UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

JOHN DOE, individually and on behalf of all others similarly situated,

Plaintiff,

vs.

CURALEAF, INC.,

Defendant.

Case No. 1:25-cv-25202

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff John Doe,[1] individually and on behalf of all other persons similarly situated, by and through his attorneys, makes the following allegations pursuant to the investigation of his counsel and based upon information and belief, except as to allegations specifically pertaining to himself and his counsel, which are based on personal knowledge.

NATURE OF THE ACTION

1. This is a class action on behalf of all individuals who have purchased medical cannabis on www.curaleaf.com and whose protected health information has been exploited.

2. Defendant Curaleaf, Inc. ("Curaleaf" or "Defendant") owns and operates www.curaleaf.com, one of the largest online pharmacies for medical marijuana. Reporting $1.34 billion in sales for the year 2024, Curaleaf dispenses marijuana to Florida residents through a license obtained from the State of Florida designating it as a medical marijuana treatment center.

3. Numerous federal and state laws impose a legal obligation on Defendant to keep protect health information about marijuana usage and consumption—including details about marijuana treatments or prescriptions—strictly confidential. *See, e.g.*, 45 CFR § 164.508 (regulations pursuant to HIPAA prohibiting covered entities from "us[ing] or disclos[ing] protected health information without an authorization"); Fla. Stat. § 381.986(10)(f)(5) (prohibiting "medical marijuana treatment centers" from "disclosing personal and confidential information of the qualified patient"); Fla. Stat. § 817.568 (prohibiting individuals and entities from "fraudulently us[ing], or possess[ing] with intent to fraudulently use, personal identification information concerning another person"); Fla. Stat. § 817.568 (prohibiting individuals and entities from "intentionally or knowingly possess[ing] … the personal identification information of another person"—including the "medical records" of that person—"without authorization").

[1] After effectuating service, Plaintiff intends to file a motion to proceed pseudonymously.

4. In violation of these serious regulatory obligations, Defendant is involved in an illicit scheme whereby it has surreptitiously integrated code into its website that discloses protected health information to third-party marketers and data brokers—which, in turn, use that protected information to assist Defendant with marketing campaigns to its customers. Specifically, Defendant aids, employs, agrees with, and conspires with Google, Inc. ("Google"), SD Technologies, Inc., ("Sweed"), InRadio, Inc., ("AdPredictive"), and StackAdapt Inc., ("StackAdapt") to eavesdrop on and disclose electronic communications sent and received by Plaintiff and Class members, including communications that contain sensitive, protected, and confidential information relating to marijuana usage and consumption.

5. By assisting third parties with intercepting sensitive and confidential communications, Defendant violated state and federal anti-wiretapping laws—along with HIPAA and other state laws prohibiting a marijuana treatment center from disclosing such information.

6. Plaintiff brings this action for legal and equitable remedies resulting from these illicit actions. This illegal scheme—which exploits customers' protected health information to boost marketing effectiveness and enhance medical marijuana sales—must be put to an end.

PARTIES

7. Plaintiff John Doe is domiciled in Miami, Florida. On June 5, 2025, Plaintiff Doe visited curaleaf.com and purchased medicinal marijuana. While doing so, Plaintiff Doe visited webpages and clicked on buttons revealing the medicinal products that he intended to purchase. After adding his medication to his cart, Plaintiff Doe navigated to the checkout page and entered his full name, phone number, email address, home address, and billing address. At no point during the transaction was Plaintiff Doe put on notice of a terms of service or privacy policy. Although unaware at the time, Plaintiff Doe is informed and believes that Defendant assisted third parties—

including but not limited to Google, Sweed, AdPredictive, and StackAdapt—with intercepting his electronic communications while he was navigating www.curaleaf.com, including communications that contained protected health information and personally identifiable information. Given that Defendant was statutorily required to safeguard protected health information and personally identifiable information from disclosure, Plaintiff Doe reasonably expected that communications revealing such information would remain confidential.

8. Plaintiff made these online transactions from web browsers in Florida.

9. Curaleaf, Inc., is a Delaware company headquartered in Stamford, Connecticut.

JURISDICTION AND VENUE

10. This Court has subject-matter jurisdiction pursuant to 28 U.S.C. § 1331 because this action arises under the laws of the United States. This Court also has subject-matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this is a class action where the aggregate claims of all members of the proposed class are in excess of $5,000,000.00, exclusive of interest and costs, there are 100 members of the putative class, and Plaintiff, as well as most members of the proposed class, are citizens of different states than Defendant.

11. This Court has personal jurisdiction over Defendant because Defendant committed an intentional act, expressly aimed at Florida, causing harm that Defendant knew would likely be suffered in Florida. This Court also has personal jurisdiction over Defendant because Defendant sells medicinal products through its interactive website, curaleaf.com, and caused those products to be delivered or picked up at its brick-and-mortar stores throughout Florida.

12. Venue is proper pursuant to 28 U.S.C. § 1391 because Defendant resides in this judicial district.

FACTUAL BACKGROUND

A. The Wiretap Act and the Florida Security of Communications Act

13. "In 1968, Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968, which deals with wiretapping and other forms of electronic surveillance." *Scott v. United States*, 436 U.S. 128, 130 (1978). Known today as the Wiretap Act, the statute remains "the primary law protecting the security and privacy of business and personal communications." S. Rep. 99-541 at *3.

14. As originally enacted, the Wiretap Act only extended to surveillance techniques in which "the contents of a communication [could] be overheard and understood by the human ear." S. Rep. 99-5441, at *2. Put differently, Congress "specifically excluded the [electronic] transmission of data from protection against private and governmental interceptions." H.R. 99-647, at *22. Less than two decades later, technological advancements forced Congress to expand the Wiretap Act's ambit:

> In the intervening years, data transmission and computer systems have become a pervasive part of the business and home environments. … Some of these new services permit an individual to use a keyboard and telephone to transmit electronic messages and data and to receive interactive services featuring banking and other financial services, shopping, news, messages and education. Many of these services also record the nature of the transactions engaged in by the user. Thus, the new technologies represent both an explosion in communication opportunities as well as surveillance possibilities. *Id.*

15. In 1986, Congress sought to address these "dramatic changes in new computer and telecommunications technologies" by "amend[ing] title III of the Omnibus Crime Control Safe Streets Act of 1968—the Federal wiretap law—to protect against the unauthorized interception of electronic communications." S. Rep. 99-5441 at *1.

16. Today, the Wiretap Act provides that "any person who intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication … shall be punished … or shall be subject to suit." 18 U.S.C.

§ 2511. The term "electronic communication" broadly encompasses "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." 18 U.S.C. § 2510(12). That includes, for example, "computer-to-computer communications," like "the transmission of financial records or funds transfers from financial institutions, medical records between hospitals and/or physicians' offices, and the transmission of proprietary data among the various offices of a company." S. Rep. 99-541 at *3.

17. Contemporaneous with Congress enacting of the Wiretap Act, state legislatures enacted their own prohibitions against eavesdropping on communications. In 1969, for example, the Florida legislature enacted its own anti-wiretapping statute—the Florida Security of Communications Act ("FSCA")—to "safeguard the privacy of innocent persons." Fla. Stat. § 934.01(4). Like the Wiretap Act, the FSCA prohibits intercepting "electronic communications." *See, e.g.*, Fla. Stat. § 934.03(1)(a). The FSCA also prohibits "procur[ing] any other person" to effectuate such interceptions. *See, e.g.*, Fla. Stat. § 934.03(1)(a); 18 U.S.C. § 2511(1)(a) (same).

18. Though largely coextensive with the Wiretap Act, the FSCA is a two-party consent statute, meaning that "all of the parties to the communication" must provide "prior consent to such interception." *See* Fla. Stat. § 934.03(3)(d).

B. History of Medical Marijuana in Florida

19. Throughout the 1800s and early 1900s, cannabis was considered a "patent medicine" in the United States,[2] prescribed for ailments ranging from "gout" to "uninterrupted insanity."[3] During this time, "[d]rug use was largely a private matter, as was drug treatment," but

[2] *See* Holland, The Pot Book: A Complete Guide to Cannabis 1 (2010).
[3] *See* https://www.civilwarmed.org/tildens-extract/.

beginning in 1909, "the federal government became progressively more involved in the field as a series of important laws, court cases, and administrative decisions effectively criminalized nonmedical narcotic use and proscribed certain treatments."[4] By the 1930s, "the Federal Bureau of Narcotics pushed states to adopt the Uniform State Narcotic Drug Act and to enact their own measures to control marijuana distribution."[5] At the federal level, Congress enacted the Marijuana Tax Act in 1937, effectively prohibiting the cultivation and distribution of cannabis for medical and nonmedical use alike.[6] Three decades later, Congress formalized that prohibition through the Comprehensive Drug Abuse Prevention and Control Act, categorizing cannabis as a Schedule I narcotic and making its use and distribution a criminal offense.[7]

20. To this day, cannabis remains a Schedule I narcotic under federal law. But "[i]n 1996, California became the first state to amend its drug laws to allow for the medicinal use of marijuana."[8] Since then, "nearly all the states have changed their laws to permit the use of marijuana (or other cannabis products) for medical purposes."[9]

21. In November 2016, "Florida became the first state in the U.S. south to legalize the use of medical marijuana to treat a variety of health conditions including chronic pain, epilepsy, and spasticity symptoms from multiple sclerosis."[10] Under Florida law, physicians cannot issue a prescription for medical marijuana without diagnosing the patient "with at least one qualifying

[4] https://www.ncbi.nlm.nih.gov/books/NBK234755/
[5] https://www.cato.org/policy-analysis/effect-state-marijuana-legalizations-2021-update#history-state-level-marijuana-legalizations
[6] https://www.cato.org/policy-analysis/effect-state-marijuana-legalizations-2021-update#history-state-level-marijuana-legalizations
[7] https://www.cato.org/policy-analysis/effect-state-marijuana-legalizations-2021-update#history-state-level-marijuana-legalizations
[8] https://www.congress.gov/crs-product/R44782
[9] https://www.congress.gov/crs-product/LSB10655
[10] https://pmc.ncbi.nlm.nih.gov/articles/PMC6936729/

medical condition" and conducting "an in-person physical examination." *See* Fla. Stat. § 381.986(4)(a). Once issued, patients must then visit a licensed "medical marijuana treatment center" to fill their prescriptions. *See* Fla. Stat. § 381.986(8).

22. Florida law continues to prohibit possessing cannabis without a prescription.

C. Medical Marijuana Usage is Sensitive and Confidential Information

23. As evinced through numerous statutes and regulations, medical marijuana usage and treatment constitute sensitive and confidential information.

24. Curaleaf operates in Florida as a licensed medical marijuana treatment center:[11]

Figure 1

The approved medical marijuana treatment centers are:

Name	Phone	Email	Authorization Status	License Number
Ayr Cannabis Dispensary	833-254-4877	Info@LibertyHealthSciences.com	Dispensing Authorization	MMTC-2015-0002
Cookies Florida	n/a	CookiesFloridaCompliance@Cookiesre.com	Dispensing Authorization	MMTC-2019-0018
Curaleaf	877-303-0741	Info.FL@Curaleaf.com	Dispensing Authorization	MMTC-2015-0001

25. As statutorily described, medical marijuana treatment centers "cultivate, process, transport, and dispense marijuana for medical use," and they serve as the exclusive source for patients to lawfully fill a cannabis prescription. *See* Fla. Stat. § 381.986(8)(e).

26. Florida law prohibits "a medical marijuana treatment center" from "disclosing personal and confidential information of the qualified patient." *See* Fla. Stat. § 381.986(10)(f)(5). Moreover, the Florida Constitution imposes an affirmative duty on the Department of Health to "protect the confidentiality of all qualifying patients." *See* Fla. Const. Art. XI, § 3(4). As part of

[11] https://knowthefactsmmj.com/mmtc/

that duty, the Department of Health has promulgated regulations requiring "medical marijuana treatment centers" to demonstrate "[e]xperience with handling confidential information" and compliance with "[t]he Health Insurance Portability and Accountability," including "[a] HIPAA complaint computer network."[12]

27. "The Health Insurance Portability and Accountability Act (HIPAA) of 1996 establishes federal standards protecting sensitive health information from disclosure without patient's consent."[13] Not every person or corporation must meet the standards imposed by HIPAA; only "covered entities," as statutorily defined, need comply. *See* 45 C.F.R. § 160.103.

28. A "covered entity" includes "[a] health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter." *Id.*

- The term "health care provider" encompasses any "person or organization who furnishes, bills, or is paid for health care in the normal course of business," and the term "health care," in turn, broadly contemplates "care, services, or supplies related to the health of an individual," including "[s]ales or dispensing of a drug, device, equipment, or other item in accordance with a prescription." *Id.*
- The term "health information" means "any information, including genetic information, whether oral or recorded in any form or medium, that: (1) is created or received by a health care provider; and (2) [r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual."
- The term "transaction" means "the transmission of information between two parties to carry out financial or administrative activities related to health care," including "[h]ealth care claims or equivalent encounter information." *Id.*

29. As these regulatory definitions make clear, medical marijuana treatment centers—like, for example, Curaleaf—constitute "covered entities" that must comply with HIPAA.

30. HIPAA generally provides that "a covered entity may not use or disclose protected health information without an authorization valid under this section." *See* 45 CFR § 164.508.

---

[12] *Id.*

[13] https://www.cdc.gov/phlp/php/resources/health-insurance-portability-and-accountability-act-of-1996-hipaa.html

31. A "disclosure" means "the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information." 45 CFR § 160.103.

32. The term "protected health information" means "individually identifiable health information," *see* 45 CFR § 160.103, and the term "individually identifiable health information," in turn, has a wordy—though important—definition: "[I]nformation that is a subset of health information, including demographic information collected from an individual, and:

a. Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

b. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

i. That identifies an individual; or

ii. With respect to which there is a reasonable basis to believe the information can be used to identify the individual." *See* 45 CFR 160.103(2).

33. To receive proper authorization from patients to use or disclose protected health information, covered entities must create an extensive and comprehensive form that "may not be combined with any other document to create a compound authorization." *See* 45 CFR § 164.508.

34. In a prescient bulletin entitled "Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates," the Department of Health and Human Services explained that "protected health information" includes "an individual's IP address, medical record number, home or email address, dates of appointments, or other identifying information that the individual may provide when interacting with the webpage."[14] As HHS further noted, "[t]he

[14] https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html#ftn8

HIPAA Rules apply when the information that regulated entities collect through tracking technologies or disclose to tracking technology vendors includes protected health information."[15]

35. The industry standard is to treat information concerning medical cannabis treatment and usage as confidential and protected by HIPAA. In Florida and elsewhere, companies recognize precisely as much and assuage consumers that such information is confidential.

- "[M]edical marijuana treatment centers are only permitted to disclose patient information to the patient or their designated caregiver, or as necessary to protect the patient's medical marijuana orders."[16]
- "In Florida, the confidentiality of medical marijuana cardholders is a serious matter, protected under both federal law and state statutes."[17]
- "In the US, medical cannabis confidentiality is protected under the Health Insurance Portability and Accountability Act (HIPAA)."[18]
- "Doctors specializing in medical cannabis cannot release any information without the patient's explicit written consent."[19]
- "Yes, medical marijuana patient privacy is protected under HIPAA."[20]
- "Like any medical records, patients expect their medial marijuana records to remain private to secure their personal information and medical history."[21]
- "HIPAA regulations apply to medical marijuana records, and additional legislation has been put into place to protect the privacy of medical marijuana patients."[22]

36. Put together, like every other health organization, federal and state laws require medical marijuana treatments centers to keep information about patients and treatments confidential. As a corollary, Plaintiff reasonably expected that his electronic communications with Defendant would remain confidential. Despite that reasonable expectation, Defendant systematically discloses such information to numerous third parties.

---

[15] *Id.*
[16] https://flmmd.com/docs/is-my-information-public-or-shared-with-anyone/
[17] https://www.arcannabisclinic.com/post/does-a-medical-marijuana-card-show-up-on-a-background-check-florida
[18] https://docmj.com/medical-marijuana-recommendations-confidential/
[19] https://www.chwmedicalmarijuana.com/medical-marijuana/mmj-privacy/
[20] https://www.veriheal.com/blog/protecting-your-privacy-hipaa-and-medical-cannabis/
[21] https://www.cannamd.com/are-my-medical-marijuana-records-private/
[22] https://www.cannamd.com/are-my-medical-marijuana-records-private/

D. Defendant's Unauthorized Disclosures of Protected Information to Google

37. Google is the largest online advertising company on the planet.[23]

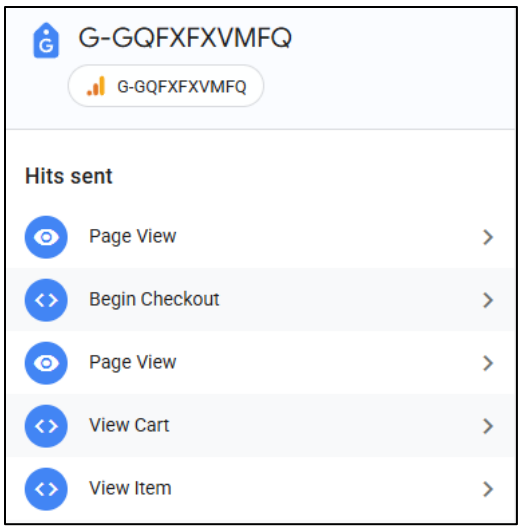
38. Defendant knowingly integrated code from Google into its website to use services—including but not limited to Google Analytics and Google Ads—to augment its advertising and analytics efforts by capturing the content of patients' electronic communications and linking those communications to patients' personally identifiable information.

39. When consumers access and navigate curaleaf.com, the Google software script that Defendant embedded on its website surreptitiously directs the user's browser to send a separate message to Google's servers. This second, secret transmission contains the original GET request sent to the host website along with additional data that Google's code is configured to collect. This transmission is initiated by Google's code and concurrent with communications with the host website. Two sets of code are thus automatically run as part of the browser's attempt to load and run Defendant's website—Defendant's own code, and Google's embedded code.

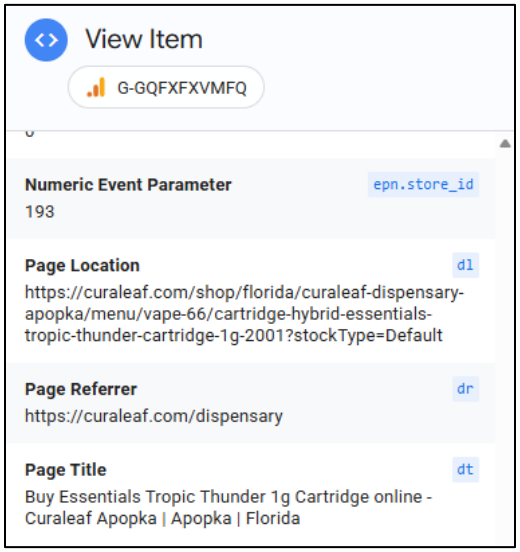
40. As evinced through network traffic, Defendant assists Google with intercepting the content of electronic communications that reveal protected health information, including: 1) full-string URLs; 2) information revealing the text of buttons that patients clicked; and 3) information revealing medicinal products that patients browsed, added to their cart, or purchased.

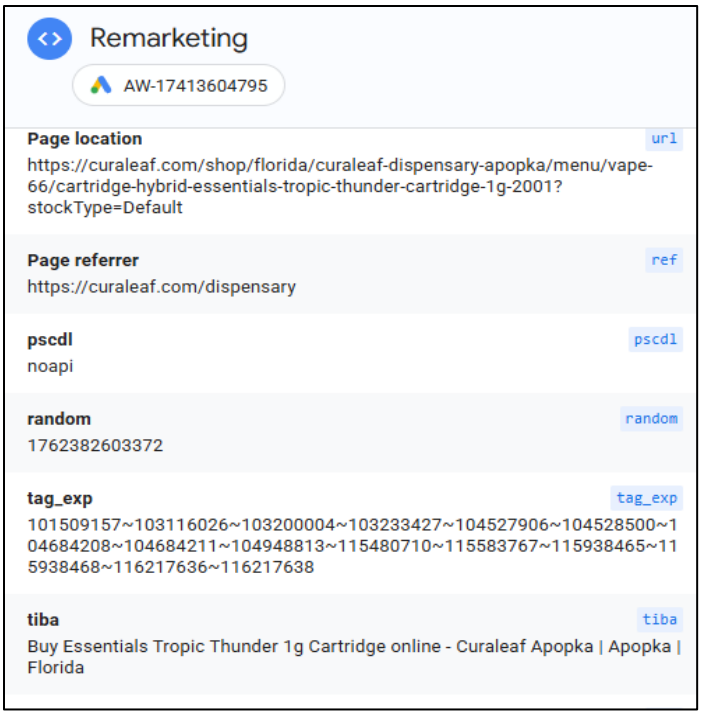
[23] https://www.emarketer.com/topics/category/google

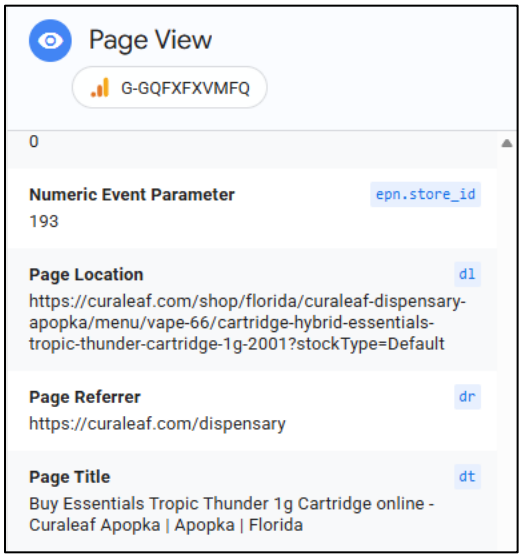
Figures 2–7

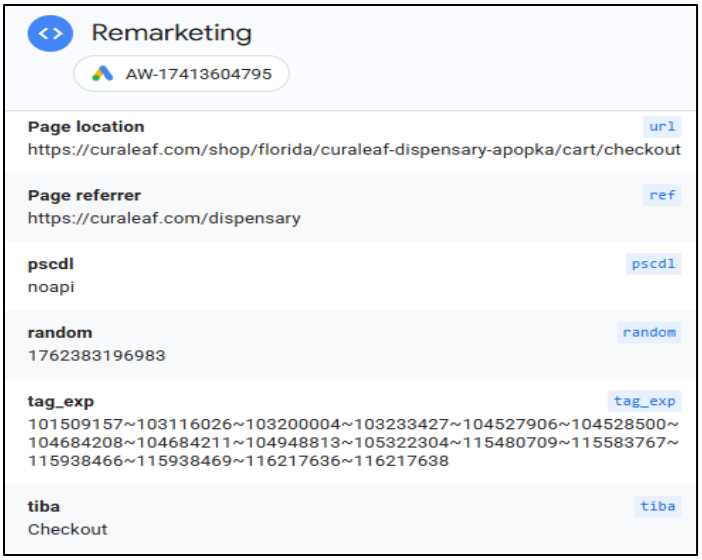

G-GQFXFXVMFQ
G-GQFXFXVMFQ
Hits sent
Page View
Begin Checkout
Page View
View Cart
View Item


AW-17413604795
AW-17413604795
Hits sent
Remarketing


View Item
G-GQFXFXVMFQ
Numeric Event Parameter
epn.store_id
193
Page Location
dl
https://curaleaf.com/shop/florida/curaleaf-dispensary-apopka/menu/vape-66/cartridge-hybrid-essentials-tropic-thunder-cartridge-1g-2001?stockType=Default
Page Referrer
dr
https://curaleaf.com/dispensary
Page Title
dt
Buy Essentials Tropic Thunder 1g Cartridge online - Curaleaf Apopka | Apopka | Florida

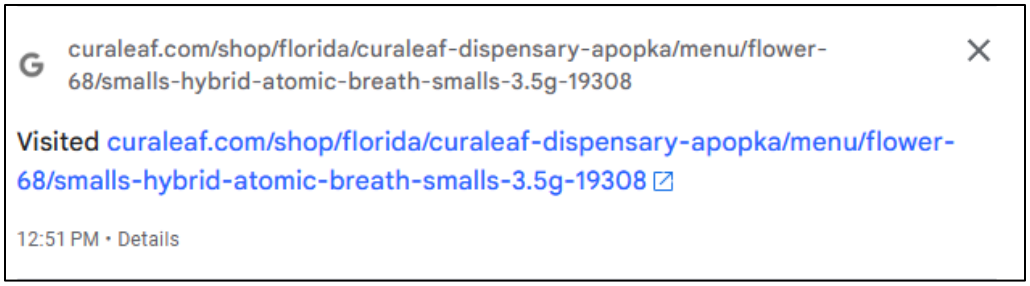

Remarketing
AW-17413604795
Page location
url
https://curaleaf.com/shop/florida/curaleaf-dispensary-apopka/menu/vape-66/cartridge-hybrid-essentials-tropic-thunder-cartridge-1g-2001?stockType=Default
Page referrer
ref
https://curaleaf.com/dispensary
pscdl
pscdl
noapi
random
random
1762382603372
tag_exp
tag_exp
101509157~103116026~103200004~103233427~104527906~104528500~104684208~104684211~104948813~115480710~115583767~115938465~115938468~116217636~116217638
tiba
tiba
Buy Essentials Tropic Thunder 1g Cartridge online - Curaleaf Apopka | Apopka | Florida


Page View
G-GQFXFXVMFQ
0
Numeric Event Parameter
epn.store_id
193
Page Location
dl
https://curaleaf.com/shop/florida/curaleaf-dispensary-apopka/menu/vape-66/cartridge-hybrid-essentials-tropic-thunder-cartridge-1g-2001?stockType=Default
Page Referrer
dr
https://curaleaf.com/dispensary
Page Title
dt
Buy Essentials Tropic Thunder 1g Cartridge online - Curaleaf Apopka | Apopka | Florida


Remarketing
AW-17413604795
Page location
url
https://curaleaf.com/shop/florida/curaleaf-dispensary-apopka/cart/checkout
Page referrer
ref
https://curaleaf.com/dispensary
pscdl
pscdl
noapi
random
random
1762383196983
tag_exp
tag_exp
101509157~103116026~103200004~103233427~104527906~104528500~104684208~104684211~104948813~105322304~115480709~115583767~115938466~115938469~116217636~116217638
tiba
tiba
Checkout

41. Google pairs those electronic communications with personally identifiable information, including direct identifiers that link to Google accounts.

Figure 8



42. As the owner and operator of the website, Defendant intended for Google to receive consumers' electronic communications and personally identifiable information. Defendant also knew that Google would then use those communications for its own commercial purposes. Indeed, companies using Google Analytics and Google Ads must agree to allow Google to "retain and use … information collected."[24]

43. Plaintiff and Class members never consented to Google intercepting the contents of their electronic communications, including those that contained their protected health information and personally identifiable information.

E. Defendant's Unauthorized Disclosures of Protected Information to Sweed

44. Sweed is a cloud-based software-as-a-service platform for cannabis retail management. Sweed offers the self-described "best technology platform in cannabis," enabling "all-in-one operations" through its "eCommerce platform,"[25] "marketing and rewards platform,"[26] and "business intelligence tools."[27]

[24] https://marketingplatform.google.com/about/analytics/terms/us-20210331/
[25] https://www.sweedpos.com/products/ecommerce
[26] https://www.sweedpos.com/
[27] https://www.sweedpos.com/products/business-intelligence

45. Through its eCommerce platform, Sweed "connects every channel with unified order management, marketing tools, and customer insights to drive engagement."[28] To link information from "online and in-person experiences," Sweed creates "universal customer profiles" that "personalize recommendations, track purchase history, and enhance loyalty with targeted marketing and rewards."[29] Through these profiles, dispensaries receive "deep insights into customer behavior, enabling personalized experiences and stronger engagement."[30]

46. For its marketing and loyalty platform, Sweed provides "advanced segmentation tools" that "group customers by behavior, preferences, and purchase history to maximize engagement."[31] To do that, Sweed "create[s] targeted lists … based on real customer activity, from product preferences to spending habits."[32] These lists "automatically update … in real time," ensuring that marketing materials are "fresh, relevant, and timely."[33]

47. Through its business intelligence tools, Sweed provides "personalized dashboards with real-time data and visualizations,"[34] thereby creating "real-time insights" and enabling dispensaries to "[a]nalyze revenue, profit margins, and transaction trends."[35]

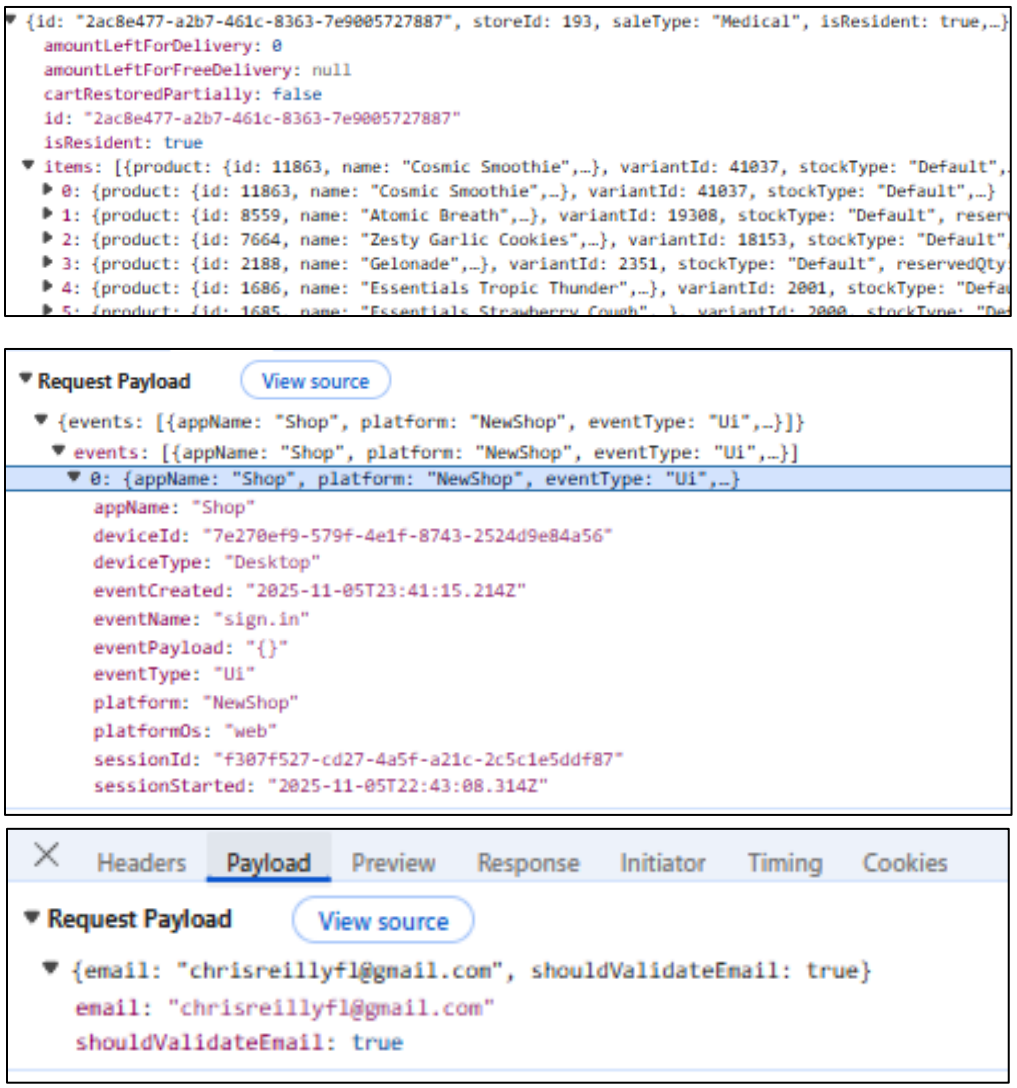
48. To augment its marketing and analytics efforts, Defendant knowingly integrates server-side code from Sweed to help intercept electronic communications and personally identifiable information. Unlike client-side tracking, server-to-server tracking operates akin to an

[28] https://www.sweedpos.com/products/ecommerce
[29] https://www.sweedpos.com/products/ecommerce
[30] https://www.sweedpos.com/products/ecommerce/universal-customer-profiles
[31] https://www.sweedpos.com/products/marketing-loyalty/advanced-segmentation
[32] https://www.sweedpos.com/products/marketing-loyalty/advanced-segmentation
[33] *Id.*
[34] https://www.sweedpos.com/products/business-intelligence
[35] https://www.sweedpos.com/products/business-intelligence/advanced-reports

automatic routing device, allowing Defendant to directly forward electronic communications and personally identifiable information to Sweed's servers as consumers navigate its website.

49. As evinced through network traffic, Defendant assists Sweed with intercepting the contents of electronic communications that reveal protected health information, including: 1) form-field entries; 2) full-string URLs; 3) information revealing the text of buttons clicked; and 4) information revealing medicinal products that patients browsed, added to their cart, or purchased.

Figures 9–11



50. Sweed pairs these electronic communications with personally identifiable information, including: 1) email addresses; 2) phone numbers; 3) first name; 4) last name; 5) IP address; 6) and other unique identifiers.

51. As the owner and operator of the website, Defendant intended for Sweed to receive consumers' electronic communications and personally identifiable information. Defendant also knew that Sweed would use those communications for its own commercial purposes. As an example, Sweed helps Defendant target patients through "AI and machine learning" systems that Sweed has built in-house. Indeed, Sweed boasts that these systems are "built natively into our platform," and they embody "the core of what we do."[36] As a general concept, "artificial intelligence refers to the general ability of computers to emulate human thought and perform tasks in real-world environments, while machine learning refers to the technologies and algorithms to identify patterns, make decisions, and improve themselves through experience and data."[37] To function effectively, "machine learning needs data from diverse sources, in diverse formats, about diverse business processes."[38] Moreover, "[a] distinct advantage of machine learning is its ability to improve as it processes more data."[39] In other words, Defendant knows that Sweed relies on using and analyzing patient records to train and improve its AI and machine learning systems.

52. Plaintiff and Class members never consented to Sweed intercepting the contents of their electronic communications, including those that contained their protected health information and personally identifiable information.

---

[36] https://www.sweedpos.com/resources/help-updates/blog/how-sweed-customers-are-already-winning-with-ai
[37] https://ai.engineering.columbia.edu/ai-vs-machine-learning/
[38] https://www.forbes.com/sites/joemckendrick/2021/06/27/the-data-paradox-artificial-intelligence-needs-data-data-needs-ai/
[39] https://aws.amazon.com/what-is/machine-learning/

F. Defendant's Unauthorized Disclosures of Protected Information to AdPredictive

53. AdPredictive offers "data-driven customer intelligence"[40] and "personalized marketing" services.[41] As AdPredictive explains, "[p]ersonalized marketing often referred to an one-to-one or individual marketing, is a strategy that involves tailoring marketing efforts and messages to specific individuals or segments."[42] By doing so, AdPredictive gains insights into "unique behaviors, characteristics, and preferences" that can help drive revenue. After receiving those insights, AdPredictive allows companies to "[t]arget customers with precisions audiences – manually entered or automatically generated by [its] strategic algorithms."[43]

54. Defendant knowingly integrates code from AdPredictive to augment its advertising and analytics efforts by capturing the content of electronic communications and linking those communications to personally identifiable information.

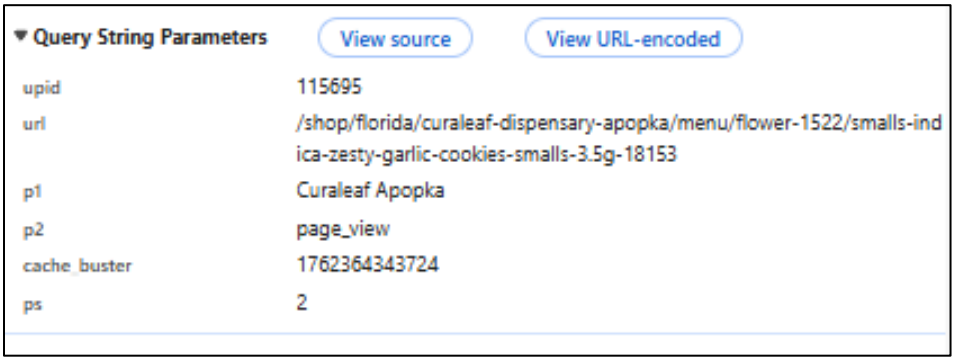
55. When consumers access and navigate curaleaf.com, AdPredictive's software script surreptitiously directs the user's browser to send a separate message to AdPredictive's servers. This second, secret transmission contains the original GET request sent to the host website along with additional data that AdPredictive's code is configured to collect. This transmission is initiated by AdPredictive's code and concurrent with the communications with the host website. Two sets of code are thus run as part of the browser's attempt to load and run Defendant's website—Defendant's own code, and AdPredictive's embedded code.

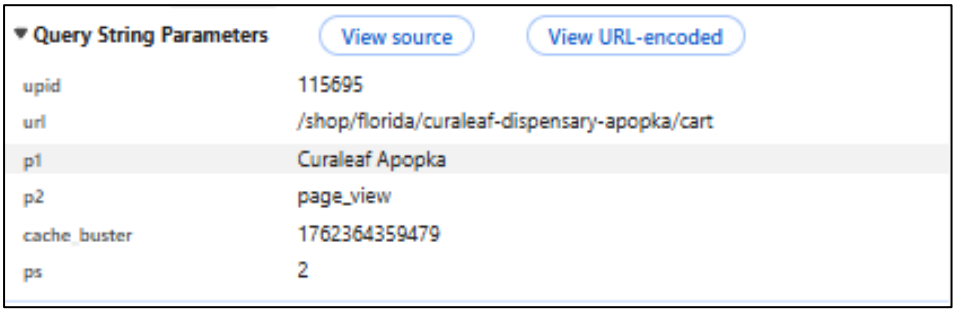
56. As evinced through network traffic, Defendant assists AdPredictive with intercepting the contents of electronic communications that reveal protected health information,

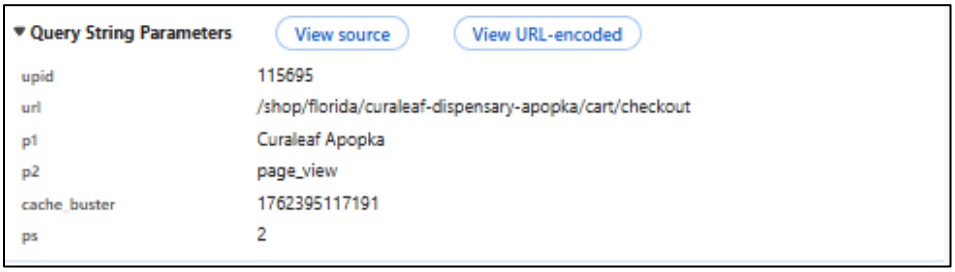
[40] https://adpredictive.com/announcements/adpredictive-announces-support-for-aws-for-advertising-marketing-initiative/
[41] https://adpredictive.com/data/personalized-marketing-adapting-in-the-cookieless-era/
[42] https://adpredictive.com/data/personalized-marketing-adapting-in-the-cookieless-era/
[43] https://web.archive.org/web/20220119113224/https://adpredictive.com/product/

including: 1) full-string URLs; 2) information revealing the text of buttons clicked; and 3) information revealing medicinal products that patients browsed, added to their cart, or purchased.

Figures 12–14







57. AdPredictive pairs these intercepted communications with personally identifiable information, including "email addresses, MAIDs [mobile advertising IDs] and IP addresses."[44] Indeed, companies are contractually obligated to "make available to AdPredictive … first-party IDs (e.g., mobile IDs, IP addresses, email addresses) to be used for matching to AdPredictive's ID graph," thereby allowing AdPredictive to "create a meta-leave customer profile visualization based

[44] https://web.archive.org/web/20210619003416/https://adpredictive.com/solutions/cookieless-data-driven-strategies/

on the matched profiles with data attributes about demographic, behavioral, purchase habits, and media consumption."[45]

58. As the owner and operator of the website, Defendant intended for AdPredictive to intercept consumers' electronic communications and personally identifiable information. Defendant also knew that AdPredictive would use those communications and personally identifiable information for its own commercial purposes. Indeed, companies must contractually grant AdPredictive with a license "to copy, reproduce, repurpose, and externally match any Client Data that is provided by Client to AdPredictive in any format, solely for performances of the Services," including but not limited to: "target advertising based on historical engagement; use of data to perform machine learning or to apply machine learning algorithms including without limitation lookalike modeling; use of data for purposes of segmenting, re-targeting, creating or supplementing user profiles or inventory profiles; passing anonymized IDs to one or more third parties for placement and/or targeting research or otherwise associating a cookie."[46]

59. Plaintiff and Class members never consented to AdPredictive intercepting the contents of their electronic communications, including those that contained their protected health information and personally identifiable information.

---

[45] AdPredictive claims to anonymize these identifiers by utilizing a "data clean room," but as the FTC has explained, such services "often default to allow both parties full access to all of the data," meaning they effectively serve as an obtuse vehicle "to combine and analyze data from different companies and export a subset of records or a derivative analysis of that data."[45] Put differently, data clean rooms merely "obfuscate privacy harms," and "[c]ompanies shouldn't view DCRs as a way to get around their obligations under the law." *See* https://s3.amazonaws.com/EULA/Master+Services+Agreement_AdPredictive+360+Customer+Vizualization_AWS_Updated+01.19.2023.pdf.

[46] https://s3.amazonaws.com/EULA/Master+Services+Agreement_AdPredictive+360+Customer+Vizualization_AWS_Updated+01.19.2023.pdf

G. Defendant's Unauthorized Disclosures of Protected Information to StackAdapt

60. StackAdapt is a "programmatic advertising platform."[47] As StackAdapt explains, "[p]rogrammatic advertising uses advertising technology and machine learning to buy, sell, and optimize digital ad placements."[48] More specifically, "[u]nlike traditional advertising, which relies on manual negotiations and insertion orders, programmatic advertising uses automated technology to identify, bid on, and deliver ads across multiple advertising channels and devices based on real-time user data, browsing behaviour, and targeting criteria."[49]

61. Defendant intentionally integrates code from StackAdapt into its website to augment its advertising and analytics efforts by capturing the content of electronic communications and linking those communications to personally identifiable information.

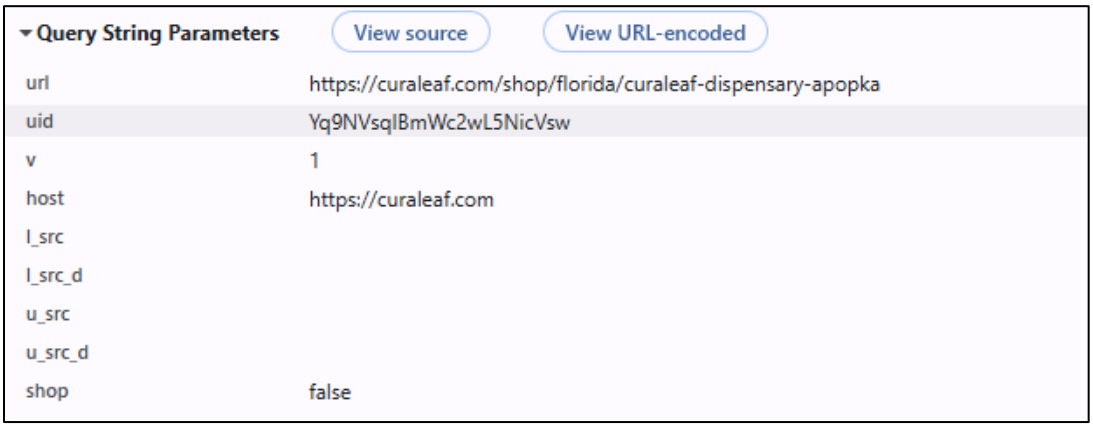
62. When consumers access and navigate curaleaf.com, StackAdapt's software script surreptitiously directs the user's browser to send a separate message to StackAdapt's servers. This second, secret transmission contains the original GET request sent to the host website along with additional data that StackAdapt's code is configured to collect. This transmission is initiated by StackAdapt's code and concurrent with the communications with the host website. Two sets of code are thus run as part of the browser's attempt to load and run Defendant's website—Defendant's own code, and StackAdapt's embedded code.

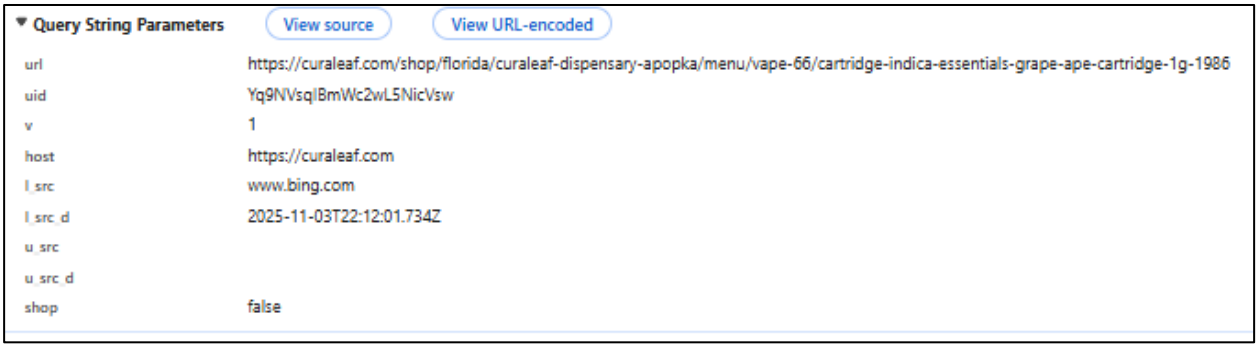
63. As evinced through network traffic, Defendant assists StackAdapt with intercepting the contents of electronic communications that reveal protected health information, including: 1)

[47] https://www.businesswire.com/news/home/20250506598881/en/StackAdapt-Launches-Integrated-Email-and-Data-Hub-Bridging-Martech-and-Programmatic-Advertising-Under-One-Platform
[48] https://www.stackadapt.com/resources/blog/what-is-programmatic-advertising
[49] *Id.*

full-string URLs; 2) information revealing the text of buttons clicked; and 3) information revealing medicinal products that patients browsed, added to their cart, or purchased.

Figures 15–16



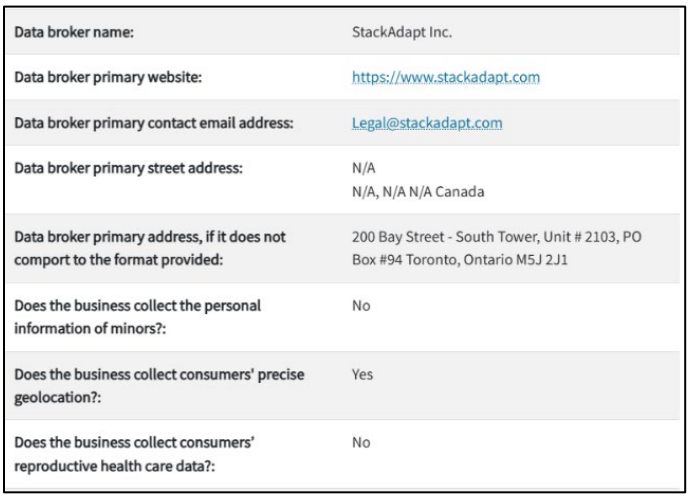


64. As the owner and operator of the website, Defendant intended for StackAdapt to intercept consumers' electronic communications and personally identifiable information. Defendant also knew that StackAdapt would use those communications for its own commercial purposes. Indeed, companies must grant StackAdapt "a non-exclusive, worldwide, perpetual, irrevocable, royalty-free license and right to access, collect (including from Client Sites), and use Client Data."[50] Moreover, companies must also agree that "StackAdapt may collect, analyze, use and process Client Data for the purposes of enhancing, improving, optimizing, analyzing the performance of, and further developing the Services, including its machine learning models."[51]

[50] https://www.stackadapt.com/legal-document-centre/terms-of-use
[51] *Id.*

65. StackAdapt is a registered data broker in California:

Figure 17



Data broker name:	StackAdapt Inc.
Data broker primary website:	https://www.stackadapt.com
Data broker primary contact email address:	Legal@stackadapt.com
Data broker primary street address:	N/A N/A, N/A N/A Canada
Data broker primary address, if it does not comport to the format provided:	200 Bay Street - South Tower, Unit # 2103, PO Box #94 Toronto, Ontario M5J 2J1
Does the business collect the personal information of minors?:	No
Does the business collect consumers' precise geolocation?:	Yes
Does the business collect consumers' reproductive health care data?:	No

66. Plaintiff and Class members never consented to StackAdapt intercepting the contents of their electronic communications, including those that contained their protected health information and personally identifiable information.

H. Defendant's Conduct Caused Economic Injury

67. Plaintiff's and Class members' online activity—including the browsing history and purchase history generated by navigating Defendant's website—has financial value. As a leading expert in data privacy, Professor Paul Schwartz at UC Berkeley, explained in an article published by the Harvard Law Review:

> Personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from the trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information.[52]

68. Numerous studies support Professor Schwartz's conclusion. In one such study, for example, researchers studied the value that 180 consumers placed on keeping personal data secure.

[52] Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2056 (2005)

As relevant here, consumers valued contact information at approximately $4.20 per year; they valued their online purchase history at $5.70 per year; and they valued their browsing history at $52 per year.[53]

69. Moreover, numerous companies offer products through which consumers can receive payment in exchange for a license to track their data. Meta Platforms, Inc., for example, ran a "Facebook Research" app in 2019 through which it paid $20 for a license to collect browsing history and other communications from consumers between the ages of 13 and 35.[54]

70. There also exists an illicit marketplace for protected health records. Indeed, "[h]ealth records are highly coveted on the black market due to the wealth of personal information they contain," selling anywhere from $60 to "upwards of $1,000."[55] "Beyond illicit markets, health data [also] holds substantial economic value for legitimate organizations."[56]

71. Defendant's conduct caused numerous third parties—including Google, Sweed, AdPredictive and StackAdapt—to profit from Plaintiff's and Class members' personal information and their activity on Defendant's website. Directly and indirectly, for example, Defendant paid these third parties to collect and analyze that information so Defendant could better target advertisements and marketing materials. Moreover, through services like "Lookalike Audiences,"[57] those third parties also received payment from companies other than Defendant to leverage Plaintiff's and Class members' protected health information and personally identifiable information for that same purpose.

---

[53] Tim Morey, *What's Your Personal Data Worth?*, DESIGN MIND (Jan. 18, 2011)
[54] Josh Constine, *Facebook pays teens to install VPN that spies on them*, TECHCRUNCH (Jan. 29. 2019), *available at* https://techcrunch.com/2019/01/29/facebook-project-atlas/
[55] https://www.forbes.com/sites/chrissamcfarlane/2025/03/29/the-wake-up-call-your-health-data-is-at-risk/
[56] *Id.*
[57] *See, e.g.*, https://www.stackadapt.com/resources/blog/audience-lookalike-expansion-targeting.

72. Put another way, Defendant and other companies paid the third parties here—including Google, Sweed, AdPredictive and StackAdapt—for services and products that relied on analyzing or otherwise exploiting Plaintiff's and Class members' personal information and their activity on Defendant's website without any renumeration to the Plaintiff or Class members.

73. Because Florida law recognizes a legal interest in unjustly earned profits, Plaintiff and Class members have an entitlement to profits earned from their personal data.

TOLLING, CONCEALMENT, AND ESTOPPEL

74. The applicable statutes of limitations have been tolled by Defendant's knowing and active concealment and denial of the facts alleged herein.

75. Defendant has never disclosed that it would or could disregard those representations and instead helps third parties intercept communications containing customers' personally identifiable information. Defendant affirmatively hid its true actions and knowingly made statements that were misleading and concealed the true nature of its conduct and operation. The circumstances of third-party trackers employed on and with respect to Defendant's website would lead reasonable users to believe third parties were not collecting their personally identifiable information or that Defendant was facilitating disclosure of the same.

76. Moreover, Plaintiff was ignorant of the information essential to pursue his claims, without any fault or lack of diligence on his own part.

77. Furthermore, under the circumstances Defendant was under a duty to disclose the true character, quality, and nature of its activities to Plaintiff. Defendant therefore is estopped from relying on any statute of limitations.

78. All applicable statutes of limitation also have been tolled by operation of the discovery rule. Specifically, Plaintiff and other Class members could not have learned through the exercise of reasonable diligence of Defendant's conduct as alleged herein.

79. Accordingly, Plaintiff and the Class could not have reasonably discovered the truth about Defendant's practices until shortly before this class litigation was commenced.

CLASS ALLEGATIONS

80. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff brings this action on behalf of himself and on behalf of all other persons similarly situated and seeks to certify the following class (the "Nationwide Class"): All persons in the United States with a prescription for medical marijuana who accessed and navigated to www.curaleaf.com.

81. Plaintiff also seeks to certify the following sub-class (the "Florida Class"): All persons in the state of Florida who accessed and navigated to www.curaleaf.com.

82. Plaintiff reserves the right to modify the class definitions, including by using additional subclasses, as appropriate based on further investigation and discovery obtained in the case.

83. Numerosity of the Classes: The Classes are composed of many thousands of individuals, the joinder of which in one action would be impracticable. The disposition of their claims through this class action will benefit both parties and the Court.

84. Existence and Predominance of Common Questions of Fact and Law: There is a well-defined community of interest in the questions of law and fact affecting proposed Class members. The questions of law and fact common to the proposed class predominate over questions affecting only individual members. Such questions include, but are not limited to, the following:

a. whether Defendant facilitated or procured the unlawful actions of third parties, including Google, Sweed, AdPredictive and StackAdapt;

b. whether Defendant obtained express consent for their conduct;

c. whether Defendant's conduct violated the Florida Security of Communications Act;

d. whether Plaintiff and the proposed Class members are entitled to damages, reasonable attorneys' fees, pre-judgement interest and costs of this suit; and

e. whether Defendant should be enjoined from similar conduct in the future.

85. Typicality: Plaintiff is asserting claims that are typical of the proposed Class members' claims because he has accessed and browsed Defendant's website, www.curaleaf.com. Plaintiff and the proposed Class members have similarly suffered harm arising from Defendant's violations of the law, as alleged herein. Such harms include invasion of privacy on matters and concerns that would be highly offensive to a reasonable person as a result of Defendant's uniform and wrongful conduct in intentionally disclosing their protected health information, personally identifiable information to third parties.

86. Adequacy of Representation: Plaintiff will fairly and adequately represent and protect the interests of the Classes. Plaintiff has retained counsel with substantial experience in prosecuting complex litigation and class actions, including privacy-protection cases. Plaintiff does not have any interests antagonistic to those of the Classes.

87. Superiority: A class action is superior to other available means for the fair and efficient adjudication of Plaintiff's and the proposed Class members' claims. Plaintiff and Class members have suffered irreparable harm as a result of Defendant's unfair, unlawful, and unconscionable conduct. Because of the size of the individual Class members' claims, few, if any, proposed Class members could afford to seek legal redress for the wrongs complained of herein. Absent the class action, the proposed Class members will continue to suffer losses and the violations of law described herein will continue without remedy, and Defendant will be permitted

to retain the proceeds of its misdeeds. Defendant continues to engage in the unlawful, unfair, and unconscionable conduct that is the subject of this Complaint.

88. Injunctive Relief: Plaintiff also satisfies the requirements for maintaining a class under Rule 23(b)(2). Defendant acted on grounds that apply generally to the proposed Classes, making final declaratory or injunctive relief appropriate with respect to the proposed Classes as a whole.

89. Particular Issues: Plaintiff also satisfies the requirements for maintaining a class action under Rule 23(c)(4). His claims consist of particular issues that are common to all Class members and are capable of class-wide resolution that will significantly advance the litigation.

CAUSES OF ACTION
COUNT I
Violation of the Wiretap Act
18 U.S.C. § 2510, *et. seq.*
(Nationwide Class)

90. Plaintiff repeats the allegations contained in paragraphs 1 through 89 as if fully set forth herein.

91. The Wiretap Act, as amended by the Electronic Communications Privacy Act of 1986, provides that "any person who … intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication … shall be subject to suit." 18 U.S.C. § 2511(1)(a).

92. The Wiretap Act also provides that, "[e]xcept as provided in section 2511(2)(a)(ii), any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate." 18 U.S.C. § 2520(a).

93. Defendant engaged in violations of the Wiretap Act by closely assisting third parties with intercepting Plaintiff's and Class members' confidential communications. As part of that enterprise, Defendant customized, configured, deployed, and intentionally integrated the computer code that intercepted electronic communications from Plaintiff and Class members while they accessed and navigated Defendant's website. Defendant took these actions to run marketing and advertising campaigns that target consumers based on their activity on Defendant's website. Indeed, Defendant paid the third parties here— Google, Sweed, AdPredictive and StackAdapt—for services and products that relied on analyzing or otherwise exploiting Plaintiff and Class members' personal information and their activity on Defendant's website.

94. Defendant also engaged in violations of the Wiretap Act by possessing and assembling the wiretapping devices while simultaneously playing an active role in the use of the computer code to intercept Plaintiff's and Class members' electronic communications.

95. By knowingly integrating code into its website, Defendant intentionally caused third parties—including but not limited to Google, Sweed, AdPredictive and StackAdapt—to intercept electronic communications. The interceptions were done contemporaneously with Plaintiff's and Class members' sending and receiving communications. The intercepted communications included the "contents" of electronic communications.

96. The transmission of data between Plaintiff and Defendant constitute "transfer[s] of signs, signals, writing, … data, [and] intelligence of [any] nature transmitted in whole or in part by a wire, radio, electromagnetics, photoelectronic, or photooptical system that affects interstate commerce[,]" and were therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(12).

97. The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

f. The computer codes and programs used by third parties—including but not limited to Google, Sweed, AdPredictive and StackAdapt—to track Plaintiff's and Class members' communications while they were navigating Defendant's website;
g. Plaintiff's and Class members' browsers or mobile applications;
h. Plaintiff's and Class members' computing and mobile devices;
i. The web and ad servers of third parties, including but not limited to Google, Sweed, AdPredictive and StackAdapt;
j. The web and ad-servers from which third parties—including but not limited to Google, Sweed, AdPredictive and StackAdapt—tracked and intercepted Plaintiff's and Class members' communications while they were using a web browser or mobile application to navigate Defendant's website;
i. The computer codes and programs used by third parties—including but not limited to Google, Sweed, AdPredictive and StackAdapt—to effectuate their tracking and intercepting of Plaintiff's and Class members' communications while they were navigating Defendant's website; and
j. The plan that third parties—including but not limited to Google, Sweed, AdPredictive and StackAdapt—carried out to effectuate their tracking and intercepting of Plaintiff's and Class members' electronic communications.

98. Plaintiff and Class members were unaware that third parties—including but not limited to Google, Sweed, AdPredictive and StackAdapt—were receiving: 1) form field entries; 2) full-string URLs; 3) information revealing the text of buttons clicked; and 4) information revealing the products that patients browsed, added to cart, and purchased.

99. Plaintiff and Class members never provided Defendant or the third parties—including but not limited to Google, Sweed, AdPredictive and StackAdapt—with consent to intercept or collect their electronic communications.

100. Defendant and the third parties—including but not limited to Google, Sweed, AdPredictive and StackAdapt—intercepted Plaintiff's and Class members' electronic communications for unlawful or tortious purposes. Those purposes include: 1) associating the content of electronic communications with preexisting consumer profiles; 2) violating HIPAA and state law by disclosing protected health information to run targeted advertisements and marketing

campaigns; and 3) aiding and abetting third parties—including but not limited to Google, Sweed, AdPredictive and StackAdapt—with using protected health information and personally identifiable information in a manner that violates state privacy laws, including those that mandate protecting "personal identification numbers" and "medical records." See Fla. Stat. § 817.011.

101. After third parties intercepted Plaintiff's and Class members' electronic communications, Defendant knowingly and unlawfully used those intercepted communications to guide its advertising and marketing efforts. When, for example, third parties—including Google, Sweed, AdPredictive and StackAdapt—received and processed Plaintiff's and Class members' electronic communications, Defendant used those communications to run targeted advertisements and personalized marketing campaigns.

102. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may award statutory damages to Plaintiff and Class members; injunctive and declaratory relief; punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by Defendant in the future; reasonable attorney's fees; and other litigation costs reasonably incurred.

COUNT II
Violation of Florida's Security of Communications Act
Fla. Stat. § 934.01
(Florida Class)

103. Plaintiff repeats the allegations contained in paragraphs 1 through 89 as if fully set forth herein.

104. Plaintiff brings this claim individually and on behalf of the members of the putative class against Defendant.

105. Florida's Security of Communications Act ("FSCA") prohibits "[i]ntentionally intercept[ing], endeavor[ing] to intercept, or procur[ing] any other person to intercept or endeavor to intercept any wire, oral, or electronic communication." Fla. Stat. § 934.03(1)(a).

106. The FSCA similarly prohibits "disclos[ing], or endeavor[ing] to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection." *See* Fla. Stat. § 934.03(1)(c).

107. The FSCA also prohibits "[i]ntentionally us[ing], or endeavor[ing] to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection." *See* Fla. Stat. § 934.03(1)(d).

108. Defendant violated the FSCA by procuring third parties—including but not limited to Google, Sweed, AdPredictive and StackAdapt—with intercepting the content of electronic communications, including those that contained protected health information and personally identifiable information.

109. Defendant violated the FSCA by employing the tracking technologies to disclose the contents of electronic communications, including those that contained protected health information and personally identifiable information.

110. Defendant violated the FSCA by using the contents of electronic communications to run marketing and advertising campaigns, including communications that contained protected health information and personally identifiable information.

111. By knowingly integrating code into its website, Defendant intentionally caused third parties—including but not limited to Google, Sweed, AdPredictive and StackAdapt—to

intercept and receive electronic communications. The interceptions were done contemporaneously with Plaintiff's and Class members' sending and receiving communications. The intercepted communications included the "contents" of electronic communications.

112. The transmission of data between Plaintiff and Defendant constitute "transfer[s] of signs, signals, writing, … data, [and] intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetics, photoelectronic, or photooptical system that affects interstate commerce[,]" and were therefore "electronic communications" within the meaning of Fla. Stat. § 934.02(1)(12).

113. The following constitute "devices" within the meaning of Fla. Stat. § 934.02(1)(4):

k. The computer codes and programs used by third parties—including but not limited to Google, Sweed, AdPredictive and StackAdapt—to track Plaintiff's and Class members' communications while they were navigating Defendant's website;
l. Plaintiff's and Class members' browsers or mobile applications;
m. Plaintiff's and Class members' computing and mobile devices;
n. The web and ad servers of third parties, including but not limited to Google, Sweed, AdPredictive and StackAdapt;
o. The web and ad-servers from which third parties—including but not limited to Google, Sweed, AdPredictive and StackAdapt—tracked and intercepted Plaintiff's and Class members' communications while they were using a web browser or mobile application to navigate Defendant's website;
i. The computer codes and programs used by third parties—including but not limited to Google, Sweed, AdPredictive and StackAdapt—to effectuate their tracking and intercepting of Plaintiff's and Class members' communications while they were navigating Defendant's website; and
k. The plan that third parties—including but not limited to Google, Sweed, AdPredictive and StackAdapt—carried out to effectuate their tracking and intercepting of Plaintiff's and Class members' electronic communications.

114. Plaintiff and Class members were unaware that third parties—including but not limited to Google, Sweed, AdPredictive and StackAdapt—were receiving: 1) form field entries; 2)

full-string URLs; 3) information revealing the text of buttons clicked; and 4) information revealing the products that patients browsed, added to cart, and purchased.

115. Plaintiff and Class members never provided Defendant or the third parties—including but not limited to Google, Sweed, AdPredictive and StackAdapt—with consent to intercept or collect their electronic communications.

116. As a result of the above actions and pursuant to Fla. Stat. § 934.10, the Court may award statutory damages to Plaintiff and Class members; injunctive and declaratory relief; punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by Defendant in the future; reasonable attorney's fees; and other litigation costs reasonably incurred.

COUNT III
Civil Theft
Fla. Stat. § 772.11
(Florida Class)

117. Plaintiff repeats the allegations contained in paragraphs 1 through 89 above as if fully set forth herein.

118. Plaintiff brings this Count individually and on behalf of the members of the putative Class.

119. Florida law provides that "[a] person commits theft if he or she knowingly obtains or uses, or endeavors to obtain or use, the property of another with intent to, either temporarily or permanently: (a) [d]eprive the other person of a right to the property or a benefit from the property; (b) [a]ppropriate the property to his or her own use or to the use of any person not entitled to the use of the property." See Fla. Stat. § 812.014. Florida law also provides that "both the actor and one who aids and abets him are principals in the first degree and may be charged and convicted of the crime." *Chudoin v. State*, 362 So. 2d 398, 401 (Fla. 2d DCA 1978).

120. The phrase "obtains or uses" means:

a. "Taking or exercising control over property."

b. "Making any unauthorized use, disposition, or transfer of property."

c. "Obtaining property by fraud, willful misrepresentation of a future act, or false promise."

d. "Conduct previously known as stealing; larceny; purloining; abstracting; embezzlement; misapplication; misappropriation; conversion; or obtaining money or property by false pretenses, fraud, or deception."

e. "Other conduct similar in nature." See Fla. Stat. § 812.012(3).

121. The term "property" means "anything of value." See Fla. Stat. § 812.012(4). This includes:

a. "Real property, including things growing on affixed to, and found on land."

b. "Tangible or intangible personal property, including rights, privileges, interests, and claims."

c. "Services." *Id.*

122. The phrase "property of another" means "property in which a person has an interest upon which another person is not privileged to infringe without consent, whether or not the other person also has an interest in the property." *See* Fla. Stat. § 812.012(5).

123. Plaintiff's and Class members' information—including but not limited to their health information, personally identifiable information, and online activity—has pecuniary value.

124. The third parties effectively charged Plaintiff and Class members by using their valuable personal information and protected health information without permission and exploiting such information for financial benefit. Plaintiff and Class members retain a stake in the profits

that Defendant and third parties earned from their personal information and other data because, under the circumstances, it is unjust for Defendant and the third parties to retain those profits.

125. As reflected by both federal and state law, Plaintiff and Class members have an interest in their health information, personally identifiable information, and online activity upon which third parties—including but not limited to Google, Sweed, AdPredictive and StackAdapt—were not privileged to infringe without consent. *See, e.g.*, 45 CFR § 164.508; Fla. Stat. § 381.986(10)(f)(5); Fla. Stat. § 817.5685(1); Fla. Stat. § 817.568(2)(a).

126. By integrating the tracking technologies into its website, Defendant knowingly aided and abetted third parties—including but not limited to Google, Sweed, AdPredictive and StackAdapt—with appropriating Plaintiff's and Class members' protected health information, personally identifiable information, and online activity.

127. Plaintiff and Class members never provided the third parties with consent to use their health information, personally identifiable information, and online activity.

128. As a result of the above actions and pursuant to Fla. Stat. § 772.11, the Court may award statutory damages to Plaintiff and Class members; injunctive and declaratory relief; punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by Defendant in the future; reasonable attorney's fees; and other litigation costs reasonably incurred.

COUNT IV
Violation of Florida's Deceptive and Unfair Trade Practices Act ("FDUTPA")
Fla. Stat. § 501.204, *et. seq.*
(Florida Class)

129. Plaintiff repeats the allegations contained in paragraphs 1 through 89 above as if fully set forth herein.

130. Plaintiff brings this Count individually and on behalf of the members of the putative Class.

131. Plaintiff is a "consumer" within the meaning of the Florida Deceptive and Unfair Trade Practices Act ("FDUTPA"), Fla. Stat. § 501.203(7), in that Plaintiff is an individual who purchased, or sought to purchase, and/or used Defendant's goods and services primarily for personal, family, or household purposes.

132. Florida law provides that "[u]nfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful." *See* Fla. Stat. § 501.204(1).

133. An "unfair practice" is one that offends established public policy and one that is immoral, unethical, oppressive, unscrupulous, or substantially injurious to consumers.

134. A "deceptive practice" is one that is likely to mislead consumers.

135. In enacting FDUTPA, the Legislature expressed its intent that "due consideration and great weight shall be given to the interpretations of the Federal Trade Commission and the federal courts relating to s. 5(a)(1) of the Federal Trade Commission Act, 15 U.S.C. § 45(a)(1), as of July 1, 2017. *See* Fla. Stat. § 501.204(2).

136. The FTC has made clear that "disclosing consumers' health information for advertising without their affirmative express may be an unfair practice."[58]

137. Under federal and state laws, Defendant was obligated to protect Plaintiff's and Class members' information—including but not limited to their health information, personally

[58] https://www.ftc.gov/business-guidance/resources/collecting-using-or-sharing-consumer-health-information-look-hipaa-ftc-act-health-breach

identifiable information, and online activity—from disclosure. *See, e.g.*, 45 CFR § 164.508; Fla. Stat. § 381.986(10)(f)(5); Fla. Stat. § 817.5685(1); Fla. Stat. § 817.568(2)(a).

138. Defendant engaged in unfair and deceptive practices by integrating tracking technologies into its website that disclosed Plaintiff's and Class members' information—including their health information, personally identifiable information, and online activity—to Google, Sweed, AdPredictive, and StackAdapt.

139. By integrating the tracking technologies into its website, Defendant received unjust enrichment and caused third parties to intrude upon Plaintiff's and Class members' seclusion. Defendant's misconduct thus caused Plaintiff and Class members to suffer actual damages.

140. As a result of the above actions and pursuant to Fla. Stat. § 501.211, the Court may award actual damages to Plaintiff and Class members; injunctive and declaratory relief; and reasonable attorney's fees.

COUNT V
Intrusion Upon Seclusion
(Florida Class)

141. Plaintiff hereby incorporates Paragraphs 1 through 89 as if fully stated herein.

142. As described herein, Defendant aided and abetted third parties with intruding upon the following legally protected privacy interests:

a. The Wiretap Act as alleged herein;
b. Florida's Security of Communications Act as alleged herein;
c. Statutory and regulatory protections for protected health information and personally identifiable information as alleged herein;

143. Plaintiff and Class members had a reasonable expectation of privacy under the circumstances in that Plaintiff and Class members could not reasonably expect Defendant would commit acts in violation of federal and state civil and criminal law.

144. Defendant's actions and the third parties' actions constitute a serious invasion of privacy in that such actions:

a. Violated several criminal laws, including the Wiretap Act;
b. Invaded the privacy rights of millions of Americans (including Plaintiff and Class members) without their consent; and
c. Constituted the unauthorized taking of valuable information from millions of Americans through deceit.

145. Committing criminal acts against millions of Americans constitutes an egregious breach of social norms that is highly offensive.

146. The surreptitious and unauthorized tracking of the internet communications of millions of Americans—particularly where, as here, such communications are sensitive and confidential—constitutes an egregious breach of social norms that is highly offensive.

147. The disclosure of personally identifiable information of millions of Americans through deceit is highly offensive behavior.

148. Plaintiff and Class members have been damaged by Defendant's invasion of their privacy and are entitled to just compensation and injunctive relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff individually and on behalf of all others similarly situated, seeks judgment against Defendant, as follows:

a. For an order certifying the putative class and naming Plaintiff as the representatives of the putative Class and Plaintiff's attorneys as Class Counsel to represent the putative Class members;
b. For an order declaring that the Defendant's conduct violates the statutes referenced herein;
c. For an order declaring that Defendant's conduct violates the statutes referenced herein;

d. For an order finding in favor of Plaintiff and the putative Class on all counts asserted herein;

e. For the statutory damages in amounts to be determined by the Court and/or jury;

f. For prejudgment interest on all amounts awarded;

g. For injunctive relief as pleaded or as the Court may deem proper; and

h. For an order awarding Plaintiff and the putative Class their reasonable attorneys' fees and expenses and cost of suit.

JURY DEMAND

Plaintiff requests a trial by jury for all issues so triable on its claims pursuant to FED R. CIV. P. 38(b) and 38(c).

Dated: November 8, 2025

Respectfully submitted,

MARCUS RASHBAUM PINEIRO & MEYERS LLP
By: ***Christopher R. Reilly***
Christopher R. Reilly, Esq.
Florida Bar No. 1025097
creilly@mnrpfirm.com
Michael A. Pineiro, Esq.
Florida Bar No. 41897
mpineiro@mrpfirm.com
One Biscayne Tower
2 S. Biscayne Blvd., Ste. 2530
Miami, Florida 33131
Telephone: (305) 400-4260

RAVINDRAN LAW FIRM, PLLC
Arun Ravindran, Esq.
Florida Bar No. 66247
arun@ravindranlaw.com
2525 Ponce de Leon Blvd., Suite 300
Miami, Florida 33134
Telephone: (305) 677-8713