UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS

MICHAEL SASGEN, on behalf of himself and sll others similarly situated, **Plaintiff,** **v.** **NORDVPN S.A., AND TEFINCOM S.A. D/B/A NORDVPN**, **Defendants.**	Case No.: _____ **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Michael Sasgen ("Plaintiff"), by his undersigned attorneys Milberg Coleman Bryson Phillips Grossman, PLLC and Wittels McInturff Palikovic, brings this consumer protection action in his individual capacity and on behalf of a class of Illinois 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 illegal "automatic renewal" tactics to trick consumers into paying for unwanted subscriptions for internet privacy and security products ("Nord Subscriptions"). Nord Security intentionally misleads consumers into thinking they can subscribe for a discrete period of time. The truth is, however, that the Nord Subscriptions automatically renew and the Company's "disclosures" regarding the ongoing charges are hidden from consumers both before and after purchase. Nord Security's enrollment and post-purchase practices therefore violate both the Illinois Automatic

Contract Renewal Act (815 ILCS 601/1 *et seq.*, ("Illinois ARL")) and the common law. Further, Nord Security intentionally makes the Nord Subscriptions difficult to cancel and fails to provide adequate notice of material changes to those subscriptions. This too violates the Illinois ARL and the common law.

2. Nord Security offers consumers 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."

3. Potential customers are directed to Nord Security's website through online searches, its sponsorship of influencers, or the Company's advertising. 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. But while consumers enroll in the Nord Subscriptions for better privacy and security, Defendants are actually collecting consumers' payment information and hard-earned money via deceptive and unlawful subscription practices. The practices are intentionally designed to trick consumers into paying unwanted subscription fees. Indeed, that is exactly what happened here, where Plaintiff enrolled in a Nord Subscription that he did not know would automatically

[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).

renew and was then charged multiple times for additional years of that subscription that he did not want.

5. 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 interpret a consumer's silence, failure to take an affirmative action to reject a product or service, or failure to cancel an agreement as acceptance or continued acceptance of the offer."[2] As the CFPB cautions, "[n]egative option programs can cause serious harm to consumers," which "is most likely to occur when sellers mislead consumers about terms and conditions, fail to obtain consumers' informed consent, or make it difficult for consumers to cancel."[3]

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

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 offerings. While each of the deceptive strategies is independently sufficient to trick consumers into making inadvertent purchases, taken together these components work together to

[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.

form an intentionally deceptive architecture that is designed to, and does, produce an unlawful outcome: saddling unwitting consumers with unwanted subscriptions.

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

9. First, during the enrollment process, Nord Security misleads consumers regarding the fact that the Nord Subscriptions automatically renew, the terms of any such automatic renewal, and the cancellation policy that applies to Nord Security's offer. For example, instead of clearly explaining to the consumer what they are actually getting into, Nord Security offers consumers what appear to be time-limited plans and withholds the relevant (and inadequate) terms that reveal otherwise. Nord Security waits until a customer reaches the payment step in its sign up process and then buries a purported "disclosure" regarding its recurring fees in a drop-down feature customers do not see unless they click on it. Instead of alerting consumers and obtaining consumers' informed and affirmative consent to automatic renewal prior to charging their payment cards or third-party payment accounts, Nord Security hides the truth.

10. Second, Nord Security employs a deceptive and highly unconventional charging practice. When a customer's subscription term is approaching its end, rather than drafting customers' payment cards or accounts after the subscription is up, 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.

11. Third, Nord Security makes canceling the Nord Subscriptions 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 failed to provide sufficient notice under Illinois law that the customer's subscription will automatically renew at least 30 days, but no more than 60 days before the subscription automatically renews, because Nord Security's "notice" email failed to provide a "mechanism for cancelling the contract."

13. 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 gauntlet and need only be tricked by one of Nord Security's traps to end up paying a hefty fee for an unwanted subscription.

14. It is not happenstance that Nord Security's customers are paying for unwanted subscriptions. This outcome 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 Nord Security transactions. Upon information and belief, Nord Security has developed customer service protocols for dealing with customers complaining about unwanted subscription charges.

15. 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.

16. 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

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

18. 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.

19. 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.

20. 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

21. Plaintiff Michael Sasgen is a citizen of Illinois.

22. 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 Illinois consumer protection statutes and the common law.

23. 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.

24. 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 Illinois and the rest of the United States purchase. For example, when a consumer visits www.nordsecurity.com they see a typical company website with the "Nord Security" logo that features "our products" (including one of the products purchased by Plaintiff), "our story," "our team" and "our values." Similarly, when top U.S. venture capital firm

Warburg Pincus and others invested $100 million in Defendants and non-Defendants NordSec Ltd. and Nord Security Inc., "Nord Security" issued a press release describing the funding as an investment in "Nord Security, a global leader in internet privacy and security solutions."[4] This same press release states that NordVPN is "the biggest and most popular VPN service in the world" and that "Nord Security was founded in Lithuania in 2012 by co-founders and co-CEOs Tom Okman and Eimantas Sabaliauskas."[5] Likewise, the "Corporate responsibility" page for "Nord Security" shows pictures of the founders, explains "our mission," and contains links to Nord Security's "corporate responsibility reports" and Nord Security's "Code of Conduct,"[6] which discusses such topics as expectations for the "Nord Security brand products, including NordVPN, NordPass, NordLocker, and NordLayer."[7]

25. Defendant Nordvpn S.A. is a Panamanian corporation incorporated under the laws of Panama.[8] Nordvpn S.A.'s principal place of business is in Amsterdam, the Netherlands.[9] Nordvpn S.A. currently "offers" Defendants and non-Defendants NordSec Ltd. and Nord Security Inc.'s products "NordVPN, NordLocker, and NordPass."[10] NordVPN is one of the products

---

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

[5] *Id.*

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

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

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

[9] *Id.*

[10] *Id.*

Defendants and non-Defendants NordSec Ltd. and Nord Security Inc. marketed and sold to Plaintiff in Illinois. Defendant Nordvpn S.A. also currently operates Defendants and non-Defendants NordSec Ltd. and Nord Security Inc.'s website, www.nordvpn.com.[11] Nordvpn S.A.'s corporate parents are 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.[12] Nordvpn S.A. shares an unnamed director with Defendant Tefincom S.A.[13]

26. Defendant Tefincom S.A. d/b/a NordVPN is a Panamanian corporation incorporated under the laws of Panama.[14] Defendant Tefincom S.A.'s principal place of business is Panama City, Panama.[15] Defendant Tefincom S.A.'s corporate parent is Stitching Raveset.[16] Defendants and non-Defendants NordSec Ltd. and Nord Security Inc. admit that Defendant Tefincom S.A. was the contracting entity for Illinois 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."

[11] *Id.*

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

[13] *Zeichner*, Dkt. No. 39-1, ¶ 8.

[14] *Zeichner*, Dkt. No. 39-3, ¶ 3.

[15] *Id.*

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

[17] *Zeichner*, Dkt. No. 39-3, ¶ 3.

27. Non-Defendant NordSec Ltd. is an internet privacy and security company headquartered in London, England.[18] NordSec Ltd. is a private limited liability company organized under the laws of England & Wales.[19] Defendants and non-Defendants NordSec Ltd. and Nord Security Inc. claim that NordSec Ltd. "once owned the intellectual property of the Nord brand."[20] NordSec Ltd.'s corporate parents are Cyberswift B.V., Cyberspace B.V., and Stalwart Holding B.V.[21] NordSec Ltd. is also an owner of non-Defendant NordSec B.V.,[22] Defendant Nordvpn S.A.,2F[23] and Nord Security Inc.[24] Public records indicate that NordSec Ltd. is a prior owner of the "NordVPN" trademark.

28. 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. 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

[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.

[25] *Zeichner*, Dkt. No. 39-2, ¶ 3.

[26] *Id.*

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

corporate parents, Cyberswift B.V. and Cyberspace B.V.[28] NordSec B.V. is also an owner of Defendant Nordvpn S.A.[29] and Nord Security Inc.[30] Defendants and non-Defendants NordSec Ltd. and Nord Security Inc.'s website www.nordsecurity.com claims that "Nord Security trademarks, trade names, company names, logos," whether registered or not, "as well as other Nord Brand features (such as Nord Security websites, applications and creative works embodied therein), are the exclusive property of NordSec B.V. ('Nord Security')."[31] NordSec B.V.'s marks include the marks "Nord Security," "NordVPN," "Nord," "NordSec," NordLocker," and "NordPass." Upon information and belief, the website Plaintiff used to enroll with Nord Security was the website owned by NordSec B.V. and one of the Nord Subscriptions he purchased bore the "Nord Security," "NordVPN," "Nord," and "NordSec" marks owned by NordSec B.V.

29. Non-Defendant Nord Security Inc. is a Delaware corporation.[32] Nord Security Inc.'s corporate parents are NordSec B.V., NordSec Ltd., and Cyberswift B.V.,[33] which is also a corporate parent of NordSec B.V.[34] and NordSec Ltd.[35] Defendants and non-Defendants NordSec Ltd. and Nord Security Inc. claim in a separate litigation that Nord Security Inc. is not the "Nord

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

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

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

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

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

[33] *Id.*

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

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

Security" that offers services to consumers like Plaintiff, instead claiming that Nord Security Inc. provides only business-to-business services.[36]

30. Upon information and belief, at all times pertinent to this action, the finances, policies, and business practices of Defendants and non-Defendants NordSec Ltd. and Nord Security Inc. are and were dominated and controlled by one another in such a manner that each individual Defendant and each of non-Defendants NordSec Ltd. and Nord Security Inc. has no separate mind, will, identity, or existence of its own and instead operated as mere instrumentalities and alter egos of one another. For example, even though public records and fine print on the www.nordsecurity.com website indicate that NordSec B.V. owns the "NordVPN" trademark, the www.nordvpn.com website states that "NordVPN is owned and operated by nordvpn S.A."[37] Similarly, that same website also states that "[b]ack in 2012, two best friends sought to create a tool for a safer and more accessible internet. Driven by the idea of internet freedom, Tom Okman and Eimantas Sabaliauskas created NordVPN."[38] Tom Okman and Eimantas Sabaliauskas are listed as directors of NordSec Ltd., but their respective LinkedIn pages claim they are co-founders of "Nord Security."[39]

31. 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

[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.*

[39] *See* https://www.linkedin.com/in/tokmanas/; *see also* https://www.linkedin.com/in/eimis/.

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 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."[40]

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.

[40] Services, CEOCORP, https://ceocorp.net/services/.

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.

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

33. Defendants and non-Defendants NordSec B.V., NordSec Ltd., and Nord Security Inc. do business in Illinois under the name "Nord Security" and interacted with Plaintiff in Illinois such that their claims described herein arise from Plaintiff's contacts with Defendants and these non-Defendants in Illinois.

34. 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

35. 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

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

e-commerce services target a wide range of customers and cater to a variety of specific interests. Given the prevalence of online and e-commerce retailers, the popularity of subscription e-commerce has grown rapidly in recent years. Indeed, as of 2022 the "subscription economy ha[d] grown more than 400% over the last 8.5 years as consumers have demonstrated a growing preference for access to subscription services[.]"[42]

36. 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."[43]

37. 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."[44] 68% of consumers subscribed to something for the first time in 2024.[45]

38. 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

---

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

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

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

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

more difficult for retailers to dominate the market due to the "highly competitive prices and broad similarities among the leading players."[46] In particular, retailers struggle with the fact that "[c]hurn rates are high, [] and consumers quickly cancel services that don't deliver superior end-to-end experiences."[47]

39. 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 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

[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 (June 25, 2019), https://www.businessinsider.com/dark-patterns-online- shopping-princeton-2019-6.

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]

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

41. 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

---

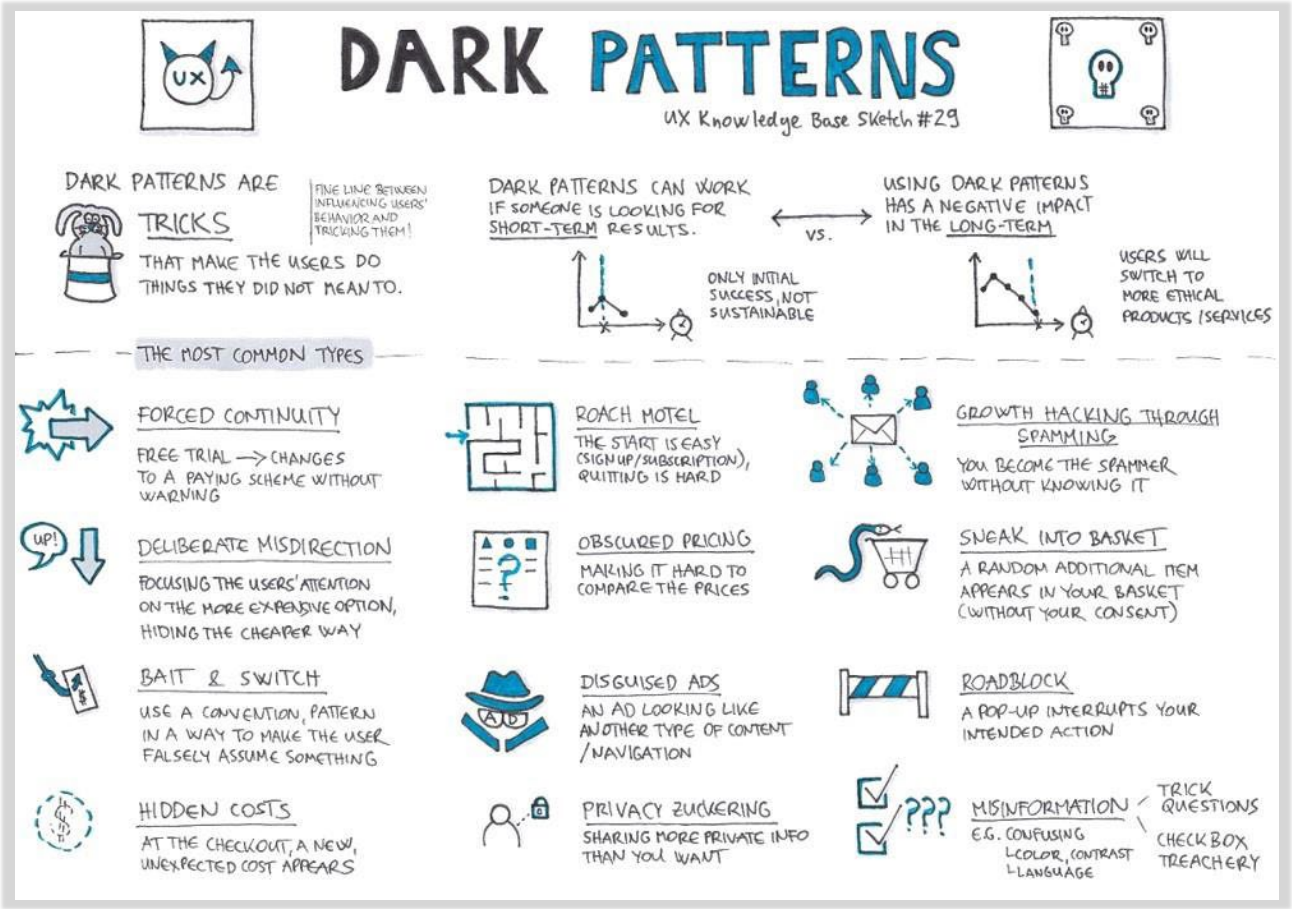
[51] Sarah Perez, *Sneaky subscriptions are plaguing the App Store*, TECHCRUNCH (Oct. 15, 2018), https://techcrunch.com/2018/10/15/sneaky-subscriptions-are-plaguing-the-app-store.

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

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

[54] *Id.*

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



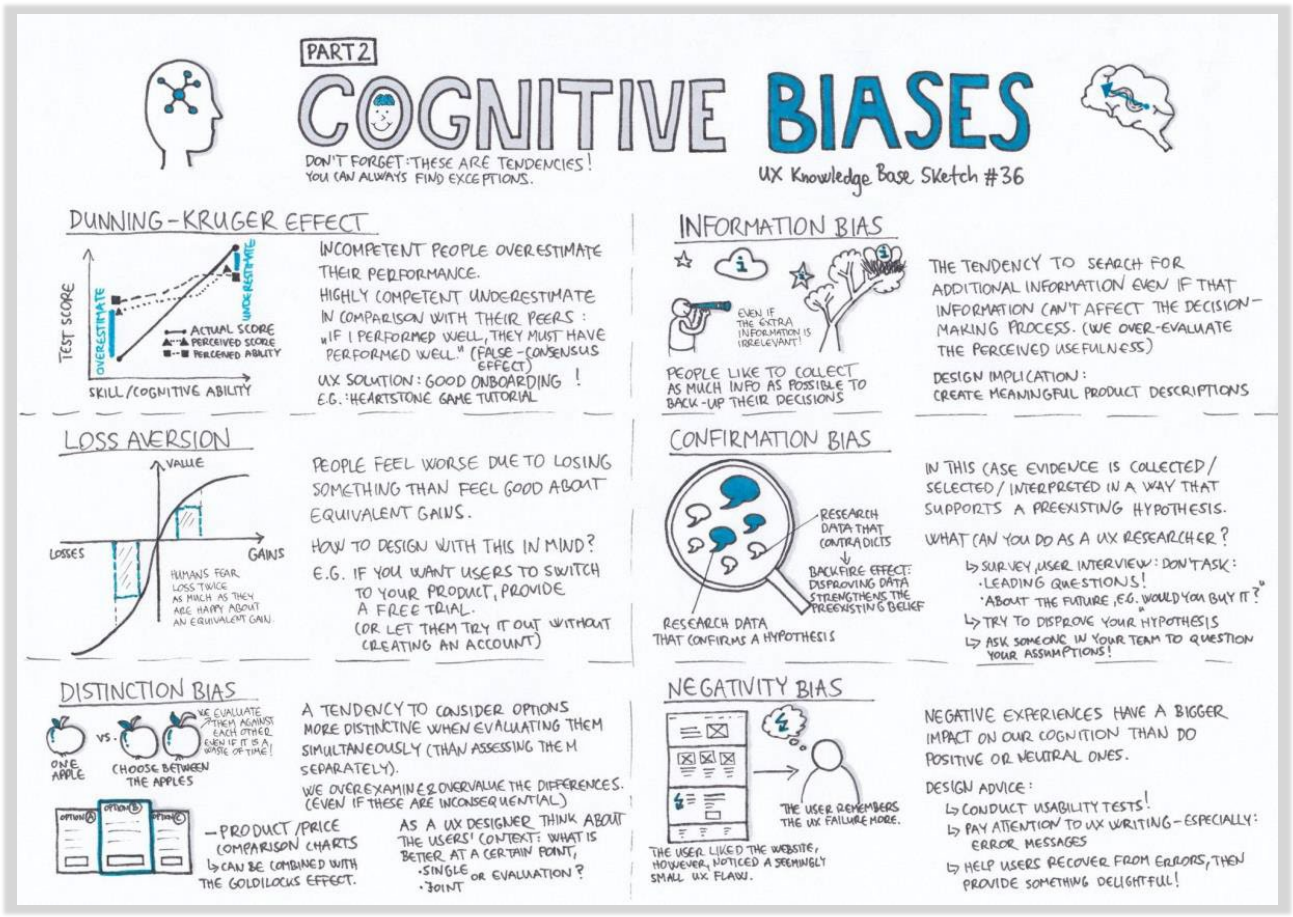
[55] *User Experience (UX): Process and Methodology*, UIUX TREND, https://uiuxtrend.com/user-experience-uxprocess/.

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

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

[58] *Id.*

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



[60] Brignull, *supra* note 57.

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

44. 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.[62]

45. 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.

---

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

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

[64] *Id.*

46. 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]

47. Nord Security has engaged in these unlawful subscription practices with great success. In 2023, Nord Security raised $100 million from investors, with the company valued at $1.6 billion.[67] Nord Security's products and services have over 15 million users, with "[m]ost of Nord's user base [] centered in the U.S."[68]

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

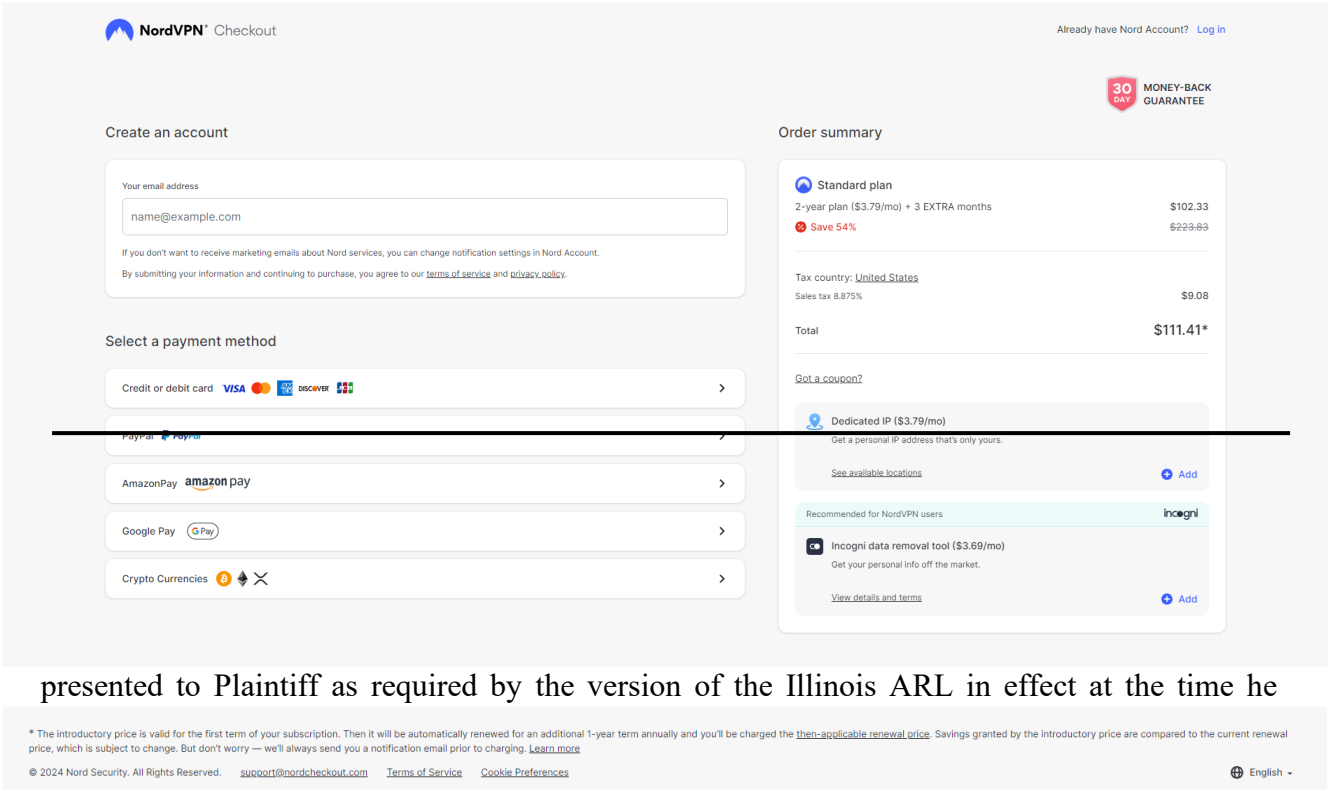
[65] Narayanan *et al*., *supra* note 62.
[66] *Id.*

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

[68] 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/.

48. Upon information and belief, the payment page for Nord Security's enrollment process during the Class Period (*see infra* ¶ 103) and that Plaintiff used in November 2020 was materially similar to the Nord Security payment page reproduced below:

49. The terms and conditions of Nord Security's automatic renewal offer were not



presented to Plaintiff as required by the version of the Illinois ARL in effect at the time he Period. The fine print below the solid black line that includes Defendants' (inadequate) "disclosures" about the automatic renewal offer is technically on Nord Security's payment screen but is not visible unless the consumer scrolls down to view it. The automatic renewal language is also not in larger type than the surrounding font. Instead, it is colored light gray rather than a more conspicuous color and is not set off from the surrounding text of the same size by symbols or other marks in a manner that clearly calls attention to the language. These are intentional design

choices Nord Security made. They also violate the Illinois ARL. *See* 815 ILCS § 601/10 (West 2004) (requiring companies like Nord Security to "disclose the automatic renewal clause clearly and conspicuously"); *see also* 815 ILCS § 601/5 ("'Clear and conspicuous' means in larger type than the surrounding text, or 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.").

50. Instead, the payment page's overall design, including the location of Nord Security's supposed "disclosure" regarding automatic renewal, its font size, and color, ***deemphasize*** the notice text rather than make it ***conspicuous***. Defendants' automatic renewal terms are also 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 supposed "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.

51. Defendants' fine print also fails to disclose key details about Nord Security's subscription practices, including the cancellation procedure.

52. 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. Nord Security's 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.

53. 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 Nord Security's cancellation procedure.

54. When a consumer selects a payment method on the payment screen (*e.g.*, credit card, Paypal, etc.), the payment method box expands, again failing to disclose Nord Security's autorenewal terms, let alone in a clear and conspicuous manner. The expanded payment boxes also do not present the consumer with any disclosure of the cancellation policy or the methods that may be used to cancel the subscription, let alone a cancellation method that is retainable by consumers that is cost-effective, timely, and easy-to-use.

55. In sum, Nord Security's payment page does not clearly and conspicuously disclose the terms of its automatically renewing subscription. In addition, during the Class Period, Nord Security's payment page failed to obtain consumers' affirmative consent to the automatic renewal terms and contains no mechanism for affirmatively consenting to the automatic renewal terms. For example, during the Class Period there was no checkbox that consumers must click to indicate that they accept those terms. *See* 815 ILCS § 601/10 (a)(ii) ("Any person, firm, partnership, association, or corporation that sells or offers to sell any products or services to a consumer pursuant to a contract, where such contract automatically renews unless the consumer cancels the contract, shall . . . not charge the consumer's credit or debit card or other payment mechanism for an automatic renewal service without first obtaining the consumer's consent to the contract containing the automatic renewal offer terms.").

56. Nowhere on the payment page does Nord Security disclose its cancellation procedure, such as how to cancel the subscription and how to turn off autorenewal, and certainly does not clearly and conspicuously disclose how to do so in a manner that is capable of being

retained by the consumer. This too violates the Illinois ARL. *See* 815 ILCS 601/10(a) (West 2004) (requiring companies like Nord Security to disclose "the cancellation procedure" for the subscription "clearly and conspicuously"); *see also* ILCS 601/10(a)(i)–(iii) (same).

57. 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 automatic renewal offer or cancellation mechanism. 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.

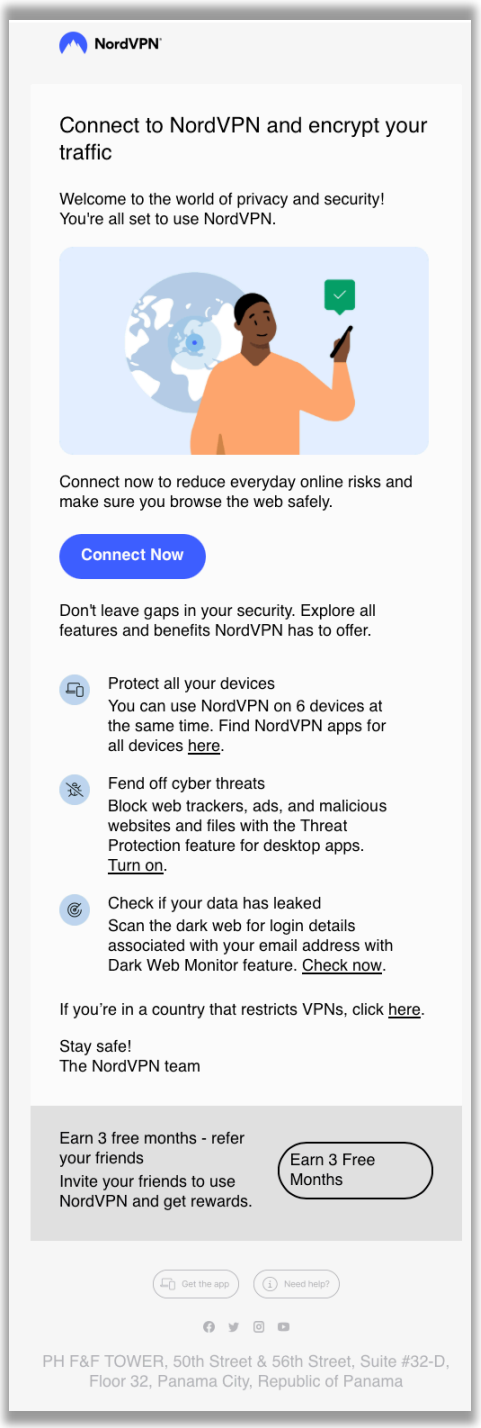
58. For example, upon information and belief, the version of Nord Security's "terms of service" at the time Plaintiff enrolled contained a paragraph labeled "Auto-Renewal," which states as follows:

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

59. This "Auto-Renewal" paragraph gives reasonable consumers the impression that they will be charged only ***after*** the original subscription ends. Meanwhile, a separate Nord Security "terms" document reveals, in a paragraph not cross referenced in the "Auto-Renewal" paragraph above, that customers on plans lasting greater than a month will be charged in advance: "at least 14 days before" the scheduled auto-renewal. This provision is itself in conflict with another provision in the same "terms" document, which states 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. None of this meet the Illinois ARL's clear and conspicuous standard.

60. During the Class Period, after a customer signed up Nord Security sent them an email with the subject line "Welcome to NordVPN!" A representative version of the acknowledgement email is shown on the following page:



NordVPN

Connect to NordVPN and encrypt your traffic

Welcome to the world of privacy and security!
You're all set to use NordVPN.

Connect now to reduce everyday online risks and make sure you browse the web safely.

Connect Now

Don't leave gaps in your security. Explore all features and benefits NordVPN has to offer.

Protect all your devices
You can use NordVPN on 6 devices at the same time. Find NordVPN apps for all devices here.

Fend off cyber threats
Block web trackers, ads, and malicious websites and files with the Threat Protection feature for desktop apps. Turn on.

Check if your data has leaked
Scan the dark web for login details associated with your email address with Dark Web Monitor feature. Check now.

If you're in a country that restricts VPNs, click here.

Stay safe!
The NordVPN team

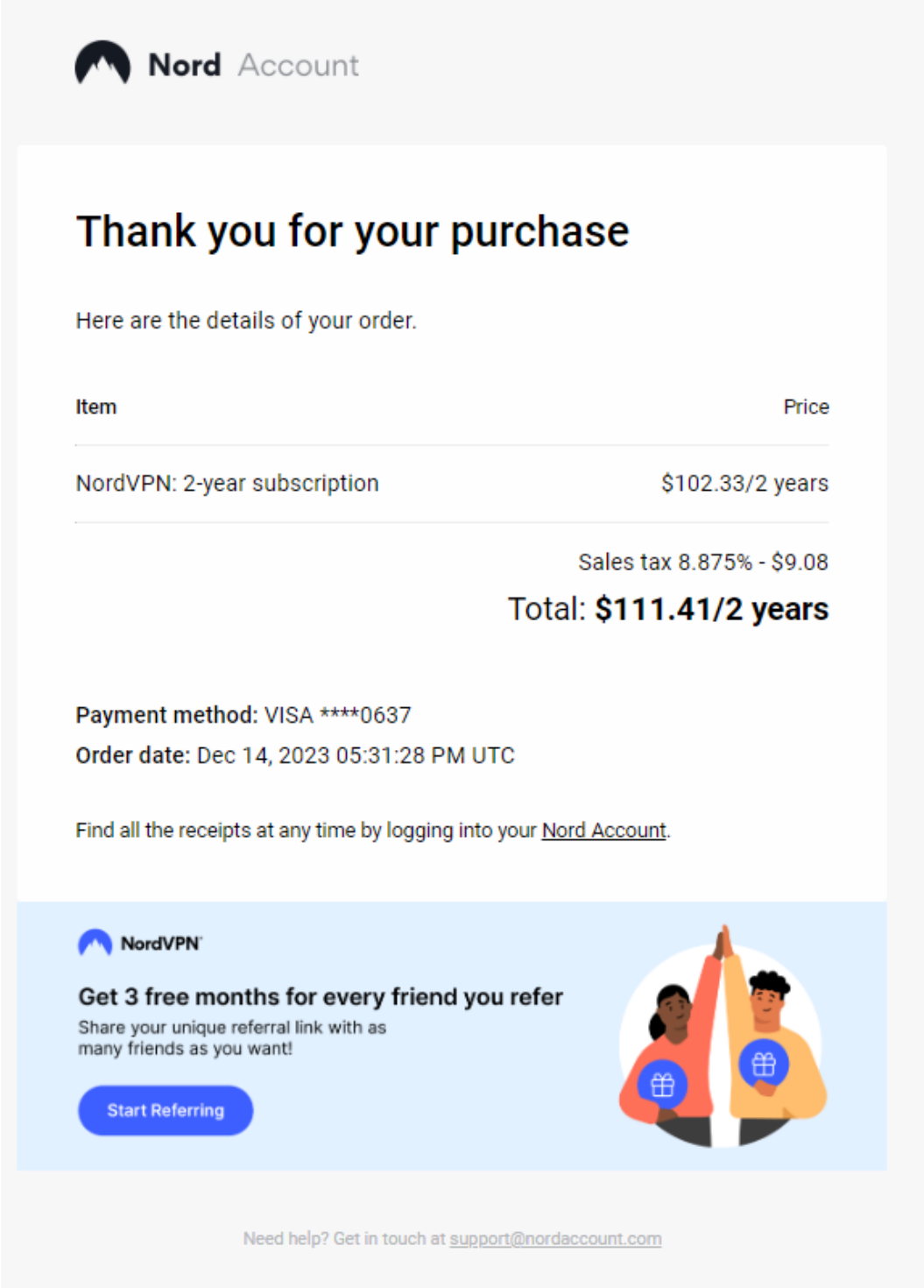
Earn 3 free months - refer your friends
Invite your friends to use NordVPN and get rewards.

Earn 3 Free Months

Get the app Need help?

PH F&F TOWER, 50th Street & 56th Street, Suite #32-D, Floor 32, Panama City, Republic of Panama

61. During the Class Period, after consumers enrolled, Nord Security also sent them an email containing the word "receipt" in the subject line. A representative version of the receipt email is shown on the following page:



Nord Account

Thank you for your purchase

Here are the details of your order.

Item	Price
NordVPN: 2-year subscription	$102.33/2 years

Sales tax 8.875% - $9.08

Total: **$111.41/2 years**

Payment method: VISA ****0637

Order date: Dec 14, 2023 05:31:28 PM UTC

Find all the receipts at any time by logging into your Nord Account.

NordVPN

Get 3 free months for every friend you refer

Share your unique referral link with as many friends as you want!

Start Referring

Need help? Get in touch at support@nordaccount.com

62. Neither Defendants' post-enrollment acknowledgement nor receipt emails meet the Illinois ARL's post purchase requirements. They do not provide "the automatic renewal offer

terms, cancellation policy, and information regarding how to cancel" for Nord Subscriptions, ILCS 601/10(a)(iii), nor disclose "how to cancel" the renewal "before the subscription or purchasing offer is fulfilled" for a Nord Subscription, *id.* § 601/10(a)(i). In fact, neither of these emails include any disclosure whatsoever about how to cancel a Nord Subscription.

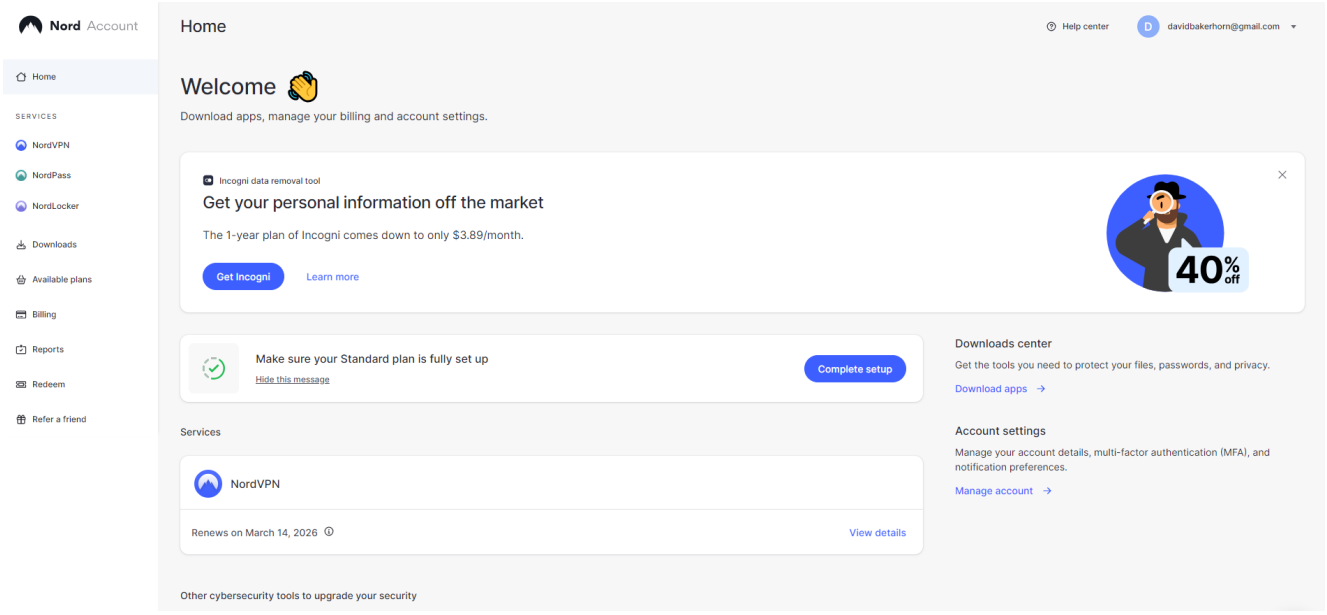
63. Moreover, neither Nord Security's acknowledgement nor receipt emails disclose "clearly and conspicuously" that the subscription will automatically renew unless the consumer cancels, *id.* § 601/5(1), § 601/10(a)(iii), the length of the renewal period, *id.* § 601/5(4), § 601/10(a)(iii), one or more "cost-effective, timely, and easy-to-use" mechanisms for cancellation, *id.* § 310/10(b-5), or a link that directs the consumer to Nord Security's cancellation process or another reasonable accessible electronic method that directs the consumer to the cancellation process, *id.*

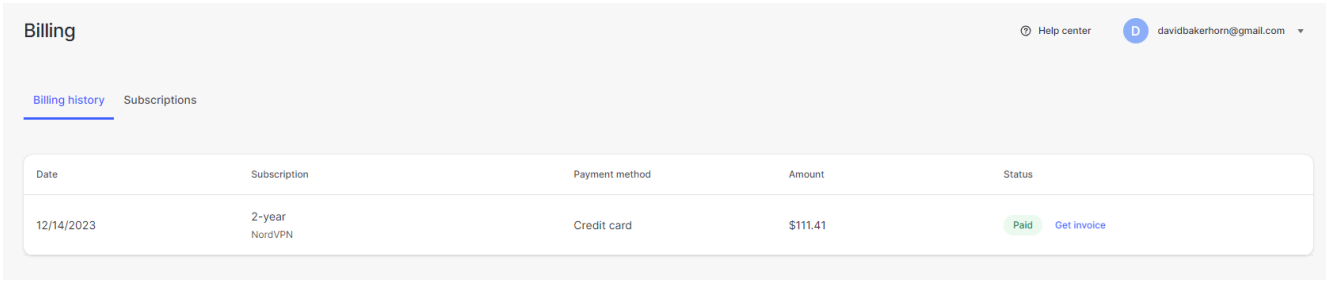
C. Nord Security's Cancellation Process Violates the Illinois ARL

64. Nord Security's cancellation process is not simple, cost-effective, timely, or easy-to-use. Nord Security also does not provide details about its subscription cancellation process that are capable of being retained by consumers. Instead, Nord Security employs the "roach motel" dark pattern strategy: it is easy to get into a Nord Subscription, but hard to get out.

65. 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 Subscription first requires consumers to (1) log into their customer account, and (2) select "Billing" from a list of at least nine options. Once "Billing" is selected, the default view on the "Billing" page does not mention anything about cancellation, and instead shows the consumer's "Billing history." Upon information and belief, Nord Security's "Home" and "Billing" pages

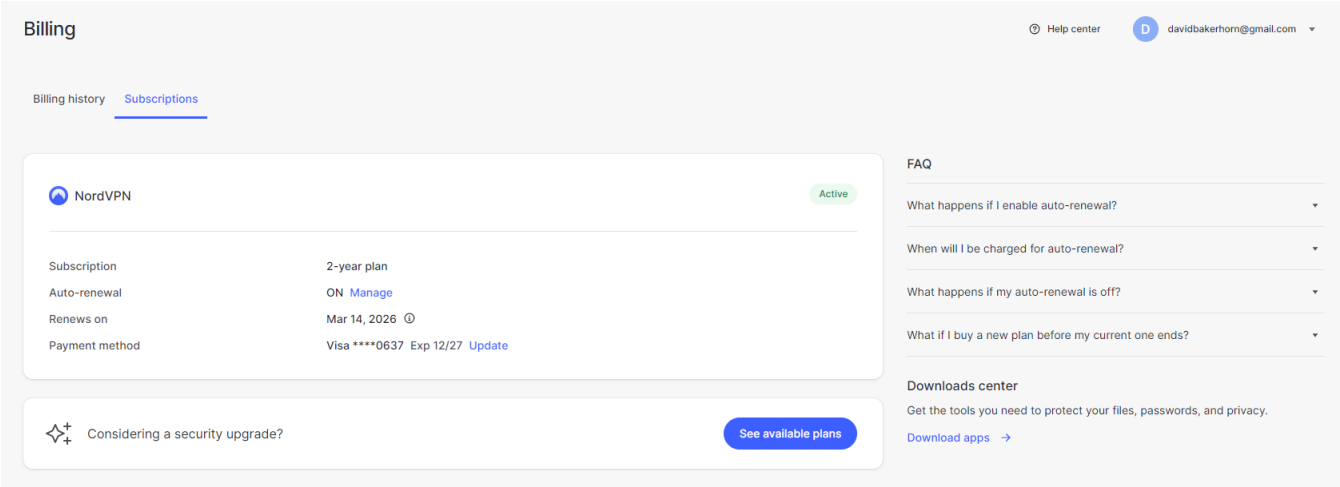
available to Plaintiff in approximately November 2020 was materially similar to Nord Security's current Home and Billing pages copied below:

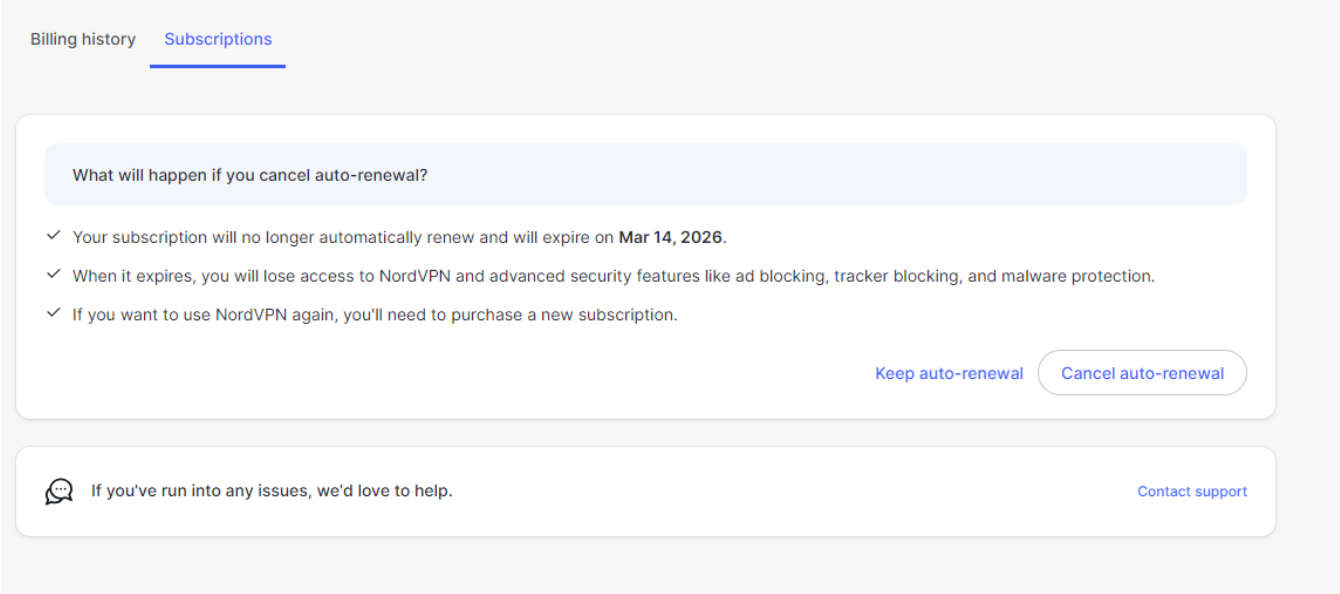




66. After navigating to Nord Security's "Billing page," consumers wishing to cancel must then (3) figure out how to navigate to the "Subscriptions" tab on the "Billing" page. Once customers access the "Subscriptions" tab, they are still not presented with a "Cancel" option. Instead, consumers must then (4) understand that they need to click on "Manage" on a line pertaining to "Auto-renewal" to finally access a page where they can cancel their account. Upon information and belief, Nord Security's "Subscriptions" tab available to Plaintiff in or around November 2020 was materially similar to the Nord Security "Subscriptions" tab as copied as the

first image below, as well as the page consumers view when they click "Manage" next to "Auto-renewal," in the second image below:





67. 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 Illinois ARL because it is not cost-effective, timely, or easy-to-use. 815 ILCS § 601/10(b-5). Nor does Nord

Security provide a toll-free telephone number or electronic mail address consumers may contact to cancel the automatic renewal, or a link to a website or other online service consumers can use to cancel. *Id.*

68. For those consumers who use Nord Security's mobile application, like Plaintiff, there is no way in which to cancel autorenewal. This too violates the Illinois ARL. *Id.* § 601/10(b-5).

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

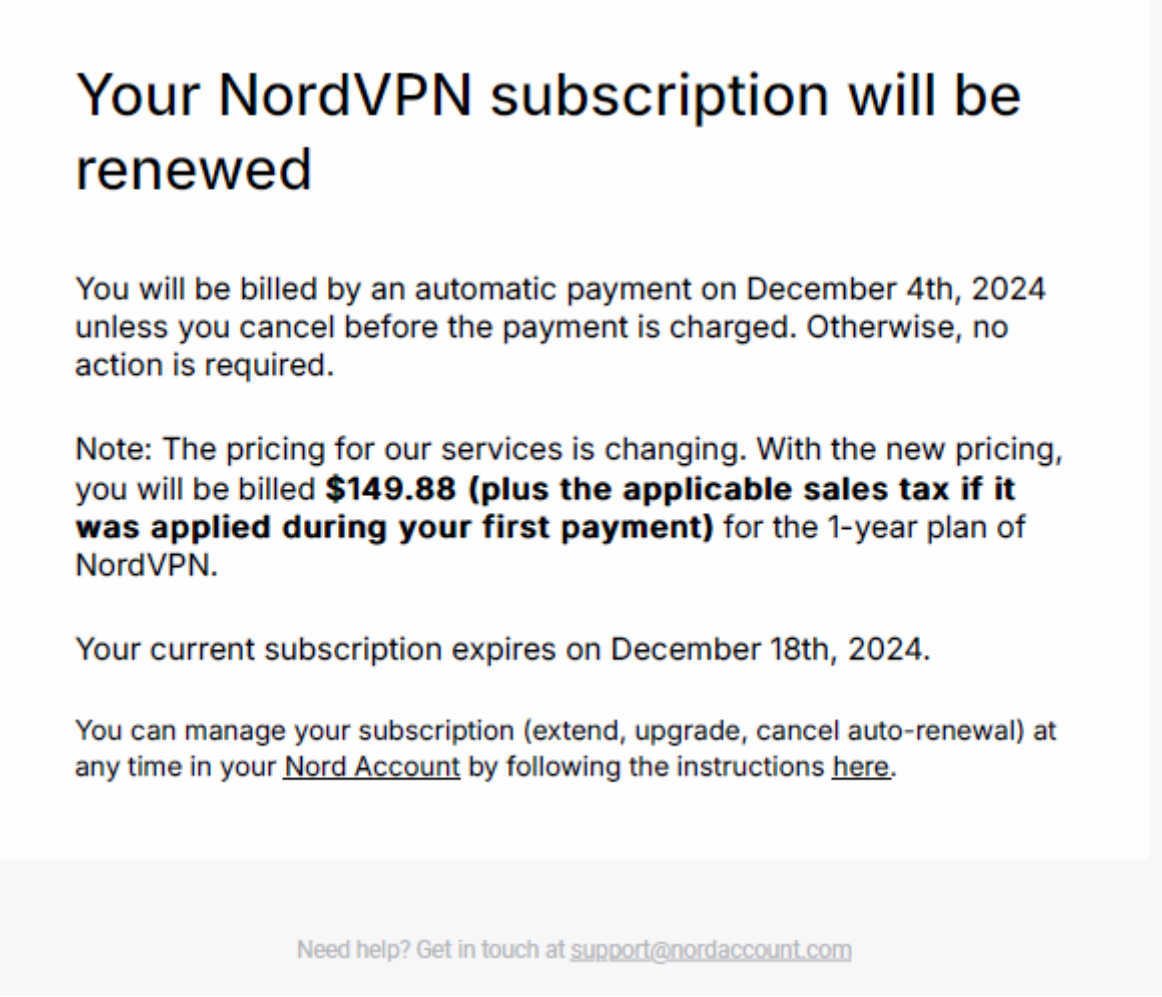
69. Nord Security offers subscriptions with an initial plan term of one year or longer that later automatically renew. For customers with such subscriptions, under the Illinois ARL Nord Security must provide notice of the upcoming automatic renewal "at least 30 days and not more than 60 days before the automatic renewal offer or continuous service offer renews." *Id.* § 601/10(b). The notice must "clearly and conspicuously" disclose: (1) that the subscription will automatically renew unless the consumer cancels; (2) a mechanism for cancelling the contract; and (3) the deadline by which the consumer must cancel to avoid being charged for a subsequent term. *Id*.

70. Prior to January 1, 2024, Nord Security was required under the Illinois ARL to provide notice of the upcoming automatic renewal "at least 30 days and not more than 60 days before the automatic renewal offer or continuous service offer renews." 815 ILCS § 601/10(b) (West 2004). That notice must "clearly and conspicuously" disclose: (1) that the subscription will automatically renew unless the consumer cancels; and (2) where the consumer could "obtain details of the automatic renewal provision and cancellation procedure (for example, by contacting the business at a specified telephone number or address or by referring to the contract)." *Id*.

71. On November 4, 2023, Nord Security charged Plaintiff Sasgen for an unwanted and unauthorized automatic renewal. On November 9, 2023, Nord Security sent Plaintiff Sasgen

an email with the subject line "Information regarding your subscription" wherein Nord Security admitted that Plaintiff Sasgen was "charged for the Nord subscription renewal without prior notice." This violated the Illinois ARL. 815 ILCS § 601/10(b) (West 2004).

72. Nord Security violated the Illinois ARL again the following year. On November 3, 2024, approximately one month before Nord Security charged Plaintiff Sasgen for an unwanted and unauthorized automatic renewal, Nord Security sent Plaintiff Sasgen an email with the subject line "Subscription renewal in 30 days." As described below, this email also violated the Illinois ARL. The email sent to Plaintiff is shown below:



Your NordVPN subscription will be renewed

You will be billed by an automatic payment on December 4th, 2024 unless you cancel before the payment is charged. Otherwise, no action is required.

Note: The pricing for our services is changing. With the new pricing, you will be billed **$149.88 (plus the applicable sales tax if it was applied during your first payment)** for the 1-year plan of NordVPN.

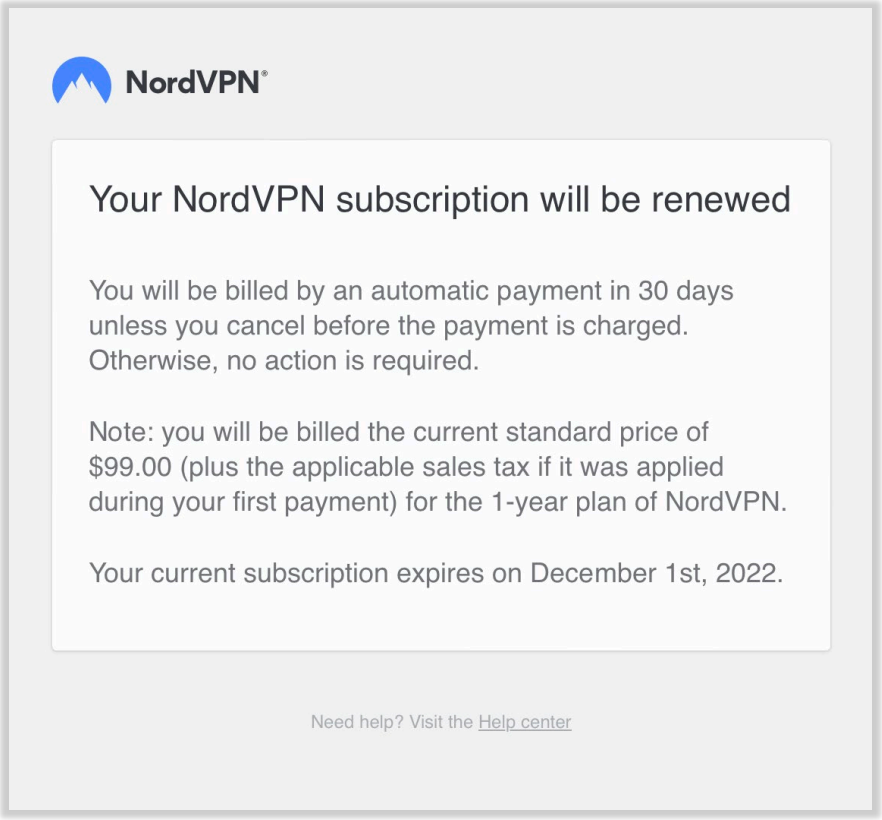
Your current subscription expires on December 18th, 2024.

You can manage your subscription (extend, upgrade, cancel auto-renewal) at any time in your Nord Account by following the instructions here.

Need help? Get in touch at support@nordaccount.com

73. 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. Although the email lists the date on which Plaintiff would purportedly be charged for a renewal (here, "December 4th"), Nord Security instead charged Plaintiff for an unwanted and unauthorized automatic renewal a day early, on December 3.

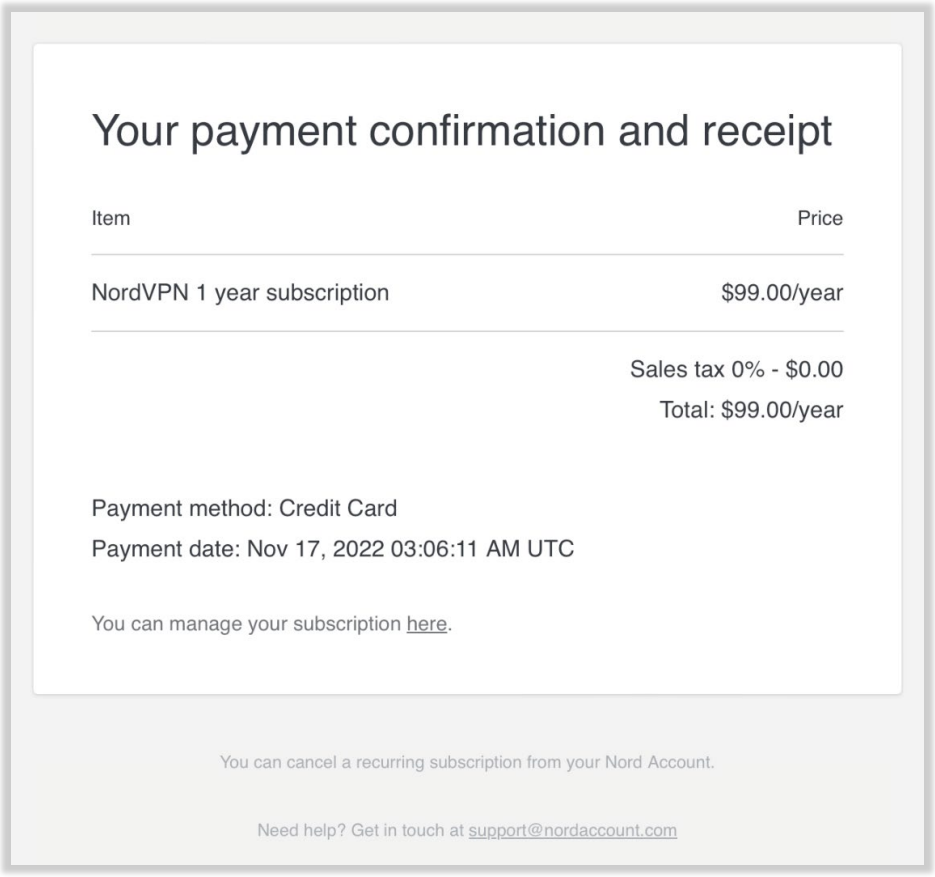
74. On information and belief, Nord Security revised its "notice" email some time in 2024 after being sued for automatic renewal violations in federal court in the Western District of North Carolina and Northern District of California. Prior to that change, Nord Security sent Class Members a different version of its "notice" email with the subject line "Subscription renewal in 30 days." A representative version of that email is shown below:



75. The prior version of Nord Security's email violates the Illinois ARL because it does not include "a mechanism for cancelling the contract." 815 ILCS § 601/10(b)(ii). The email simply states that the user must "cancel" to avoid a charge but provides no information whatsoever on how to do so, let alone one or more methods. 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."67F[69]

76. 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 receipt email also violates the ARL, it does arguably at least try to provide consumers with clues on how to cancel. For example, as shown below, the automatic renewal receipt email states in faint grey text 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 states (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 on the following page:

[69] https://support.nordvpn.com/hc/en-us.



Your payment confirmation and receipt

Item	Price
NordVPN 1 year subscription	$99.00/year

Sales tax 0% - $0.00

Total: $99.00/year

Payment method: Credit Card

Payment date: Nov 17, 2022 03:06:11 AM UTC

You can manage your subscription here.

You can cancel a recurring subscription from your Nord Account.

Need help? Get in touch at support@nordaccount.com

E. How Nord Security's Subscription Scheme Injured Plaintiff

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

78. On approximately November 18, 2020, Plaintiff enrolled in a three-year subscription to Nord Security's NordVPN product offering for $108.43.

79. After signing up for Nord Security's VPN service, Plaintiff downloaded the NordVPN mobile application.

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

81. 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 November 2020 because Nord Security did not adequately disclose to Plaintiff that it would begin charging non-refundable recurring annual fees that were ***more*** than his initial three-year subscription.

82. Nonetheless, on or about November 4, 2023 (less than three years after Plaintiff purchased the three-year plan) Nord Security charged Plaintiff's credit card $108.43 without his knowledge or permission for a one-year NordVPN subscription set to begin on or about November 18, 2023. Nord Security then emailed Plaintiff and admitted that it failed to notify him about the upcoming automatic renewal.

83. On or about December 10, 2024, Nord Security again charged Plaintiff's credit card $163.37 without his knowledge or permission for a one-year NordVPN subscription set to begin on or about December 17, 2024.

84. At some point after Nord Security made the first unauthorized charge to Plaintiff's credit card in December 2023, Plaintiff discovered that Nord Security had been repeatedly charging his credit card without his knowledge or permission.

85. Thereafter, Plaintiff searched for information on the internet about how to cancel the unauthorized subscription but was unable to do so.

86. At some point after second unauthorized renewal charge, Plaintiff was finally able to cancel autorenewal of his Nord Subscriptions.

87. Nord Security did not "clearly and conspicuously" disclose to Plaintiff that it would automatically renew his Nord Subscription for a one-year term after his initial three-year plan expired. 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.

88. Similarly, Nord Security did not "clearly and conspicuously" disclose to Plaintiff how he could cancel his Nord 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.

89. Nord Security failed to provide Plaintiff with the legally required notice of upcoming automatic renewal of his Nord Subscription. For the first automatic renewal, Nord Security admitted that it failed to provide any notice whatsoever. For the second automatic renewal, Nord Security's supposed "notice" email misleadingly stated the date and time it would process the automatic renewal charges.

90. Plaintiff did not authorize or want his Nord Subscription to renew once, let alone twice.

91. Plaintiff was injured when Nord Security charged his credit card $108.43 and $163.37, for a total of $271.80, for a Nord Subscription he did not want and did not want to pay for.

92. 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.

93. Plaintiff intends to purchase products and services in the future for himself from internet security companies, including Nord Security, as long as he can gain some confidence in Nord Security's representations about its products and services and subscription practices,

including autorenewal and cancellation. Moreover, Nord Security still has Plaintiff's payment information and could use it process unauthorized payments in the future.

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

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

RULE 9(B) ALLEGATIONS

96. 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:

97. **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 Illinois through a deceptive subscription scheme by making the material misrepresentations and omissions alleged in detail above in violation of Illinois consumer protection statutes and the common law, including with respect to automatic renewal and cancellation, leaving many consumers who sign up for a Nord Security product offering paying for subscriptions that they do not want.

98. **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 Subscriptions that they do not want.

- Nord Security conducts its deceptive subscription scheme by failing to meet the post purchase requirements that the Illinois ARL imposes on an automatically renewing product or service. During the Class period, Nord Security did not provide "an acknowledgment that includes the automatic renewal offer terms, cancellation policy, and information regarding how to cancel, which may be accomplished by linking to a resource that provides instructions that account for different platforms and services, in a manner that is capable of being retained by the consumer," 815 ILCS § 601/10(a)(iii). In fact, Nord Security's receipt email does not include any disclosure whatsoever about how to cancel a Nord 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 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 notify consumers of the "deadline by which the consumer must cancel to avoid being charged for a subsequent term," or a "a mechanism for cancelling the contract." 815 ILCS 601/10(b)(ii)–(iii).

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

100. 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 Subscription in November 2020, through Nord Security's acknowledgment and receipt emails sent to Plaintiff, Nord Security's "terms of service" and "terms" hyperlinks, and Plaintiff's unsuccessful attempts to cancel his account after learning that Nord Security had charged him for one or more unwanted automatic renewals sometime after November 2023 and December 2024. Nord Security uses the same or substantially similar deceptive and unlawful subscription practices scheme for all of its customers.

101. 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. As a direct result of this scheme, Defendants have successfully reaped tens of millions in unlawful charges at the expense of unsuspecting customers.

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

CLASS ACTION ALLEGATIONS

103. 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 Illinois (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").

104. 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.

105. 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.

106. 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.

107. 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.

108. 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.

109. 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.

110. 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.

111. 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 Illinois ARL;

b. Whether Defendants' conduct violates the applicable Illinois 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.

112. 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.

113. 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 Illinois ARL;

b. Whether Defendants' conduct violates the applicable Illinois 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; and

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

114. 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

ILLINOIS AUTOMATIC CONTRACT RENEWAL ACT, 815 ILCS 601/1 *et seq.*

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

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

117. The Illinois ARL requires that companies that sell or offer to sell any products or services to a consumer pursuant to a contract that automatically renews unless the consumer cancels the contract to disclose the automatic renewal offer terms clearly and conspicuously in the contract before the subscription or purchasing agreement is fulfilled and in visual proximity to the request for consent to the offer, and to not charge consumers for any payments in connection with such a contract without first obtaining the consumer's consent. 815 ILCS 601/10(a)(i)–(ii).

118. At the time Plaintiff enrolled in a Nord Subscription, the Illinois ARL required companies like Nord Security to "disclose the automatic renewal clause clearly and conspicuously in the contract, including the cancellation procedure." 815 ILCS 601(a) (West 2004).

119. Where products or services are sold on an automatically renewing basis under a specified contractual term of term of 12 months or more, companies like Nord Security must notify the consumer in writing of the automatic renewal. *See* 815 ILCS 601/10(b); *see also* 815 ILCS 601/10(b) (West 2004). Such written notice must be provided to the consumer no less than 30 days and no more than 60 days before the cancellation deadline pursuant to the automatic renewal offer terms. 815 ILCS 601/10(b); *see also* 815 ILCS 601/10(b) (West 2004). The notice must disclose clearly and conspicuously, in a retainable form, that unless the consumer cancels the contract it will automatically renew, a mechanism for cancelling the contract, which shall be offered in a manner in which the consumer commonly interacts with the business, and the deadline by which the consumer must cancel to avoid being charged for a subsequent term.815 ILCS 601/10(b).

120. The autorenewal notice provision in effect prior to January 1, 2024, required the autorenewal notice disclose clearly and conspicuously that unless the consumer cancels the contract it will automatically renew, and where the consumer can obtain details of the automatic renewal provision and cancellation procedure (for example, by contacting the business at a specified telephone number or address or by referring to the contract). 815 ILCS 601/10(b) (West 2004).

121. Beginning in 2022, the Illinois ARL required that any covered entity provide a toll-free telephone number, electronic mail address, a postal address if the seller directly bills the consumer, or another cost-effective, timely, and easy-to use mechanism for cancellation. 815 ILCS 601/10(b-5) (West 2021).

122. Nord Security violated the Illinois ARL as described in detail above, by:

a. Failing to clearly and conspicuously disclose the automatic renewal clause clearly and conspicuously in the contract;

b. During the Class Period, failing to obtain consumers' affirmative consent to the automatic renewal offer terms before charging consumers for Nord Subscriptions;

c. During the Class Period, failing to provide an acknowledgement that includes the automatic renewal offer terms, cancellation policy, and information regarding how to cancel;

d. Failing to provide a cost-effective, timely, and easy-to-use mechanism for cancellation; and

e. Failing to provide proper notice of future autorenewal payments as mandated by the Illinois ARL.

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

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

COUNT II

ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT

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

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

127. 815 ILCS § 505/1 *et seq.* (the "ICFA") prohibits "unfair methods of competition and unfair or deceptive acts or practices," including "any deception, fraud, false pretense, false promise, misrepresentation or the concealment, suppression, or omission of any material fact, with intent that others rely upon the concealment, suppression or omission of such material fact."

128. Nord Security committed unlawful practices under the ICFA because violations of the Illinois ARL constitute unlawful practices under the ICFA. 815 ILCS § 601/15.

129. Nord Security committed unfair and/or deceptive practices under the ICFA because it imposed charges without complying with all applicable requirements of 815 ILS § 601/1 *et seq.*, as alleged above.

130. The above unfair and deceptive practices and acts by Defendants were immoral, unethical, oppressive, and unscrupulous.

131. Defendants' actions were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff and the Illinois Class Members.

132. As a result of Defendants' unlawful, unfair, and deceptive business practices, Plaintiff and Class Members suffered monetary damages.

133. Plaintiff and the Illinois Class Members seek relief under 815 ILCS § 505/10a, including, but not limited to injunctive relief, damages, restitution, punitive damages and attorneys' fees and costs.

COUNT III

CONVERSION

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

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

136. 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.

137. 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.

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

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

140. 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.

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

COUNT IV

UNJUST ENRICHMENT

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

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

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

145. 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.

146. 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 V

MONEYS HAD AND RECEIVED

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 Class.

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

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

151. Defendants have not fully returned the moneys.

152. 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 Milberg Coleman Bryson Phillips Grossman, 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, costs, reasonable attorneys' fees, costs, and expenses; and

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

Dated: June 20, 2025

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC

/s/ Gary M. Klinger
Gary M. Klinger
227 W. Monroe St., Ste. 2100
Chicago, Illinois 60606
Tel: 866-252-0878
gklinger@milberg.com

WITTELS MCINTURFF PALIKOVIC
J. Burkett McInturff*
305 Broadway, 7th Floor
New York, New York 10007
Tel: (914) 775-8862
jbm@wittelslaw.com

* *Pro Hac Application Forthcoming*

Co-Counsel for Plaintiff and the Proposed Class