirmative consent to the automatic renewal offer prior to charging consumers' payment cards or third-party accounts.

10. Second, Nord Security's scheme continues post-sign up. The Company's receipt and acknowledgement emails sent to consumers after they enroll in a Nord Security subscription do not include the automatic renewal offer terms, the cancellation policy, or information regarding how to cancel in a manner that is capable of being retained by the consumer. In fact, these emails contain no information whatsoever on the automatic renewal offer or how to cancel a subscription.

11. Third, Nord Security makes canceling exceedingly difficult and requires customers to figure out—with no help from the Company—that to Defendants, cancelling means 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”).

12. Fourth, Nord Security fails to provide sufficient notice under Colorado law that the customer’s subscription will automatically renew at least 25 days, but no more than 40 days before the subscription automatically renews, because Nord Security’s “notice” email fails to: (1) “inform the consumer of the process for canceling the automatic renewal contract;” and (2) “provide a simple, cost-effective, timely, easy-to-use, and readily accessible mechanism for canceling an automatic renewal contract,” such as a “one-step online cancellation link.”

13. Fifth, 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.

14. 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 “simple, cost-effective, timely, easy-to-use, and readily accessible [cancellation] mechanism,” which Nord Security does not have.

15. Again, 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.

16. These outcomes are not only unsurprising, but are in fact the result of Defendants' intentional and bad-faith design choices. Defendants are well aware that their scheme is tricking customers, as complaints about Nord Security are legion, with hundreds of consumers complaining on sites like Trustpilot, SiteJabber, and Reddit or directly to Nord Security. 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.

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

18. Only through a class action can consumers remedy Defendants' 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 Plaintiff and the Class in violation of the law.

JURISDICTION AND VENUE

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

20. 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 Defendants.

21. 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.

22. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b). Substantial acts in furtherance of the alleged improper conduct occurred within this District, as Plaintiff resides in this District, and Defendants reside in this District for venue purposes. *Id.* § 1391(c)(2).

PARTIES

23. Plaintiff Tim Peterson is a citizen of Colorado and lives in Timnath, Colorado. He enrolled in a Nord Security subscription on January 2, 2022.

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

25. Upon information and belief, with respect to all actions and decisions relevant to this action, Defendants along with non-Defendants NordSec Ltd., NordSec B.V., 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.

26. Defendants, along with non-Defendants NordSec Ltd., NordSec B.V., 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 Colorado 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 the product 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., NordSec B.V., 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 Security" shows pictures of the founders, explains "our mission," and contains links to Nord Security's "corporate responsibility reports" and Nord Security's "Code

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

⁵ *Id.*

of Conduct,”⁶ which discusses such topics as expectations for the “Nord Security brand products, including NordVPN, NordPass, NordLocker, and NordLayer.”⁷

27. 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., NordSec B.V., and Nord Security Inc.’s products “NordVPN, NordLocker, and NordPass.”¹⁰ NordVPN is the product Defendants and non-Defendants NordSec Ltd., NordSec B.V., and Nord Security Inc. marketed and sold to Plaintiff in Colorado. Defendant Nordvpn S.A. also currently operates Defendants and non-Defendants NordSec Ltd., NordSec B.V., and Nord Security Inc.’s website, www.nordvpn.com.¹¹ Nordvpn S.A.’s corporate parents are NordSec B.V., 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

28. 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

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-cv-2462 (N.D. Cal.), Dkt. No. 39-1, ¶ 3.

⁹ *Id.*

¹⁰ *Id.*

¹¹ *Id.*

¹² *Zeichner*, Dkt. No. 37.

¹³ *Zeichner*, Dkt. No. 39-1, ¶ 8.

¹⁴ *Zeichner*, Dkt. No. 39-3, ¶ 3.

is Panama City, Panama.¹⁵ Defendant Tefincom S.A.’s corporate parent is Stitching Raveset.¹⁶ Defendants and non-Defendants NordSec Ltd., NordSec B.V., and Nord Security Inc. admit that Defendant Tefincom S.A. was the contracting entity for Colorado 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.”

29. 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., NordSec B.V., 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 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.

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.

30. Non-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., NordSec B.V., 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., NordSec B.V., 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 the Nord Security product he purchased bore the “Nord Security,” “NordVPN,” “Nord,” and “NordSec” marks owned by NordSec B.V.

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>.

31. 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., NordSec B.V., and Nord Security Inc. claim in a separate litigation that Nord Security Inc. is not the “Nord Security” that offers services to Colorado consumers, instead claiming that Nord Security Inc. provides only business-to-business services.³⁶

32. Upon information and belief, at all times pertinent to this action, the finances, policies, and business practices of Defendants and non-Defendants NordSec Ltd., NordSec B.V., 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., NordSec B.V., 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

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.*

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

33. Upon information and belief, Defendants and non-Defendants NordSec Ltd., NordSec B.V., 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., NordSec B.V., 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., NordSec B.V., 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., NordSec B.V., 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., NordSec B.V., 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., NordSec B.V., 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., NordSec B.V., and Nord Security Inc. share employees. For example, the LinkedIn pages of many of Defendants and non-Defendants NordSec Ltd., NordSec B.V., 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

³⁹ See <https://www.linkedin.com/in/tokmanas/>; see also <https://www.linkedin.com/in/eimis/>.

⁴⁰ Services, CEOCORP, <https://ceocorp.net/services/>.

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., NordSec B.V., 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., NordSec B.V., and Nord Security Inc.

34. Both Defendants and non-Defendants NordSec Ltd., NordSec B.V., and Nord Security Inc. have been represented by the same counsel in cases filed in North Carolina and California, where non-Defendants NordSec Ltd., NordSec B.V., and Nord Security Inc. were also named as defendants.

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

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

FACTUAL ALLEGATIONS

A. Background on the Subscription e-Commerce Industry

37. 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.

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

Given the prevalence of online and e-commerce retailers, subscription e-commerce has grown rapidly in popularity in recent years. Indeed, the “subscription economy has grown more than 400% over the last 8.5 years as consumers have demonstrated a growing preference for access to subscription services[.]”⁴² According to the Washington Post, analysts at UBS predict the subscription economy will expand into a \$1.5 trillion market by 2025, up from \$650 billion in 2020.⁴³

38. The production, sale, and distribution of subscription-based products and services is a booming industry that has exploded in popularity 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.”⁴⁴

39. 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, even after the pandemic subsides in the United States.”⁴⁵

40. 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

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 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/>.

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

⁴⁵ Heather Long and Andrew Van Dam, *supra* note 43.

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 manipulative designs.”⁵⁰ That is, to facilitate consumer inertia, some subscription e-commerce companies, including Defendants, “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

41. 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

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.*

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 (Jun. 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>.

subscription marketing plan.”⁵² Moreover, “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.

42. 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 (ISO) 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

43. 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-

⁵² Heather Long and Andrew Van Dam, *supra* note 43 (“‘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>.

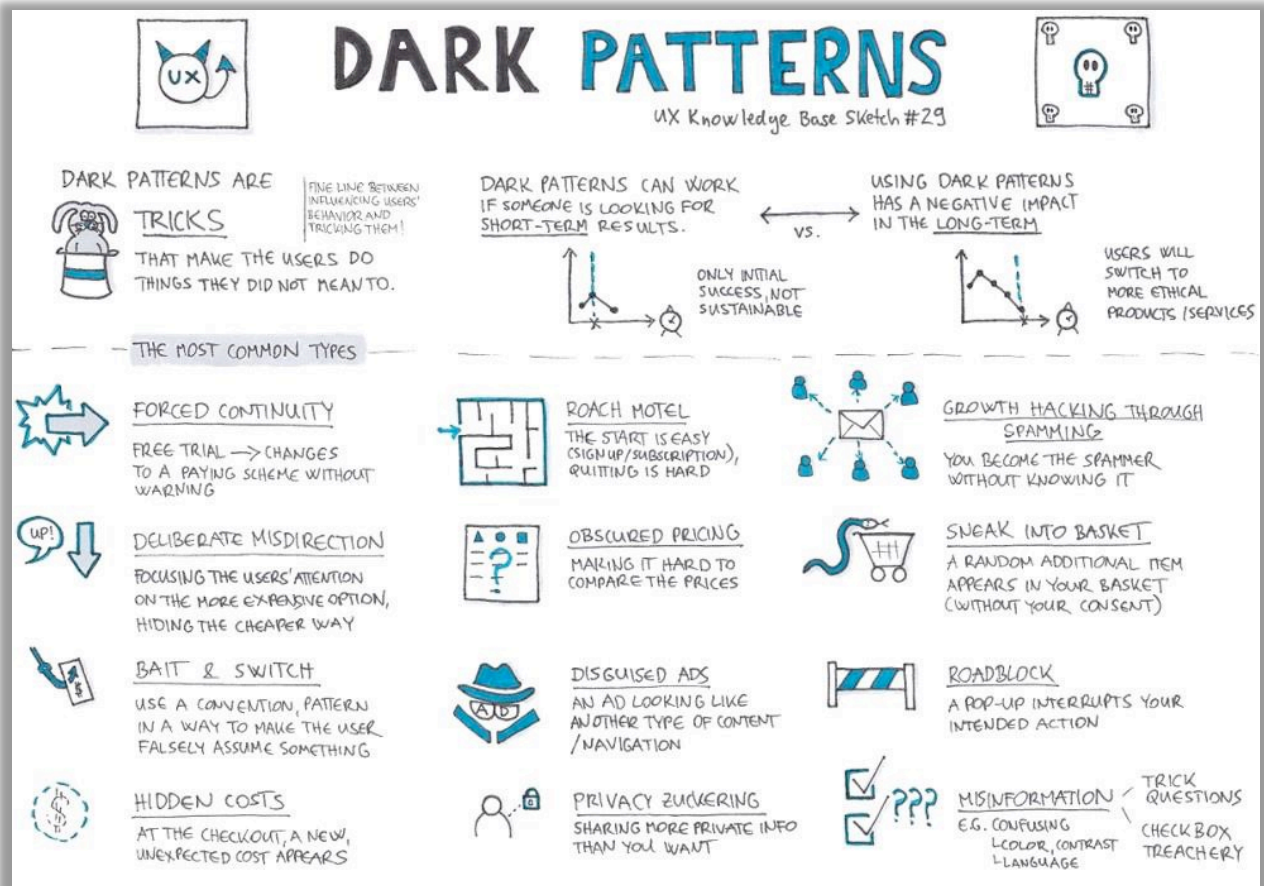
⁵³ Heather Long and Andrew Van Dam, *supra* note 43.

⁵⁴ *Id.*

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>.

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 following image provides some examples of commonly employed dark patterns:⁵⁹



44. 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 following image

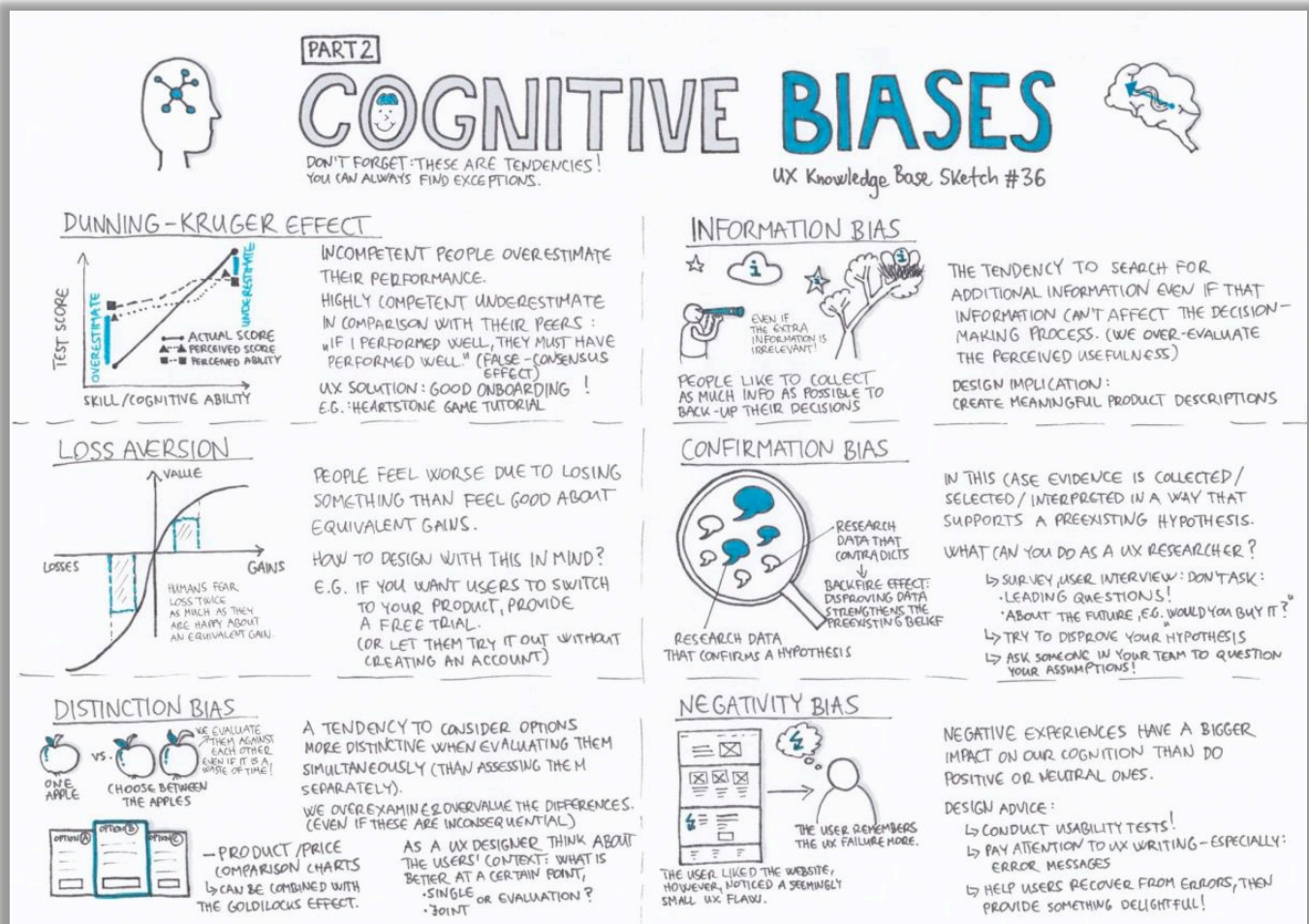
⁵⁷ Harry Brignull, *Bringing Dark Patterns to Light*, MEDIUM (June 6, 2021), <https://harrybr.medium.com/bringing-dark-patterns-to-light-d86f24224ebf>.

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>.

⁶⁰ Brignull, *supra* note 57.

provides examples of cognitive biases, including some that Defendants employ in their cancellation process:⁶¹



45. 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

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

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>.

46. 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 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.

47. 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

48. Defendants have engaged in these unlawful subscription practices with great success. In 2023, Nord Security raised \$100 million from investors, with the company valued at \$3 billion.⁶⁷ Nord Security’s products and services have over 15 million users.

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>.

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>.

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

49. Upon information and belief, the payment page for Nord Security’s enrollment process that Plaintiff used in January 2022 was materially similar to the Nord Security payment page reproduced below:

The screenshot displays the NordVPN checkout interface. At the top, it says 'NordVPN Checkout' and 'Already have Nord Account? Log in'. A '30 DAY MONEY-BACK GUARANTEE' badge is visible. The page is divided into two main sections: 'Create an account' and 'Order summary'.

Create an account: Includes a text field for 'Your email address' with the placeholder 'name@example.com'. Below it, a note states: '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: Lists several options with right-pointing arrows: 'Credit or debit card' (with logos for VISA, Mastercard, American Express, and Discover), 'PayPal', 'AmazonPay', 'Google Pay', and 'Crypto Currencies'.

Order summary: Shows the 'Standard plan' as a '2-year plan (\$3.79/mo) + 3 EXTRA months' for '\$102.33', with a 'Save 54%' indicator showing a crossed-out price of '\$223.83'. It also lists 'Tax country: United States' with a 'Sales tax 8.875%' of '\$9.08', resulting in a 'Total' of '\$111.41*'. Below this, there are links for 'Got a coupon?' and 'See available locations'. A section 'Recommended for NordVPN users' features 'Incogni data removal tool (\$3.69/mo)' with a description 'Get your personal info off the market.' and a 'View details and terms' link.

* 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@nordcheckout.com](#) [Terms of Service](#) [Cookie Preferences](#)

50. 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 the Colorado Autorenewal Law, Colo. Rev. Stat. § 6-1-732 (“ARL”). The solid black line added above signifies that the fine print on Nord Security’s payment screen that includes Defendants’ (inadequate) “disclosures” about their automatic renewal offer 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* Colo. Rev. Stat. § 6-1-732(2)(a) (requiring companies like Nord Security “to present the automatic renewal offer terms in a clear and conspicuous manner before the automatic renewal contract is executed”).

51. Instead, the payment page’s overall design, including the location of Defendants’ supposed “disclosure,” its font, 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.






52. Defendants’ fine print also fails to disclose key details about Nord Security’s subscription practices, including the cancellation policy and information on how to cancel.

53. 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.

54. 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.

55. When a consumer selects a payment method on the payment screen (e.g., credit card, PayPal), the payment method box expands, again failing to disclose Nord Security’s autorenewal terms, let alone do so in a clear and conspicuous manner. Like the below-the-fold “disclosures” that consumers must scroll to see, these “disclosures” are rendered in small, light gray text that is not in larger type than the surrounding text, in contrasting type, font, or color to the surrounding text of the same size, or 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:


3. Select a payment method

Credit or debit card     


Payment information

First name

Last name


Card number 

Expiration date

CVV/CVC 

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

Services are subscription based and will automatically renew until you cancel. See subscription and cancellation [terms](#).

[Continue](#)  You're 100% backed by our 30-day money-back guarantee.

Payments are processed in USD. Payment provider fees may apply.

56. The expanded payment boxes also do not present the consumer with any information about the length of the renewal term, information on recurring charges that will be made to the consumer’s payment account as part of the automatic renewal, or a description of the

cancellation policy or the methods that may be used to cancel the subscription, let alone a method that is easily accessible.

57. In sum, 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.

58. 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.

59. Instead, Nord Security provides tiny, inconspicuous hyperlinks to "terms of service" and "terms" which themselves do not clearly and conspicuously explain the nature of Nord Security's trial and promised refund, autorenewal charges, or its cancellation mechanism. Instead, Nord Security scatters confusing, inconsistent, and inaccurate provisions addressing these and other issues across multiple sections of these documents (which total more than 9,500 words), burying them inconspicuously in dense surrounding text.

60. Moreover the (inadequate) "disclosures" in Nord Security's below-the-fold text and in the expanded payment boxes also violate the ARL for an additional reason. While they purport to "[u]tilize an online link" to "direct[] a consumer" to additional information about the automatic renewal, those links are not "labeled with, or is directly adjacent to, a clear and conspicuous disclosure that states that by purchasing the good or service, the consumer agrees to enroll in an automatic renewal contract" and thus violate subsection 2(b) of the ARL. *See* Colo. Rev. Stat. § 6-1-732(2)(b)(III).

61. Moreover, because consumers must scroll down to view the below-the-fold automatic renewal terms at the bottom of the page, any links in or around Nord Security's

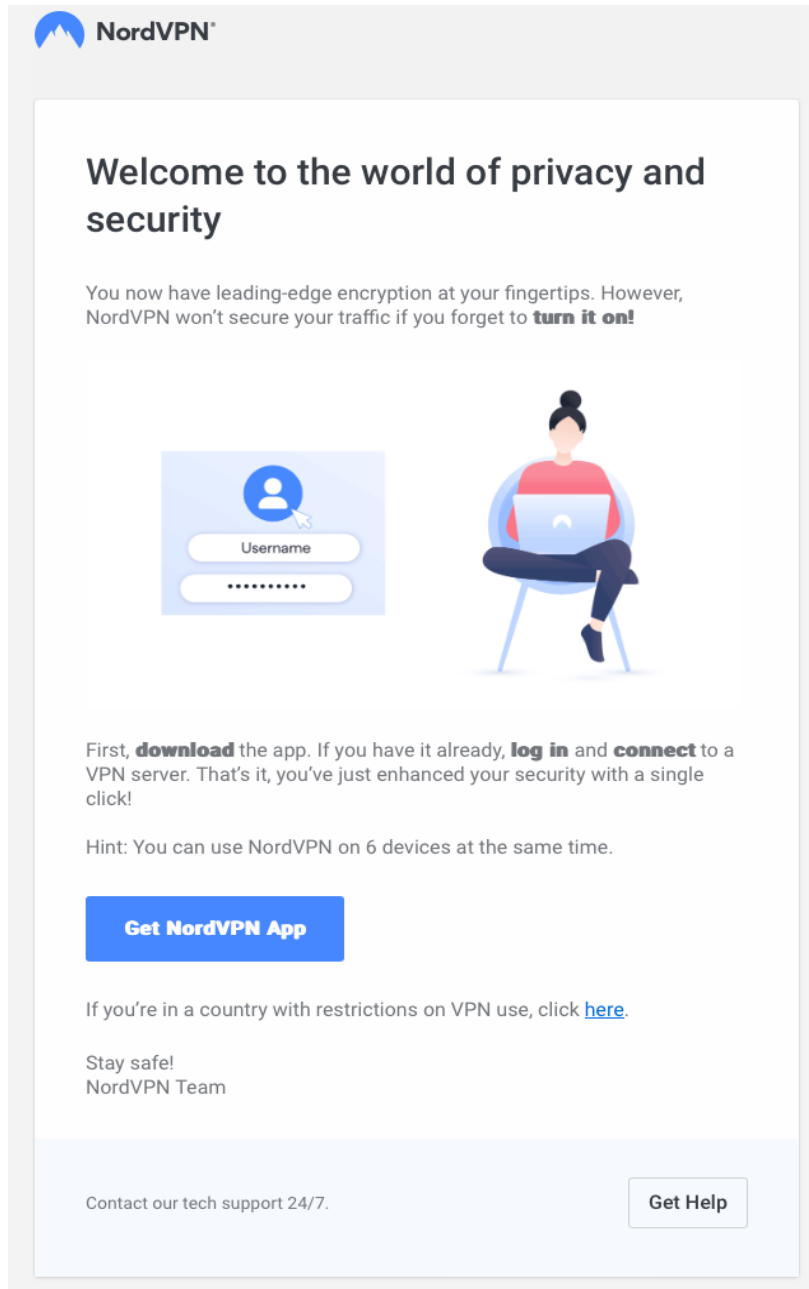
automatic renewal offer that purport to direct consumers additional details about the automatic renewal contract are not “directly adjacent” to the button the consumer uses to purchase a Nord Security product. *See id.* § 6-1-732(2)(b)(II).

62. Upon information and belief the then-most recent version of Nord Security’s “terms of service” linked to at the time Plaintiff enrolled in his Nord Security subscription contain the following sentence in the “Payments” paragraph:

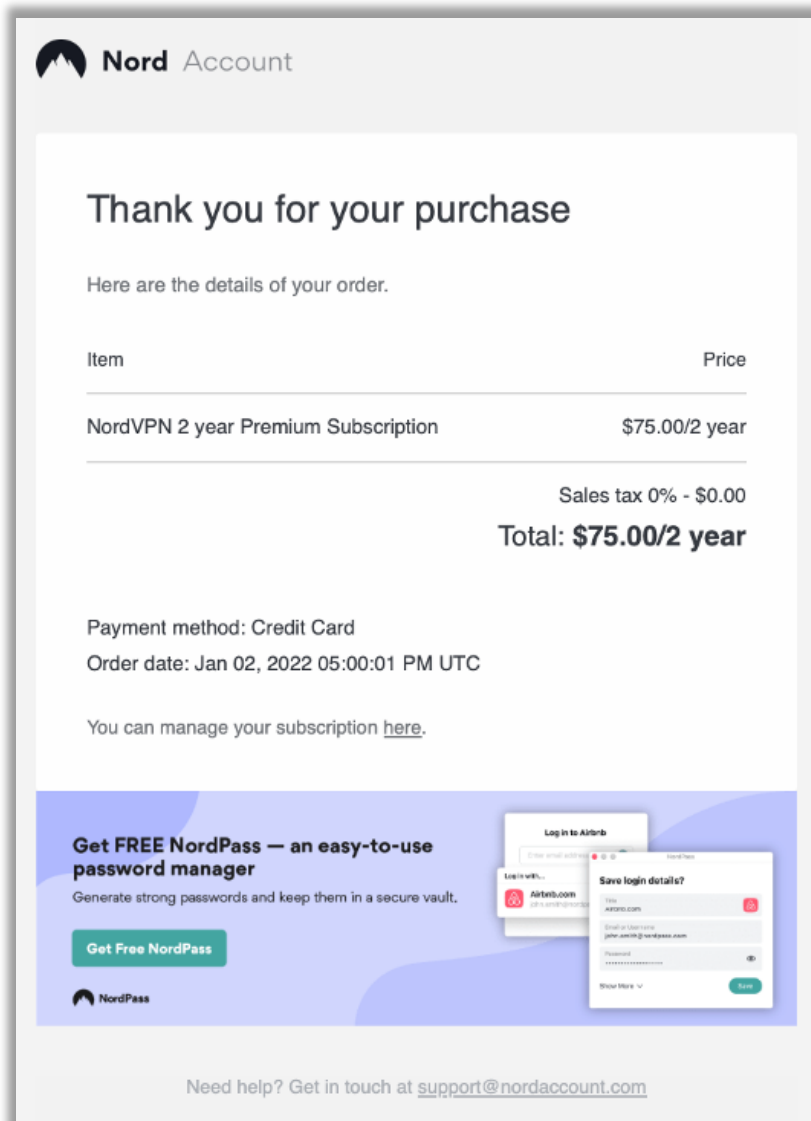
Your service will automatically be renewed, and your chosen payment method will be charged at the end of each service period, unless you decide to cancel your automatic payments for the Services before the end of the then-current subscription.

63. 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 “Payment” paragraph excerpted 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.

64. After Plaintiff enrolled in Nord Security, Nord Security sent Plaintiff an email with the subject line “Welcome to NordVPN!” A representative version of the acknowledgement email sent to Plaintiff and other consumers is shown on the next page:



65. After Plaintiff enrolled in Nord Security, Nord Security also sent Plaintiff an email containing the word “receipt” in the subject line. The content of the email sent to Plaintiff is shown on the next page:



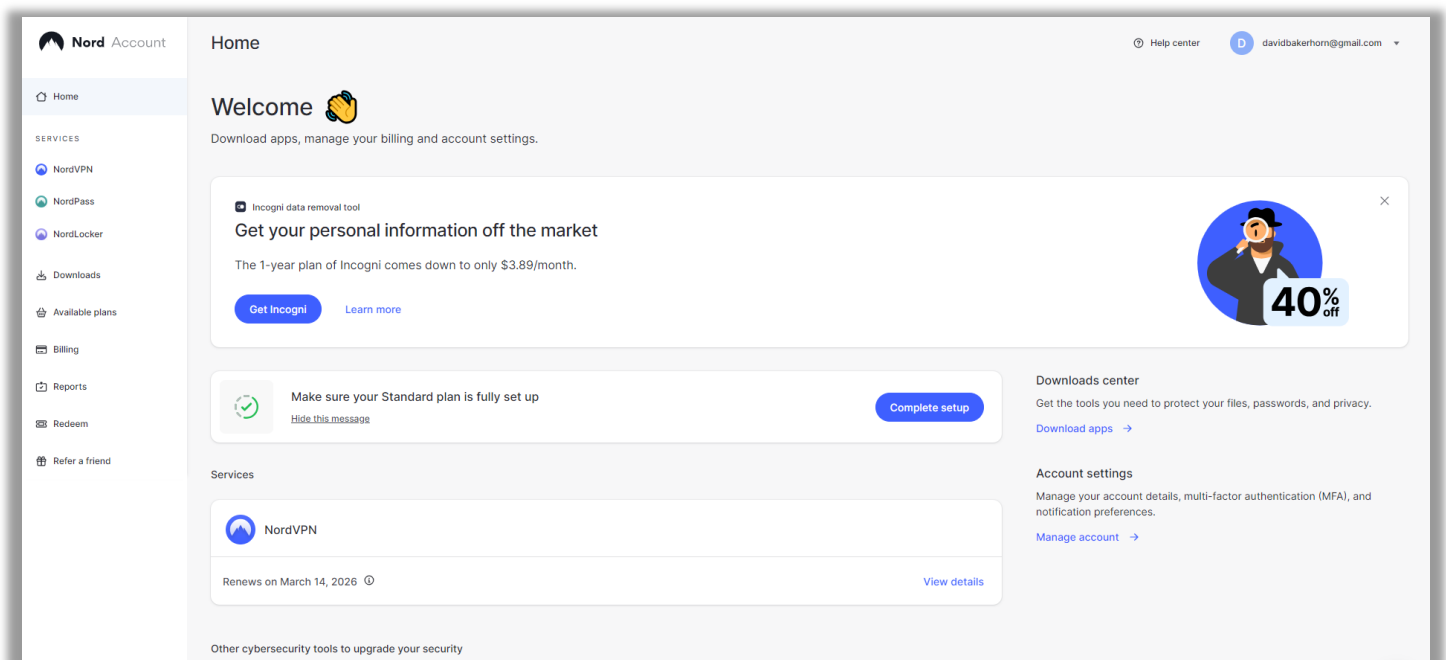
66. Neither Defendants’ post-enrollment acknowledgement nor receipt emails meet the post-purchase requirements that the ARL imposes on an automatically renewing product or service. They do not provide any information on Nord Security’s “automatic renewal offer terms, the cancellation policy, [nor] information regarding how to cancel.” Colo. Rev. Stat. § 6-1-732(2)(c); *see also id.* § 6-1-732(1)(c)(I) (defining “automatic renewal offer terms” to include five disclosures that must be “clear and conspicuous”).

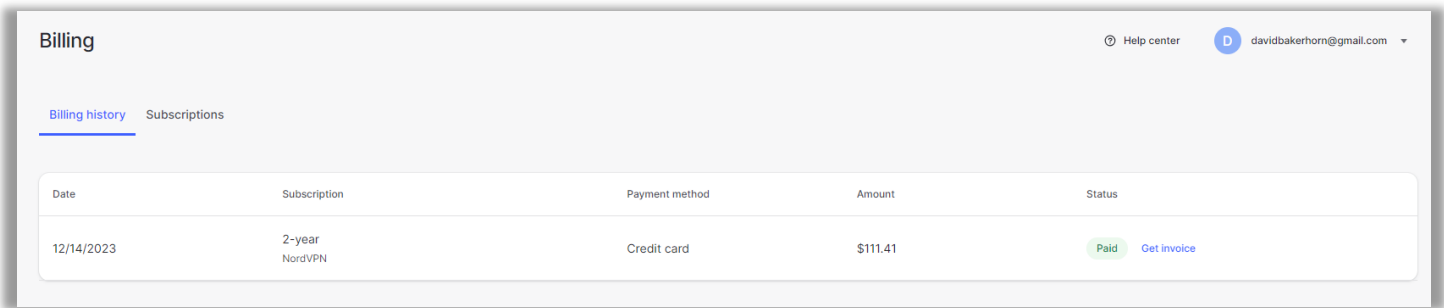
67. Nord’s failure to comply with the ARL’s protections injured Plaintiff and Class Members.

C. Nord Security’s Cancellation Process Violates the ARL

68. Nord Security’s cancellation process is not “simple, cost-effective, timely, easy-to-use, [nor] readily accessible to consumers.” Colo. Rev. Stat. § 6-1-732(2)(d). 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.

69. 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 during the period of his enrollment were materially similar to Nord Security’s current Home and Billing pages copied below and on the next page:



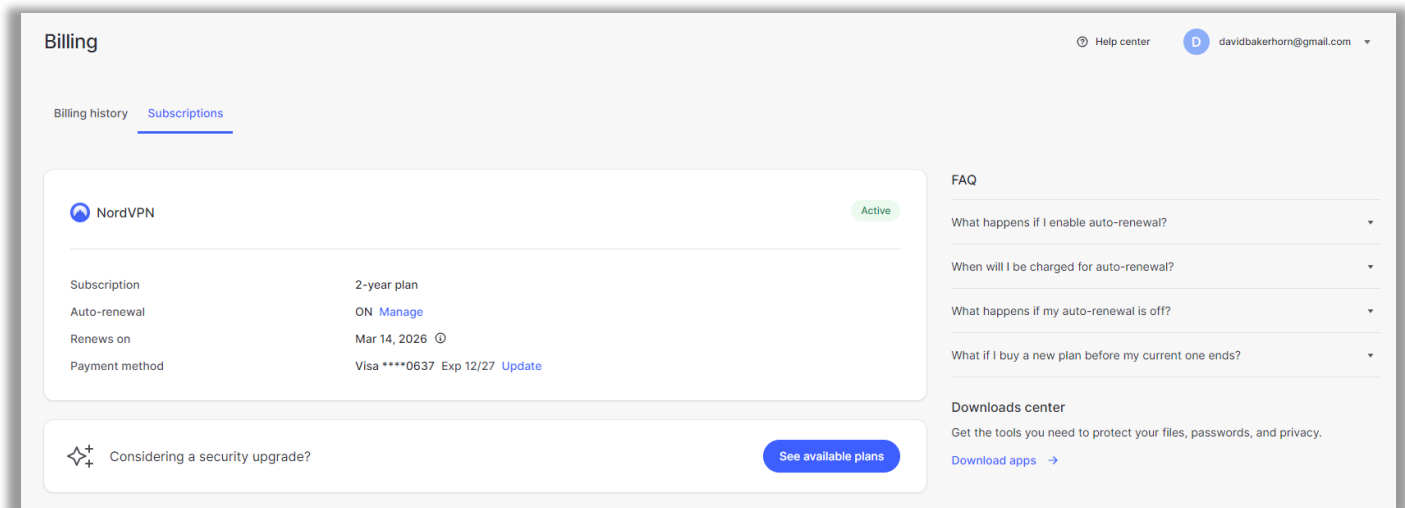


Billing Help center David Bakerhorn

[Billing history](#) [Subscriptions](#)

Date	Subscription	Payment method	Amount	Status
12/14/2023	2-year NordVPN	Credit card	\$111.41	Paid Get invoice

70. 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 during the period of his enrollment was materially similar to the Nord Security “Subscriptions” tab as copied below, as was the page consumers view when they click “Manage” next to “Auto-renewal,” in the image on the next page:



Billing Help center David Bakerhorn

[Billing history](#) [Subscriptions](#)

NordVPN Active

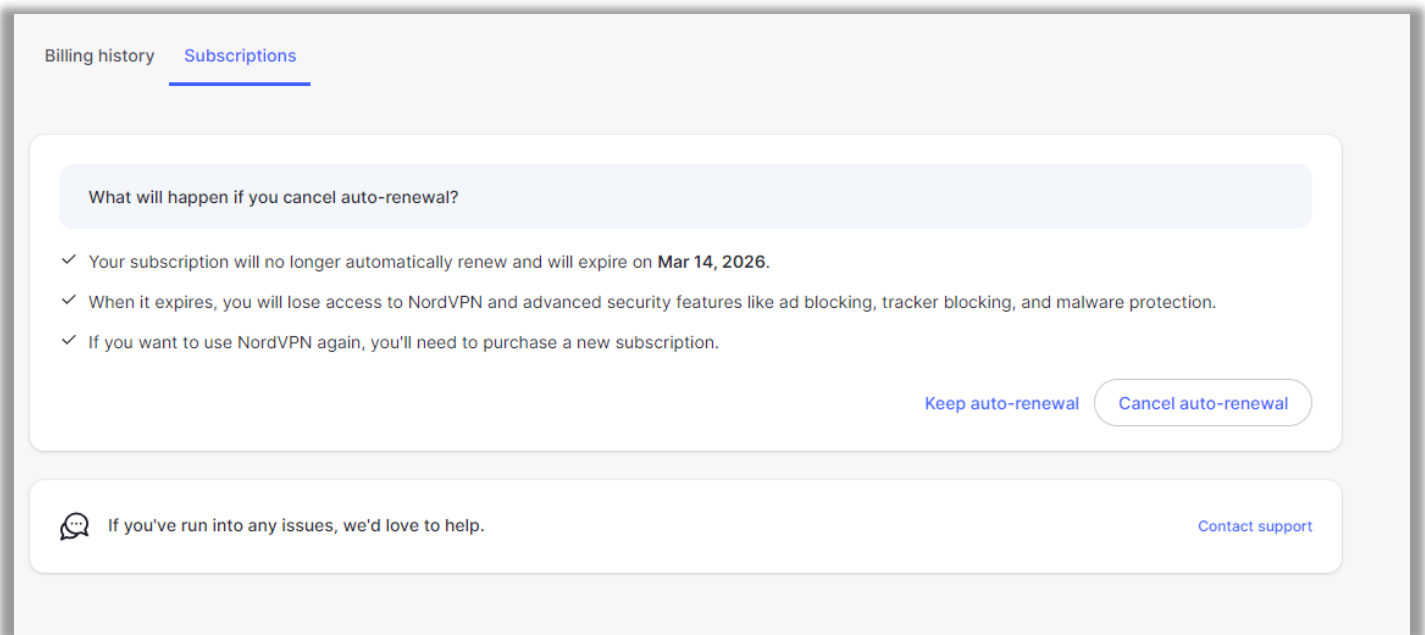
Subscription	2-year plan
Auto-renewal	ON Manage
Renews on	Mar 14, 2026 ⓘ
Payment method	Visa ****0637 Exp 12/27 Update

⚙️ Considering a security upgrade? [See available plans](#)

FAQ

- What happens if I enable auto-renewal? ▾
- When will I be charged for auto-renewal? ▾
- What happens if my auto-renewal is off? ▾
- What if I buy a new plan before my current one ends? ▾

Downloads center
Get the tools you need to protect your files, passwords, and privacy.
[Download apps](#) →



71. 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 simple, cost-effective, timely, easy-to-use, or readily accessible to consumers.” Colo. Rev. Stat. § 6-1-732(2)(d).

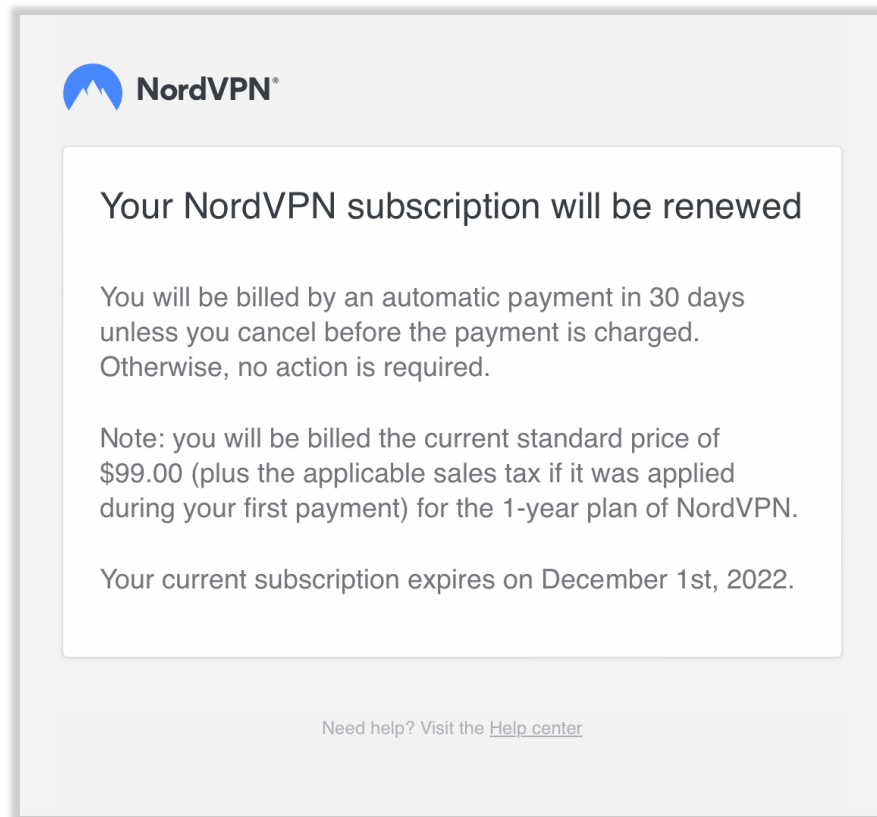
72. For those consumers who use Nord Security’s mobile application, like Plaintiff, there is no way to in which to cancel autorenewal in the mobile app. This too violates the ARL. *Id.*

D. Nord Security’s Insufficient Autorenewal “Notice” Violates the ARL

73. Under the ARL, Nord Security must provide notice of the upcoming automatic renewal “at least twenty-five and no more than forty days before the first automatic renewal.” *Id.* § 6-1-732(4)(b). The notice must inform the consumer of the simple, cost-effective, timely, easy-to-use, and readily accessible process for cancelling the automatic renewal. *Id.* § 6-1-732(4)(a); *see also id.* § 6-1-732(2)(d). It must also “provide clear and accurate information about the identity of the sender.” *Id.* § 6-1-732(4)(a).

74. During the time that Plaintiff was a Nord Security customer, counsel’s investigation shows that approximately one month before executing some autorenewals, Nord Security may have sent consumers an email with the subject line “Subscription renewal in 30 days.”

75. A true and accurate example of this email is shown below:



76. While Plaintiff has no record of receiving such an email, the email, if sent, fails to comply with the ARL. Nord Security’s email misleads the customer as to the date by which the customer must cancel to avoid being charged for an automatic renewal. The email lists the date on which the current subscription period expires (in the example, “December 1st”), but carefully and intentionally omits the fact that the customer must cancel at least 14 days prior to December 1st to avoid being charged again.

77. Nord Security’s email is intended to mislead consumers into thinking that they can avoid an autorenewal charge if they cancel by the subscription expiration date.

78. Nord Security’s email also omits the *time* a consumer must cancel their subscription in order to avoid future charges. For example, the representative email shown above was received by a Nord Security customer on October 17, 2022 at 8:05 p.m. PDT. But a consumer who attempted to cancel their Nord Security subscription on November 16, 2022 (30 days later) might find that they were too late: for example, the customer sent the above email was billed automatically on November 16, 2022 at 7:06 p.m. PST, with nearly 5 hours remaining in the day.

79. Nord Security’s email does not “inform the consumer of the process for canceling the automatic renewal contract.” *See* Colo. Rev. Stat. § 6-1-732(4)(a). The email simply states that the user must “cancel” to avoid a charge but provides no information whatsoever on how to do so. For example, the Nord Security email does not provide a “one-step online cancellation link.” *Id.* at § 6-1-732(2)(d)(I). Indeed, the only link that Nord Security provides—in tiny, light gray font at the bottom of the email, which is not clear and conspicuous—is to Nord Security’s “Help center.” The landing page consumers go to if they click on the link to the “Help center” does not even include the word “cancel.”⁶⁸

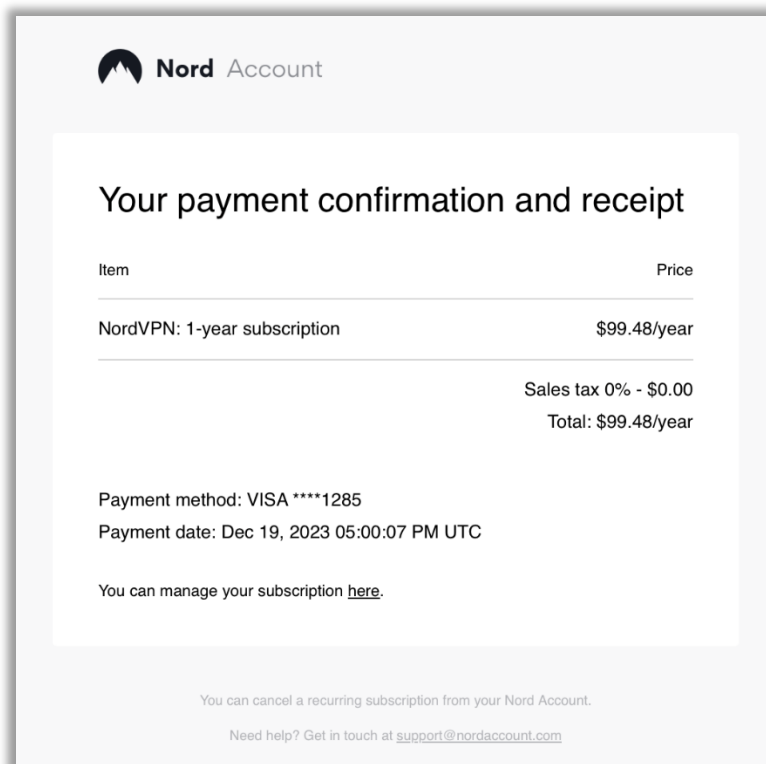
80. Nord Security’s email also does not “provide clear and accurate information about the identity of the sender.” *Id.* § 6-1-732(4)(a).

81. Instead, it is supposedly sent from “The NordVPN team,” a vague and confusing reference in light of the multitude instrumentalities and alter egos employed by each Defendant. *See supra* ¶¶ 25–36.

82. Nord Security’s email, sent prior to automatic renewal, is in stark contrast to Nord Security’s receipt email it sends *after* a consumer has been charged for an automatic renewal—and when it is too late to cancel and avoid the charge. Although Nord Security’s automatic renewal

⁶⁸ <https://support.nordvpn.com/hc/en-us>.

receipt email also violates the ARL, it does at least attempt to provide consumers with clues on how to cancel. For example, as shown below, the automatic renewal receipt email states that the consumer “can manage [their] subscription here” where “here” is a hyperlink to a login page for Nord Security’s account dashboard. It also advises (albeit again neither clearly nor conspicuously) that the consumer “can cancel a recurring subscription from your Nord Account” and tells the consumer that they may “[g]et in touch” with the Company using the email address support@nordaccount.com, as reproduced below:



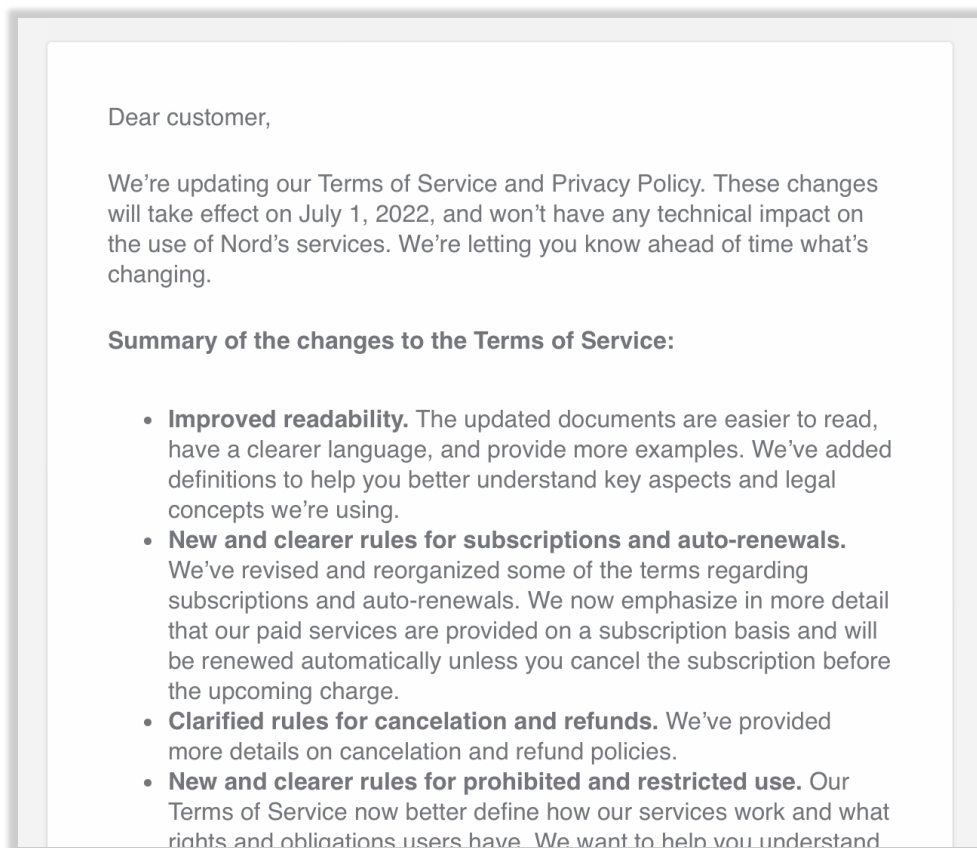
E. Nord Security Violates the ARL’s Requirements with Respect to Material Changes to Consumers’ Automatic Renewal Terms

83. In at least July 2022, Nord Security made material changes to the automatic renewal terms applicable to Plaintiff and other Colorado consumers whose accounts were set to automatically renew.

84. On or about June 17, 2022, Nord Security sent Colorado consumers an email regarding updates to Nord Security’s “Terms of Service” effective July 1, 2022. In relevant part, the email stated that the Company 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.”

85. An excerpt of the June 17, 2022 email sent to Plaintiff that contains material changes to the terms of Nord Security customers’ automatic renewal contract is reproduced below:



86. The June 17, 2022 emails 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 contract terms on July 1, 2022. *See* Colo. Rev. Stat. § 6-1-732(3).

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)).

87. The June 17, 2022 email also fails to comply with the ARL's material change provision because it does not "provide to the consumer, in a manner that may be retained by the consumer, . . . information regarding cancellation of the automatic renewal contract," including information" on the "simple, cost-effective, timely, easy-to-use, and readily accessible mechanism" that the ARL requires Nord Security to offer. *Id.* Indeed, the email provides ***no*** information whatsoever on how to cancel.

88. The changes Nord Security made to its automatic renewal terms on July 1, 2022 were material. For example, the June 17, 2022 email states that the Terms of Service will be changed to provide "more details on cancelation and refund polices." A "description of [a company's] cancellation policy" is one of the automatic renewal offer terms that must be disclosed to consumers under the ARL, Colo. Rev. Stat. § 6-1-732(1)(b)(II)., and thus notice of any material changes to that policy must be made in a manner that complies with Colo. Rev. Stat. § 6-1-732(3), which Nord Security's June 17, 2022 email fails to do.

89. Nord Security's "notice" email before a customer's subscription is automatically renewed, as described above at ¶¶ 73–82, likewise contains material changes to automatic renewal terms, including the length of the subscription term and the price. Nord Security's supposed "notice" email thus also fails to comply with the ARL's material change provision because it does not provide "information regarding cancellation of the automatic renewal contract" "in a manner that may be retained by the consumer." Colo. Rev. Stat. § 6-1-732(3).

F. How Nord Security's Subscription Practices Injured Plaintiff

90. Plaintiff was injured by Nord Security's unlawful and deceptive subscription scheme because had Plaintiff known he was enrolling in an automatically renewing subscription, he would not have enrolled in a Nord Security subscription.

91. On approximately January 2, 2022, Plaintiff enrolled in a two-year subscription to Nord Security's NordVPN service.

92. On January 2, 2022, Plaintiff received a receipt from Nord Security for \$75.00 for the NordVPN service.

93. After signing up for Nord Security's VPN service, Plaintiff downloaded the NordVPN desktop and mobile applications.

94. Plaintiff decided he did not want to continue with Nord Security after his two-year plan ended.

95. Having decided not to continue with Nord Security, Plaintiff believed that once his plan period was over, he would no longer be a Nord Security customer. Indeed, Plaintiff never expected to pay Nord Security anything beyond what he had already paid in January 2022 because Nord Security did not adequately disclose to Plaintiff that it would begin charging non-refundable recurring fees of \$99.48 on a yearly basis after his two-year plan concluded.

96. Nonetheless, on or about December 19, 2023, less than two years after Plaintiff purchased the two-year plan, Nord Security charged Plaintiff's credit card \$99.48 without his knowledge or permission for a one-year NordVPN subscription set to begin on or about January 2, 2024.

97. At some point after Nord Security made the unauthorized \$99.48 charge to Plaintiff's credit card in December 2023, Plaintiff discovered that Nord Security had charged his credit card without his knowledge or permission.

98. Thereafter, Plaintiff attempted to cancel his Nord Security subscription but was unable to do so.

99. Nord Security did not “clearly and conspicuously” disclose to Plaintiff that it would automatically renew his Nord Security subscription for a one-year term at \$99.48 after his initial two-year plan expired.

100. 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.

101. Similarly, Nord Security did not “clearly and conspicuously” disclose to Plaintiff how he could cancel his Nord Security subscription. 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.

102. Nord Security failed to provide Plaintiff with the legally required notice of upcoming automatic renewal of his Nord Security subscription.

103. Nord Security also failed to clearly and conspicuously provide required notices of material changes made to its automatic renewal terms and did not disclose how to cancel Plaintiff’s Nord Security subscription in its June 2022 email, as well as the email sent to Plaintiff that included material changes to the terms of Plaintiff’s initial Nord Security subscription in the price and length for the autorenewal made in 2023.

104. Plaintiff did not authorize or want his Nord Security subscription to renew.

105. Plaintiff was injured when Nord Security subscription charged his credit card \$99.48 for a Nord Security subscription he did not want and did not want to pay for.

106. 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 Security subscription.

107. 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.

108. 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 of 2023, 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

109. 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:

110. **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 Colorado through a deceptive subscription scheme by making the material misrepresentations and omissions alleged in detail above in violation of Colorado 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 service paying for subscriptions that they do not want.

111. 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 "written acknowledgment that includes the automatic renewal offer terms, the cancellation policy, and information regarding how to cancel in a manner that is capable of being retained by the consumer," Colo. Rev. Stat. § 6-1-732(2)(c). In fact, neither Nord Security's acknowledgment nor receipt emails 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) “inform the consumer of the process for canceling the automatic renewal contract;” (2) utilize a cancellation process that is “simple, cost-effective, timely, easy-to-use, and readily accessible;” and (3) “provide clear and accurate information about the identity of the sender” of the notice. 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.

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

113. **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 on approximately January 2, 2022, through Nord Security’s acknowledgment and receipt emails sent to Plaintiff, Nord Security’s “terms of service” and “terms” hyperlinks, Nord Security’s June 17, 2022 material change email, and Plaintiff’s unsuccessful attempt to cancel his account after learning that Nord Security had charged him for an unwanted automatic renewal sometime after December 19, 2023. Nord Security uses the same or substantially similar deceptive and unlawful subscription practices scheme for all of its customers.

114. **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.

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

CLASS ACTION ALLEGATIONS

116. 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 Colorado (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”).

117. 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.

118. 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.

119. 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.

120. 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.

121. 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.

122. 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.

123. 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.

124. 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 Colorado ARL;

- b. Whether Defendants' conduct violates the applicable Colorado consumer protection statutes;
- 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.

125. 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.

126. 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 the applicable Colorado consumer protection statutes;
- 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.

127. 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

COLORADO CONSUMER PROTECTION ACT **(COLO. REV. STAT. § 6-1-101, *et seq.*)**

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

129. Plaintiff brings this claim on his own behalf and on behalf of each member of the Class pursuant to Colo. Rev. Stat 6-1-105(i), (u), (kk), and (rrr), which provide, in pertinent part, that “a person engages in a deceptive trade practice when, in the course of such person’s business, vocation, or occupation, the person:

* * *

(i) Advertises goods, services, or property with intent not to sell them as advertised;

* * *

(u) Fails to disclose material information concerning goods, services, or property which information was known at the time of an advertisement or sale if such failure to disclose such information was intended to induce the consumer to enter into a transaction;

* * *

(kk) Violates any provision of article 6 of this title;

* * *

(rrr) Either knowingly or recklessly engages in any unfair, unconscionable, deceptive, deliberately misleading, false, or fraudulent act or practice[.]”

130. Article 6 of Title 6, “Unsolicited Goods,” Colo. Rev. Stat. § 6-6-101, *et seq.* renders any “unsolicited goods,” including “services delivered to a person who has not ordered, solicited, or agreed to purchase them” *id.* at § 6-6-101(1), intended for the recipient “a gift to the recipient, who may use them or dispose of them in any manner he sees fits without any obligation to the sender,” *id.* at § 6-6-102(2), and further prohibits the sender from billing the recipient for those goods, *id.* at § 6-6-103(1). Any contract between Plaintiff and Defendants is therefore void and unenforceable.

131. In addition, Colo. Rev. Stat. § 6-1-105(3) provides: “The deceptive trade practices listed in this section are in addition to and do not limit the types of unfair trade practices actionable at common law or under other statutes of this state.”

132. Through their deceptive subscription scheme as alleged throughout this Complaint, Defendants engaged in deceptive acts or practices that violated the Colorado Consumer Protection Act 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.

133. By violating Colorado’s auto-renewal law as alleged throughout this Complaint, Defendants are liable to Plaintiff and the Class for committing a deceptive act.

134. 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.

135. Defendants knew or should have known that their conduct violated the Colorado Consumer Protection Act.

136. Plaintiff and Class Members suffered monetary damages as a result of Defendants' conduct.

137. 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.

138. Defendants are liable to Plaintiff and Class Members for actual damages sustained.

COUNT II
CONVERSION

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

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

141. 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.

142. 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.

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

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

145. 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.

146. 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

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

148. Plaintiff brings this claim on his own behalf and on behalf of each member of the Multistate Class under Colorado law or the laws of each of the states where Defendants do business that permit an independent cause of action for unjust enrichment, or, alternatively, on behalf of each member of the individual State Classes under the laws of those States.

149. In all states where Defendants do business, there is no material difference in the law of unjust enrichment as applied to the claims and questions in this case.

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

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 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 Classes 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 \$100,000,000, 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: November 19, 2024

WITTELS MCINTURFF PALIKOVIC

/s/ J. Burkett McInturff

J. Burkett McInturff

Ethan D. Roman

Daniel J. Brenner

305 BROADWAY, 7TH FLOOR

NEW YORK, NEW YORK 10007

Tel: (914) 775-8862

jbm@wittelslaw.com

edr@wittelslaw.com

djb@wittelslaw.com

**MILBERG COLEMAN BRYSON PHILLIPS
GROSSMAN, PLLC**

Scott C. Harris

J. Hunter Bryson

900 W. MORGAN STREET

RALEIGH, NORTH CAROLINA 27603

Tel: 919-600-5000

sharris@milberg.com

hbryson@milberg.com

Co-Counsel for Plaintiff and the Proposed Class

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [NordVPN Lawsuit Filed Over Allegedly Illegal Automatic Subscription Renewal Practices](#)
