Hart L. Robinovitch (AZ SBN 020910)
**ZIMMERMAN REED LLP**
14646 North Kierland Blvd., Suite 145
Scottsdale, AZ 85254
Telephone: (480) 348-6400
Facsimile: (480) 348-6415
Email: hart.robinovitch@zimmreed.com

David S. Almeida (*pro hac vice forthcoming*)
Elena A. Belov (*pro hac vice forthcoming*)
**ALMEIDA LAW GROUP LLC**
849 W. Webster Avenue
Chicago, Illinois 60614
Tel: (312) 576-3024
david@almeidalawgroup.com
elena@almeidalawgroup.com

*Attorneys for Plaintiffs & the Classes*

**IN THE UNITED STATES DISTRICT COURT**

**DISTRICT OF ARIZONA**

MONTANA STRONG and DEBRA YICK, *individually and on behalf of all others similarly situated*,

Plaintiffs,

v.

LIFESTANCE HEALTH GROUP, INC. d/b/a LifeStance, a Delaware corporation,

Defendant.

**Case No. _____**

**CLASS ACTION COMPLAINT**

**JURY TRIAL DEMANDED**

# CLASS ACTION COMPLAINT

Plaintifs MONTANA STRONG and DEBRA YICK bring this class action lawsuit, individually and on behalf of all others similarly situated, against LIFESTANCE HEALTH GROUP, INC. d/b/a LifeStance ("LifeStance" or "Defendant") and allege, upon personal knowledge as to their own actions, their counsel's investigation and upon information and good faith belief as to all other matters, as follows:

## NATURE OF THE ACTION

1. Information concerning a person's physical and mental health is among the most confidential and sensitive information in our society and the mishandling of such information can have serious consequences, including, but certainly not limited to, discrimination in the workplace and/or denial of insurance coverage.[1]

2. Simply put, if people do not trust that their sensitive private information will be kept private and secure, they may be less likely to seek medical treatment which can lead to much more serious health consequences down the road. In addition, protecting medical information and making sure it is kept confidential and not disclosed to any unauthorized entities is vitally necessary to maintain public trust in the healthcare system as a whole.

3. The need for data security (and transparency) is particularly acute when it comes to the rapidly expanding world of digital telehealth providers. Of all the information the average internet user shares with the technology companies, health data—and especially mental health

[1] *See* Lindsey Ellefson, *Telehealth Sites Put Addiction Patient Data at Risk: New research found pervasive use of tracking tech on substance-abuse-focused health care websites, potentially endangering users in a post-Roe world*, WIRED (Nov. 16, 2022), available at https://www.wired.com/story/substance-abuse-telehealth-privacy-tracking-tech/ (last visited April 15, 2023) ("While the sharing of any kind of patient information is often strictly regulated or outright forbidden, it's even more verboten in addiction treatment, as patients' medical history can be inherently criminal and stigmatized."); *see also* Todd Feathers, Simon Fondrie-Teitler, Angie Waller & Surya Mattu, *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, THE MARKUP (June 16, 2022), available at https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites (last visited April 15, 2023).

data[2]–is some of the most valuable and controversial.[3]

4. Despite dealing with extremely sensitive and personal issues like depression, suicide, domestic violence and PTSD, many telehealth sites appear to value the collection and monetization of user data over all else.[4]

5. These mental health apps are a data harvesting bonanza as "[n]early all the apps reviewed gobble up users' personal data . . . Further, some apps harvest additional data from third-party platforms (like Facebook), elsewhere on users' phones, or data brokers."[5]

6. These telehealth companies are collecting, in some instances, "ultra-sensitive personal data" about patients ranging from those seeking information about their reproductive rights and options, those seeking information regarding their addictions and . . . those seeking mental health counseling.[6]

---

[2] Mental health sites are collecting far more data than is necessary and certainly more than is disclosed to users. For instance, social media behemoths like Facebook are often notified each and every time a person opens a particular mental health app, essentially signaling to the social media company how often those patients are going to a session and when they booked appointments.

[3] Protected and highly sensitive medical information collected by healthcare entities includes many categories, from intimate details of an individual's conditions, symptoms, diagnoses and treatments to personally identifying information to unique codes which can identify and connect individuals to the collecting entity. *See* Molly Osberg & Dhruv Mehrotral, *The Spooky, Loosely Regulated World of Online Therapy*, JEZEBEL (Feb. 19, 2020), available at https://jezebel.com/the-spooky-loosely-regulated-world-of-online-therapy-1841791137 (last visited April 15, 2023).

[4] *See, e.g., Top Mental Health and Prayer Apps Fail Spectacularly at Privacy, Security*, MOZILLA (May 2, 2022), available at https://foundation.mozilla.org/en/blog/top-mental-health-and-prayer-apps-fail-spectacularly-at-privacy-security/ (last visited April 15, 2023).

[5] *Id.* (stating that "others are taking advantage of this. Silicon Valley investors are pouring hundreds of millions of dollars into these apps. Insurance companies get to collect extra data on the people they insure. And data brokers are enriching their databases with even more sensitive data").

[6] Grace Oldham & Dhruv Mehrotra, *Facebook and Anti-Abortion Clinics Are Collecting Highly Sensitive Info on Would-Be Patients*, REVEAL (June 15, 2022), available at https://revealnews.org/article/facebook-data-abortion-crisis-pregnancy-center/ (noting that such "personal data can be used in a number of ways. The centers can deliver targeted advertising, on Facebook or elsewhere, aimed at deterring an individual from getting an abortion. It can be used to build anti-abortion ad campaigns – and spread misinformation about reproductive health

7. It is not difficult to imagine what use a social media company might have for tracking a person who is struggling with their mental health and how often they seek therapy; in 2017, a leaked Facebook sales pitch showed the company boasting of how its algorithm could identify and target teenagers who were feeling "insecure" and "worthless," "overwhelmed" or "anxious."

8. Moreover, there is unfortunately still some stigma in dealing with mental health issues; impermissibly disclosed medical information could be particularly damaging to patients seeking care for substance use disorders, among many other problematic outcomes for users of telehealth services.[7]

9. And, while mobile health options have been celebrated by some as a way to expand treatment, the tangible, real-world implications and potential for abuse is staggering:

> [T]he sensitive information people share during treatment for substance use disorders could easily impact their employment status, ability to get a home, custody of their children, and even their freedom. Health care providers and lawmakers recognized long ago that the potential threat of losing so much would deter people from getting life-saving help and set up strict laws to protect those who do seek treatment. ***Now, experts worry that data collected on telehealth sites could bring about the harm [the law] was designed to prevent and more, even inadvertently***.[8]

10. LifeStance is a mental healthcare company "focused on providing evidence-based, medically driven treatment services for children, adolescents, and adults suffering from a variety of mental health issues in an outpatient care setting, both in-person and through its digital health

---

– targeted at people with similar demographics and interests. And, in the worst-case scenario now contemplated by privacy experts, that digital trail might even be used as evidence against abortion seekers in states where the procedure is outlawed") (last visited April 15, 2023).

[7] *See* Lindsey Ellefson, *Telehealth Sites Put Addiction Patient Data at Risk: New research found pervasive use of tracking tech on substance-abuse-focused health care websites, potentially endangering users in a post-Roe world*, WIRED (Nov. 16, 2022), available at https://www.wired.com/story/substance-abuse-telehealth-privacy-tracking-tech/ (last visited April 15, 2023) ("While the sharing of any kind of patient information is often strictly regulated or outright forbidden, it's even more verboten in addiction treatment, as patients' medical history can be inherently criminal and stigmatized.").

[8] *Id.* (emphasis added).

telemedicine offering."[9] The company offers both outpatient care services via in-person locations and telemedicine, and it has over 600 locations nationwide and employs more than 5,200 psychiatrists, advanced practice nurses, psychologists and therapists.

11. LifeStance Health offers the following mental health services: (i) Psychiatric appointments, which can include medication management along with cognitive behavioral therapy; (ii) Medication management, ongoing consultation with a psychiatrist regarding the outcomes and effectiveness of prescribed medications; (iii) Individual therapy, which can include generalist/integrative therapy, cognitive behavioral therapy, dialectical behavioral therapy, eye movement desensitization and reprocessing and intensive outpatient programs and (iv) Group therapy, which includes addiction group therapy, group therapy for PTSD, grief group therapy, and additional issues if necessary, facilitated by a therapist.

12. LifeStance owns, maintains and controls a website, www.LifeStance.com (the "Website"), and through various subsidiaries, provides management services to a number of entities engaged in the provision of behavioral healthcare services, all of which are included in the Website.[10]

13. Plaintiffs and Class Members who visited and used (collectively, the "Users") Defendant's Website understandably thought they were communicating *only* with their trusted healthcare providers.

14. Unfortunately, LifeStance intentionally chose to put its profits over the privacy of its Users, which number several million. Specifically, LifeStance installed certain tracking technologies on its Website in order to intercept and to send personally identifiable information ("PII") and protected health information ("PHI," and with "PII," "Private Information") to third parties such as Meta Platforms, Inc. d/b/a Facebook ("Facebook") and/or Google LLC without the informed consent of its Users.

15. The Private Information illegally sent to these third parties is, in turn, associated

[9] https://lifestance.com/why-lifestance (last visited April 15, 2023); *see also* 10-K, filed by Defendant on or about March 9, 2023 (available at: https://investor.lifestance.com/sec-filings/sec-filing/10-k/0000950170-23-007018)(last visited April 17, 2023).

[10] *See* https://lifestance.com/privacy-policy/ (last visited April 15, 2023).

with other information to create very fulsome user profiles that are mined for marketing and other commercial purposes. For example, in the case of information sent by LifeStance to Facebook, such information was then linked to Plaintiffs' unique Facebook user ID ("Facebook ID" or "FID") so that there was no anonymity in that Facebook and/or any third parties who were able to access the information would be able to associate such personal health data with Plaintiffs and all class members.

16. Despite warnings that healthcare companies were disclosing Private Information to social media companies by embedding and using Meta Pixels (and/or similar technologies) as far back as at least February 2020, LifeStance breached confidentiality and violated Plaintiffs' (as well as millions of other users') privacy when it unilaterally chose to embed the Pixel to share Private Information with third parties.[11]

17. As detailed herein, LifeStance owed common law, statutory and regulatory duties to keep Plaintiffs' and class members' communications and medical information safe, secure and confidential. First, the disclosure of Plaintiffs' and class members' Private Information via the Pixel contravenes the letter and spirit of HIPAA's "Standards for Privacy of Individually Identifiable Health Information" (also known as the "Privacy Rule") which governs how health care providers must safeguard and protect Private Information.

18. While healthcare organizations regulated under HIPAA may use third-party tracking tools, such as Google Analytics or Meta Pixel, they can do so only in a very limited way:

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health

[11] Molly Osberg & Dhruv Mehrotral, *The Spooky, Loosely Regulated World of Online Therapy*, JEZEBEL (Feb. 19, 2020), available at https://jezebel.com/the-spooky-loosely-regulated-world-of-online-therapy-1841791137 (last visited April 15, 2023); *see also* Timothy M. Hale, PhD & Joseph C. Kvedar, MD, *Privacy and Security Concerns in Telehealth*, (Dec. 2014), https://journalofethics.ama-assn.org/article/privacy-and-security-concerns-telehealth/2014-12, AMA JOURNAL OF ETHICS (last visited April 20, 2023) (illustrating that problems with privacy and telehealth apps started to surface as early as 2014).

> data… ***If such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.*** [12]

19. Moreover, the Office for Civil Rights at HHS has made clear, in a recent bulletin entitled *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, that the transmission of such protected information violates HIPAA's Privacy Rule:

> Regulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. ***For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.***[13]

20. Further, Defendant breached its statutory and common law obligations to Plaintiffs and class members by, *inter alia*: (i) failing to adequately review its marketing programs to ensure its Website was safe and secure; (ii) failing to remove or disengage technology that was known and designed to share Users' Private Information; (iii) failing to obtain the prior written consent of Plaintiffs and class members to disclose their Private Information to Facebook and/or others before doing so; (iv) failing to take steps to block the transmission of Plaintiffs' and class members' Private Information through Facebook Pixels; (v) failing to warn Plaintiffs and class members that their Private Information was being shared with third parties without express consent and (vi) otherwise failing to design and monitor its Properties to maintain the security, confidentiality and integrity of patient Private Information.

---

[12] *Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html, HHS.GOV (last visited April 15, 2023) (noting that "HIPAA Identifiers" include name; address (all geographic subdivisions smaller than state, including street address, city county, and zip code); all elements (except years) of dates related to an individual (including birthdate, admission date, discharge date, date of death, and exact age); telephone numbers; email address; medical record number; health plan beneficiary number; account number; device identifiers and serial numbers; web URL; internet protocol (IP) address; and any other characteristic that could uniquely identify the individual).

[13] *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates,* available at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html, HHS.GOV (emphasis added) (last visited April 15, 2023).

21. Despite incorporating the Facebook Pixel and CAPI into its Website and servers, LifeStance has never disclosed to Plaintiffs or Class Members that it shared their sensitive and confidential communications and Private Information with Facebook.[14] Defendant (or any third-parties) did not obtain Plaintiff's and class members' prior consent before sharing their sensitive and confidential communications and Private Information with third-parties such as Facebook.

22. As a result of Defendant's conduct, Plaintiffs and class members have suffered numerous injuries, including: (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Pixel; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private Information; (v) statutory damages and (vi) continued and ongoing risk to their Private Information.

23. Plaintiffs seek, on behalf of themselves and a class of similarly situated persons, to remedy these harms and therefore assert the following statutory and common law claims against LifeStance: (i) Violation of the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et. seq*.; (ii) Violation of the California Confidentiality of Medical Information Act, Cal. Civ. Code §§ 56, *et seq*. ; (iii) Violation of Electronic Communications Privacy Act, 18 U.S.C. § 2511(1), *et seq*., Unauthorized Interception, Use and Disclosure; (iv) Violation of Electronic Communications Privacy Act, 18 U.S.C. § 2511(3)(a), *et seq*., Unauthorized Divulgence by Electronic Communications Service; (v) Violation of The Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq*. – Unlawful Business Practices; (vi) Violation of The Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code § 17200, *et seq*. – Unfair Prong; (vii)

---

[14] In contrast to Defendant, in recent months several medical providers which have installed the Facebook Pixel on their web properties have provided their patients with notices of data breaches caused by the Pixel transmitting PHI to third parties. *See*, *e.g.*, *Cerebral, Inc. Notice of HIPAA Privacy Breach*, available at https://cerebral.com/static/hippa_privacy_breach-4000c6eb21449c2ecd8bd13706750cc2.pdf (last visited April 15, 2023); *Advocate Aurora says 3M patients' health data possibly exposed through tracking technologies* (Oct. 20, 2022), available at https://www.fiercehealthcare.com/health-tech/advocate-aurora-health-data-breach-revealed-pixels-protected-health-information-3 (last visited April 15, 2023); *Novant Health notifies patients of potential data privacy incident* (Aug. 12, 2022), available at https://www.novanthealth.org/home/about-us/newsroom/press-releases/newsid33987/2672/novant-health-notifies-patients-of-potential-data-privacy-incident-.aspx (last visited April 15, 2023).

violation of A.R.S. §44-1521 *et seq.* (viii) Violation of New York General Business Law § 349, *et seq.*; (ix) Common Law Invasion of Privacy – Intrusion Upon Seclusion and (x) Breach of Confidence.

## THE PARTIES

24. Plaintiffs MONTANA STRONG is, and at all relevant times was, an individual residing in Afton, Chenango County, in the State of New York.

25. Plaintiffs DEBRA YICK is, and at all relevant times was, an individual residing in San Francisco, San Francisco County, in the State of California.

26. Defendant LIFESTANCE HEALTH GROUP, INC. d/b/a LifeStance is incorporated in the State of Delaware, and its principal place of business is located at 4800 N. Scottsdale Road in Scottsdale, Arizona 85251.

## JURISDICTION & VENUE

27. This Court has subject matter jurisdiction further to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds $5 million, exclusive of interest and costs, and minimal diversity exists because at least one class member and Defendant are citizens of different states.

28. This Court has federal question jurisdiction further to 29 U.S.C. § 1331 because this complaint alleges violation of federal laws, specifically the Electronic Communications Privacy Act, 18 U.S.C. § 2511(1), *et seq*.

29. The Court has personal jurisdiction over Defendant LifeStance because its principal place of business and headquarters are located in Scottsdale, Arizona, and it regularly engages in extensive business throughout the country and the State of Arizona. Defendant's actions, conduct and omissions emanating in and from its principal offices in Arizona, as described further herein, harmed class members nationwide, including Plaintiffs.

30. Venue is proper in this judicial district pursuant to 18 U.S.C.§ 1391(b)(1) because Defendant's principal place of business is in this judicial district and a substantial part of the events or omissions giving rise to the claims asserted herein occurred in this judicial district.

## FACTUAL ALLEGATIONS

### *A. The Use of Tracking Technologies in the Telehealth Industry.*

31. Tracking tools[15] installed on many hospitals', telehealth companies' and other healthcare providers' websites (and other digital properties) are collecting patients' and other visitors' confidential and private health information—including details about their medical conditions, prescriptions and appointments, among *many* other things—and sending that information to third party vendors without prior, informed consent.[16]

32. Investigative journalists have published several reports detailing the seemingly ubiquitous use of tracking technologies on hospitals,' health care providers' and telehealth companies' digital properties to surreptitiously capture and to disclose their Users' personal health information ("PHI").[17]

33. Regarding telehealth companies specifically, the aptly titled report *"Out Of Control": Dozens of Telehealth Startups Sent Sensitive Health Information to Big Tech Companies*, a joint investigation by STAT and The Markup of 50 direct-to-consumer telehealth companies found that virtual care websites were providing sensitive medical information they

---

[15] The Office for Civil Rights at the HHS has defined "tracking technology" as a script or code on a website or mobile app used to gather information about users as they interact with the website or mobile app. After information is collected through tracking technologies from websites or mobile apps, it is then analyzed by owners of the website or mobile app ("website owner" or "mobile app owner"), or third parties, to create insights about users' online activities. *See Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates,* https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html, HHS.GOV (last visited April 15, 2023).

[16] *See, e.g.*, Todd Feathers, Simon Fondrie-Teitler, Angie Waller & Surya Mattu, *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, THE MARKUP (June 16, 2022), https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites (last visited April 15, 2023).

[17] *See, e.g.*, Dave Muoio & Annie Burky, *Advocate Aurora, WakeMed get served with class action over Meta's alleged patient data mining*, FIERCE HEALTHCARE (Nov. 4, 2022), https://www.fiercehealthcare.com/health-tech/report-third-top-hospitals-websites-collecting-patient-data-facebook (last visited April 15, 2023).

collect to the world's largest advertising platforms.[18]

34. Many telehealth sites had at least one tracker—from Meta, Google, TikTok, Bing, Snap, Twitter, LinkedIn or Pinterest—that collected patients' answers to medical intake questions.[19] These pixels are snippets of code that track internet and app users as they navigate through a website, logging which pages they visit, which buttons they click and certain information they enter into forms. In exchange for installing the pixels, third party platforms (*e.g.,* Facebook and Google) provide website owners analytics about the advertisements they have placed as well as tools to target people who have visited their web properties.

35. Of all the information the average internet user shares with the technology companies, health data—and especially mental health data[20]– is some of the most valuable and controversial. While the information captured and disclosed without permission may vary depending on the pixel(s) embedded, these "data packets" can be extensive, sending, for example, not just the name of a physician and field of medicine, but also the first name, the last name, email address, phone number and zip code and city of residence entered into the booking form.

36. In addition, that data is linked to a specific internet protocol ("IP") address.[21] The

---

[18] Todd Feathers, Katie Palmer (STAT) & Simon Fondrie-Teitler, *"Out Of Control": Dozens of Telehealth Startups Sent Sensitive Health Information to Big Tech Companies: An investigation by The Markup and STAT found 49 out of 50 telehealth websites sharing health data via Big Tech's tracking tools*, MARKUP (Dec. 13, 2022), https://themarkup.org/pixel-hunt/2022/12/13/out-of-control-dozens-of-telehealth-startups-sent-sensitive-health-information-to-big-tech-companies (last visited April 15, 2023).

[19] *See id.* (noting, "[t]rackers on 25 sites, including those run by industry leaders Hims & Hers, Ro, and Thirty Madison, told at least one big tech platform that the user had added an item like a prescription medication to their cart, or checked out with a subscription for a treatment plan").

[20] Mental health sites are collecting far more data than is necessary and certainly more than is disclosed to Users. As detailed in the Jezebel article, social media behemoths like Facebook are often notified each and every time a person opens a particular mental health app, essentially signaling to the social media company how often those patients are going to a session and when they booked appointments.

[21] Even IP addresses – which in theory could be connected to several members of the same household – are considered PHI *even when the individual does not have an existing relationship*

Meta Pixel, for example, sends information to Facebook via scripts running in a person's internet browser so each data packet comes labeled with an IP address that can be used in combination with other data to identify an individual or household.[22]

37. Even if Users somehow become aware that a given website is utilizing pixels to collect and to disseminate their data without permission, the third-party platforms have designed (and the site owners have implemented) workarounds that cannot be evaded by savvy users.

38. Facebook's workaround, for example, is called Conversions API (CAPI). CAPI is an effective workaround because it does not intercept data communicated from the user's browser; rather, CAPI "is designed to create a direct connection between [Web hosts'] marketing data and [Facebook]." Thus, the (supposedly) private communications between patients and Defendant, which are necessary to use Website, are actually received by Defendant and stored on its server before CAPI collects and sends the Private Information contained in those communications directly from Defendant to Facebook. Client devices do not have access to host servers and thus cannot prevent (or even detect) this transmission.[23]

39. Thus, without any knowledge, authorization or action by a User, a website owner (like LifeStance) can use its source code to commandeer a user's computing device, causing the

---

*with the regulated healthcare entity* since when the medical provider collects this information through its website or mobile app, it is indicative that the individual has received or will receive health care services or benefits from the medical provider. *See* HHS.gov, USE OF ONLINE TRACKING TECHNOLOGIES BY HIPAA COVERED ENTITIES & BUSINESS ASSOCIATES, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaaonline-tracking/index.html (last visited April 15, 2023).

[22] In addition, if the person is (or recently has) logged into Facebook when they visit a particular website, some browsers will attach third-party cookies—another tracking mechanism—that allow Meta to link pixel data to specific Facebook accounts.

[23] While there is no way to confirm with certainty that a Web host like Defendant has implemented workarounds like CAPI without access to the host server, companies like Facebook instruct the companies it partners with to "[u]se the Conversions API in addition to the [] Pixel, and share the same events using both tools," because such a "redundant event setup" allows Defendant "to share website events [with Facebook] that the pixel may lose." Thus, it is reasonable to infer that Facebook's customers who implement the Meta Pixel in accordance with Facebook's documentation will also implement the Conversions API workaround. *See Best practices for Conversions API,* https://www.facebook.com/business/help/308855623839366?id=818859032317965, FACEBOOK.COM (last visited April 15, 2023).

device to contemporaneously and invisibly re-direct the users' communications to third parties.

40. In this case, LifeStance employed the Meta Pixel and, upon information and good faith belief, CAPI and/or other similar technologies, to intercept, duplicate and re-direct Plaintiffs' and Class Members' Private Information to third parties like Facebook and Google.

***B. LifeStance Discloses Plaintiffs' and Class Members' Private Information to Facebook.***

41. LifeStance "offers long-term online care and medication management for a wide range of mental health conditions," from depression and PTSD to bipolar disorder and alcohol dependence, through therapy and medication.[24]

42. Defendant uses the Website to connect Plaintiffs and Class Members to its digital healthcare platforms with the goal of increasing profitability.

43. Defendant purposely installed the Pixel and other tracking tools on its Web Properties and programmed the Properties to surreptitiously share its patients' private and protected communications with Facebook, including communications that contain Plaintiffs' and Class Members' Private Information.

44. In order to understand Defendant's unlawful data sharing practices, it is important to first understand basic web design and tracking tools.

45. Facebook operates the world's largest social media company and generated $117 billion in revenue in 2021, roughly 97% of which was derived from selling advertising space.[25]

46. In conjunction with its advertising business, Facebook encourages and promotes entities and website owners, such as Defendant, to utilize its "Business Tools" to gather, identify, target and market products and services to individuals.

47. Facebook's Business Tools, including the Pixel, are bits of code that advertisers can integrate into their webpages, mobile applications and servers, thereby enabling the interception and collection of user activity on those platforms.

---

[24] https://lifestance.com/ (last visited April 20, 2023).

[25] META REPORTS FOURTH QUARTER AND FULL YEAR 2021 RESULTS, https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx, INVESTOR.FB.COM (last visited April 15, 2023).

48. The Business Tools are automatically configured to capture "Standard Events" such as when a user visits a particular webpage, that webpage's Universal Resource Locator ("URL") and metadata, button clicks, etc.[26]

49. Notably, advertisers, such as Defendant, can track other user actions and can create their own tracking parameters by building a "custom event."[27]

50. One such Business Tool is the Pixel which "tracks the people and type of actions they take."[28] When a user accesses a webpage with the Pixel, their communications with the host webpage are instantaneously and surreptitiously duplicated and sent to Facebook's servers—traveling from the user's browser to Facebook's server.

51. Notably, this transmission only occurs on webpages that contain the Pixel. Thus, Plaintiffs' and Class Member's Private Information would not have been disclosed to Facebook but for Defendant's decisions to install the Pixel on its Website.

52. Similarly, Plaintiffs' and Class Member's Private Information would not have been disclosed to Facebook via CAPI but for Defendant's decision to install and implement that tool on its Website.

53. By installing and implementing both tools, Defendant caused Plaintiffs' and Class Member's communications to be intercepted and transmitted to Facebook via the Pixel, and it caused a second improper disclosure of that information via CAPI.

---

[26] *Specifications for Facebook Pixel Standard Events*, https://www.facebook.com/business/help/402791146561655?id=1205376682832142, FACEBOOK. COM (last visited Mar. 21, 2023); *see*, META PIXEL, GUIDES, ADVANCED, https://developers.facebook.com/docs/facebook-pixel/advanced/, FACEBOOK.COM (last visited April 15, 2023); *see also* BEST PRACTICES FOR META PIXEL SETUP, https://www.facebook.com/business/help/218844828315224?id=1205376682832142, FACEBOOK. COM (last visited April 15, 2023); META MARKETING API, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/ FACEBOOK. COM (last visited April 15, 2023).

[27] ABOUT STANDARD AND CUSTOM WEBSITE EVENTS, https://www.facebook.com/business/help/964258670337005?id=1205376682832142, FACEBOOK. COM (last visited Mar. 21, 2023); *see also* META MARKETING API, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/, FACEBOOK. COM (last visited April 15, 2023).

[28] RETARGETING, https://www.facebook.com/business/goals/retargeting, FACEBOOK. COM (last visited April 15, 2023).

54. As explained below, these unlawful transmissions are initiated by Defendant's source code concurrent with communications made via the Website.

***C. LifeStance's Method of Transmitting Plaintiffs' & Class Members' Private Information via the Meta Pixel and/or CAPI.***

55. Web browsers are software applications that allow consumers to navigate the web and view and exchange electronic information and communications over the internet. Each "client device" (such as computer, tablet, or smart phone) accesses web content through a web browser (*e.g.*, Google's Chrome browser, Mozilla's Firefox browser, Apple's Safari browser and Microsoft's Edge browser).

56. Every website is hosted by a computer "server" that holds the website's contents and through which the entity in charge of the website exchanges communications with Internet users' client devices via web browsers.

57. Web communications consist of HTTP Requests and HTTP Responses, and any given browsing session may consist of thousands of individual HTTP Requests and HTTP Responses, along with corresponding cookies:

- **HTTP Request**: an electronic communication sent from the client device's browser to the website's server. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (i.e., web address), GET Requests can also send data to the host server embedded inside the URL, and can include cookies.
- **Cookies**: a small text file that can be used to store information on the client device which can later be communicated to a server or servers. Cookies are sent with HTTP Requests from client devices to the host server. Some cookies are "third-party cookies" which means they can store and communicate data when visiting one website to an entirely different website.
- **HTTP Response**: an electronic communication that is sent as a reply to the client device's web browser from the host server in response to an HTTP Request. HTTP Responses may consist of a web page, another kind of file, text information, or error codes, among other data. [29]

58. A patient's HTTP Request essentially asks the Defendant's Website to retrieve certain information (such as a physician's "Book an Appointment" page), and the HTTP

[29] One browsing session may consist of hundreds or thousands of individual HTTP Requests and HTTP Responses.

Response renders or loads the requested information in the form of "Markup" (the pages, images, words, buttons, and other features that appear on the patient's screen as they navigate Defendant's Website).

59. Every website is comprised of Markup and "Source Code." Source Code is a set of instructions that commands the website visitor's browser to take certain actions when the web page first loads or when a specified event triggers the code.

60. Source Code may also command a web browser to send data transmissions to third parties in the form of HTTP Requests quietly executed in the background without notifying the web browser's user. The Pixel Defendant uses Source Code that does just that. The Pixel acts much like a traditional wiretap.

61. When patients visit Defendant's Web Properties via an HTTP Request to LifeStance's server, that server sends an HTTP Response including the Markup that displays the Webpage visible to the user and Source Code including Defendant's Pixel.

62. Thus, Defendant is, in essence, handing patients a tapped device and once the Webpage is loaded into the patient's browser, the software-based wiretap is quietly waiting for private communications on the Webpage to trigger the tap, which intercepts those communications intended only for Defendant and transmits those communications to third parties, including Facebook and Google. Such conduct occurs on a continuous, and not sporadic, basis.

63. Third parties, like Facebook, place third-party cookies in the web browsers of users logged into their services.

64. These cookies uniquely identify the user and are sent with each intercepted communication to ensure the third-party can uniquely identify the patient associated with the Personal Information intercepted.

65. With substantial work and technical know-how, internet users can sometimes circumvent this browser-based wiretap technology. This is why third parties bent on gathering Private Information, like Facebook, implement workarounds that cannot be evaded by savvy users.

66. Facebook's workaround, for example, is called CAPI, which is an "effective" workaround because it does not intercept data communicated from the user's browser. Instead, CAPI "is designed to create a direct connection between [Web hosts'] marketing data and [Facebook]."

67. Thus, the communications between patients and Defendant, which are necessary to use Defendant's Website, are actually received by Defendant and stored on its server before CAPI collects and sends the Private Information contained in those communications directly from Defendant to Facebook.

68. Client devices do not have access to host servers and thus cannot prevent (or even detect) this transmission.

69. While there is no way to confirm with certainty that a Web host like Defendant has implemented workarounds like CAPI without access to the host server, companies like Facebook instruct Defendant to "[u]se the CAPI in addition to the [] Pixel, and share the same events using both tools," because such a "redundant event setup" allows Defendant "to share website events [with Facebook] that the pixel may lose."[30]

70. The third parties to whom a website transmits data through pixels and associated workarounds do not provide any substantive content relating to the user's communications. Instead, these third parties are typically procured to track user data and communications for marketing purposes of the website owner (i.e., to bolster profits).

71. Thus, without any knowledge, authorization, or action by a user, a website owner like Defendant can use its source code to commandeer the user's computing device, causing the device to contemporaneously and invisibly redirect the Users' communications to third parties.

72. In this case, Defendant employed the Tracking Pixel and CAPI to intercept, duplicate and re-direct Plaintiff's and Class Members' Private Information to Facebook.

73. For example, when a patient visits https://lifestance.com/ and selects "Find Provider" in New York, NY, the patient's browser automatically sends an HTTP Request to

[30] *See* https://www.facebook.com/business/help/308855623839366?id=818859032317965 (last visited April 18, 2023).

Defendant's web server. The Defendant's web server automatically returns an HTTP Response, which loads the Markup for that particular webpage as depicted below.

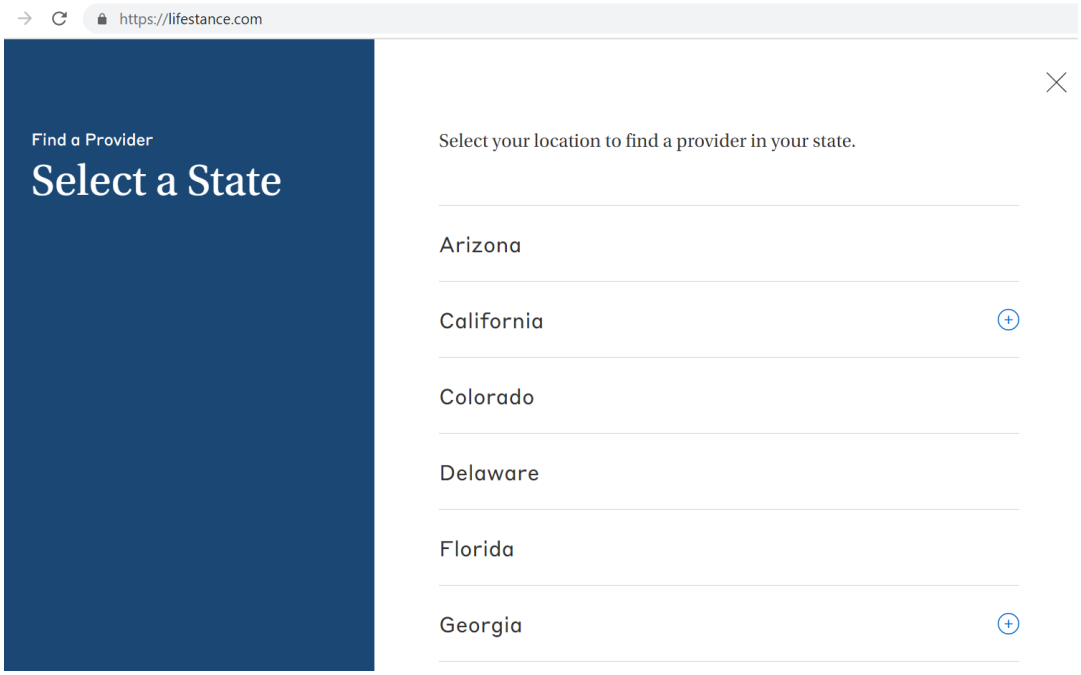


***Figure 1. Image taken from*** *https://www.lifestance.com*

74. The patient visiting this particular web page only sees the Markup, not the Defendant's Source Code or underlying HTTP Requests and Responses.

75. In reality, Defendant's Source Code and underlying HTTP Requests and Responses share the patient's personal information with Facebook, including the fact that the patient is looking for psychological treatment – along with the patient's unique Facebook identifiers.


***Figure 2. An HTTP single communication session sent from the device to Facebook that reveals that the User clicked on Find Provider button to make an online appointment, along with one of the patient's Facebook personal identifiers (datr field).***[31]

[31] One of the user's personal identifiers from Facebook, represented as the datr cookie highlighted in the image above, has been redacted to preserve the user's anonymity.

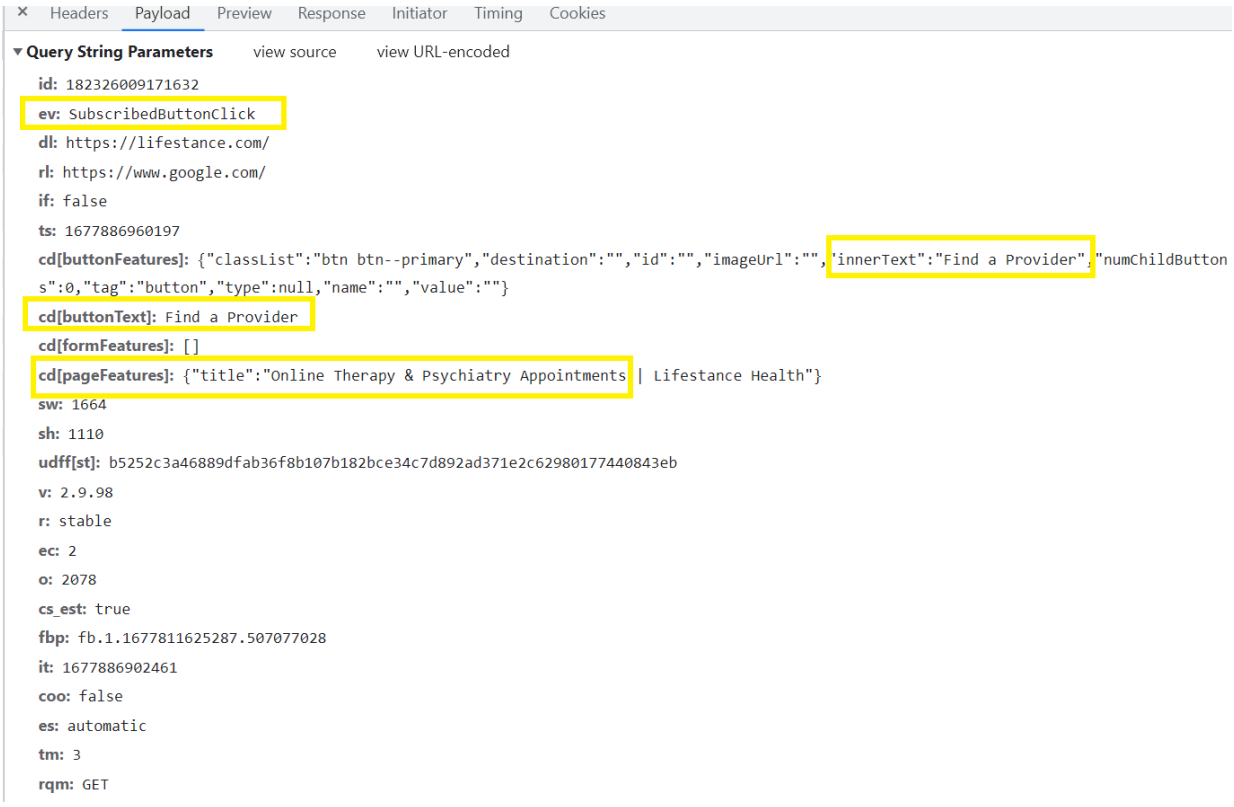


***Figure 3. An easier to read representation of data sent to Facebook when a patient clicks on Find Provider button to make an appointment.***

76. In addition to controlling a website's Markup, Source Code executes a host of other programmatic instructions and can command a website visitor's browser to send data transmissions to third parties via pixels or web bugs,[32] effectively open a spying window through which the webpage can funnel the visitor's data, actions, and communications to third parties.

77. Looking to the previous example, Defendant's Source Code manipulates the patient's browser by secretly instructing it to duplicate the patient's communications (HTTP Requests) and send those communications to Facebook.

78. This occurs because the Pixel embedded in Defendant's Source Code is programmed to automatically track and transmit a patient's communications, and this occurs contemporaneously, invisibly and without the patient's knowledge.

79. Thus, without its patients' consent, Defendant has effectively used its source code

[32] These pixels or web bugs are tiny image files that are invisible to website users. They are purposefully designed in this manner, or camouflaged, so that users remain unaware of them.

to commandeer patients' computing devices thereby re-directing their Private Information to third parties.

80. The information that Defendant's Pixel sends to Facebook may include, among other things, patients' PII, PHI and other confidential information.

81. Consequently, when Plaintiff and Class Members visit Defendant's website and communicate their Private Information, it is transmitted to Facebook, including, but not limited to, patient status, conditions and treatments, physician selected, specific button/menu selections, and appointment type and date.

***D. Defendant's Pixel and/or CAPI Tracking Practices caused Plaintiff's & Class Members' PII & PHI to be sent to Facebook.***

82. Defendant utilizes Facebook's Business Tools and intentionally installed the Pixel and CAPI on its Website to secretly track patients by recording their activity and experiences in violation of its common law, contractual, statutory and regulatory duties and obligations.

83. Defendant's Web Pages contain a unique identifier which indicates that the Pixel is being used on a particular webpage, identified as 18232600917632 on www.lifestance.com.

84. The Pixel allows Defendant to optimize the delivery of ads, measure cross-device conversions, create custom audiences and decrease advertising and marketing costs.

85. However, Defendant's Website does not rely on the Pixel in order to function.

86. While seeking and using Defendant's services as a medical provider, Plaintiff and Class Members communicated their Private Information to Defendant via its Website.

87. Defendant did not disclose to Plaintiff and Class Members that their Private Information would be shared with Facebook as it was communicated to Defendant.

88. Plaintiff and Class Members never consented, agreed, authorized or otherwise permitted Defendant to disclose their Private Information to Facebook, nor did they intend for Facebook to be a party to their communications with Defendant.

89. Defendant's Pixel and CAPI sent non-public Private Information to Facebook, including but not limited to Plaintiff's and Class Members': (i) status as medical patients; (ii) health conditions; (iii) sought treatment or therapies; (iv) appointment requests and appointment

booking information; (v) locations or facilities where treatment is sought; and (vi) which web pages were viewed.

90. Importantly, the Private Information Defendant's Pixel sent to Facebook was sent alongside Plaintiff's and Class Members' personal identifiers, including patients' IP address and cookie values thereby allowing individual patients' communications with Defendant, and the Private Information contained in those communications, to be linked to their unique Facebook accounts.

91. Through the source code deployed by Defendant, the cookies that it uses to help Facebook identify patients include but are not necessarily limited to cookies named: c_user, datr, fr, and fbp.[33]

92. The c_user cookie or FID is a type of third-party cookie assigned to each person who has a Facebook account and it is composed of a unique and persistent set of numbers.

93. A user's FID is linked to their Facebook profile, which generally contains a wide range of demographic and other information about the user, including pictures, personal interests, work history, relationship status, and other details. Because the user's Facebook Profile ID uniquely identifies an individual's Facebook account, Meta—or any ordinary person—can easily use the Facebook Profile ID to quickly and easily locate, access, and view the user's corresponding Facebook profile.

94. The datr cookie identifies the patient's specific web browser from which the patient is sending the communication. It is an identifier that is unique to the patient's specific web browser and is therefore a means of identification for Facebook users. Facebook keeps a record of every datr cookie identifier associated with each of its users, and a Facebook user can obtain a redacted list of all datr cookies associated with his or her Facebook account from Facebook.

[33] Defendant's Website tracks and transmits data via first-party and third-party cookies. C_user, datr, and fr cookies are third-party cookies. The fbp cookie is a Facebook identifier that is set by Facebook source code and associated with Defendant's use of the Facebook Pixel. The fbp cookie emanates from Defendant's Website as a putative first-party cookie, but is transmitted to Facebook through cookie synching technology that hacks around the same-origin policy.

95. The fr cookie is a Facebook identifier that is an encrypted combination of the c_user and datr cookies.[34]

96. Defendant deprived Plaintiff and Class Members of their privacy rights when it: (i) implemented technology (i.e., the Facebook Pixel) that surreptitiously tracked, recorded and disclosed Plaintiff's and other online patients' confidential communications and Private Information; (ii) disclosed patients' protected information to Facebook—an unauthorized third-party and (iii) undertook this pattern of conduct without notifying Plaintiff or Class Members and without obtaining their express written consent.

### *E. Defendant's Pixel Disseminates Patient Information Via www.lifestance.com*

97. If a patient uses www.lifestance.com to look for a doctor, they may select the "Find Provider" tab, which takes them to the "Find Provider" page. On this page Defendant asks the patient to narrow their search results by state and city.

98. Once the patient selects their state and city, Defendant asks them to narrow their search results by numerous filters, from treatment areas to provider gender and services provided.

[34] *See* Gunes Acar, Brendan Van Alsenoy, Frank Piessens, Claudia Diaz, and Bart Preneel, Facebook Tracking Through Social Plug-ins: Technical Report prepared for the Belgian Privacy Commission (March 27, 2015) (available at https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_pluginsv1.0.pdf ) (last visited April 20, 2023).

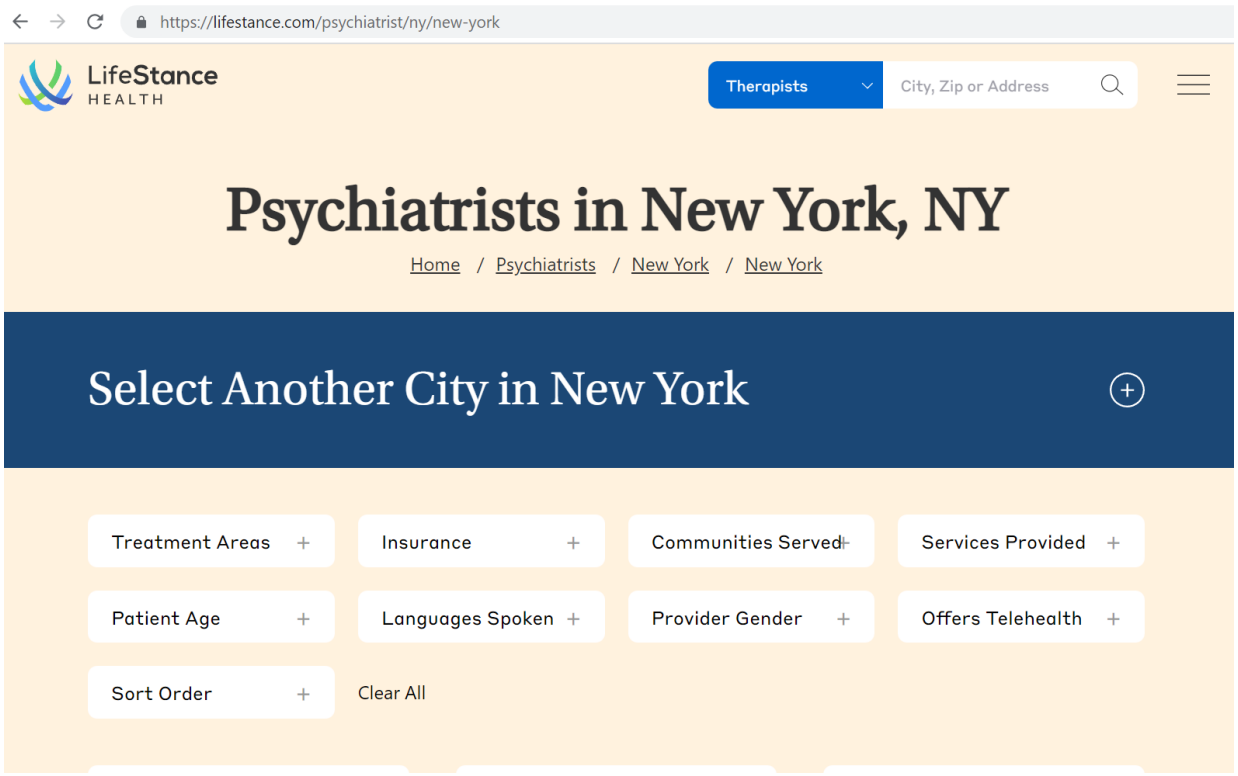


***Figure 4. Defendant directs patients to its "Find a Provider" webpage for psychiatrists in New York, NY, with embedded Pixels – which are invisible to the regular user.***

99. If a user selects filters or enters keywords into the search bar on the "Find a Provider" webpage, the filters and search terms are transmitted via the Facebook Pixel. Similarly, if a patient uses the Website's general search bar or chat, the terms and phrases the patient types are transmitted to Facebook, even if they contain a patient's treatment, procedures, medical conditions, and related queries.

100. This information is automatically sent from the patient's device to Facebook, and it reveals the patient's personal identifiers, including but not limited to, their IP address, FID, datr and fr cookies, along with each search filter the patient selected.

101. Without alerting the user, Defendant's Pixel sends each and every communication the user made to the Defendant via the Webpage to Facebook, and the images below confirm that the communications Defendant sends to Facebook contain the user's Private Information.

102. For example, a patient can search for a provider specializing in alcohol and drug use issues, with the option of using additional filters - from provider's gender to their additional

specialties.

103. After taking any of these actions on the 'Find a Provider' pages, patients are subsequently directed to the Provider Search Results page, and their selections or search parameters are automatically transmitted by the Pixel to Facebook along with the user's unique personal identifiers, as evidenced by the images below.

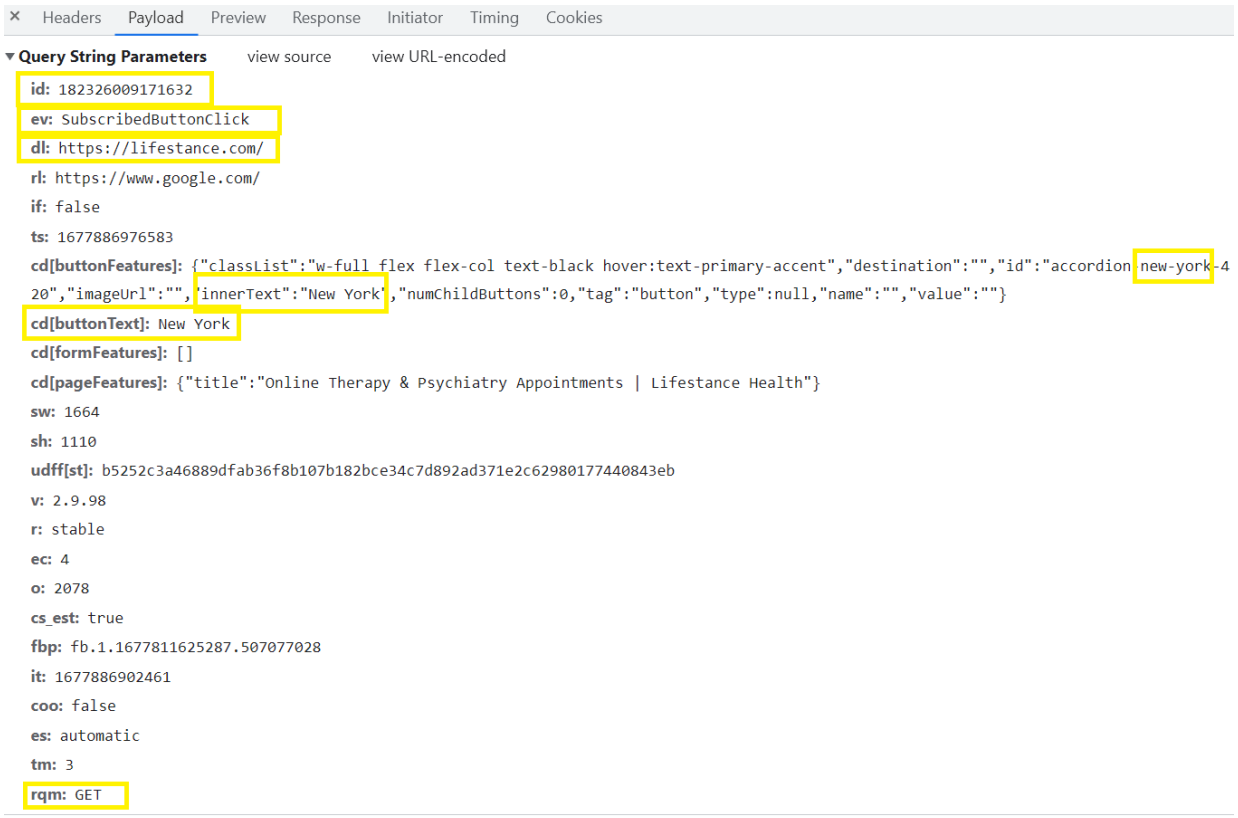


***Figure 5. Defendant's transmission to Facebook of patient's search parameters showing location search terms (New York, NY)***

85. The first line of highlighted text, "id: 182326009171632," refers to the Defendant's Pixel ID for this particular Webpage and confirms that the Defendant has downloaded the Pixel into its Source Code on this particular Webpage.

86. The second line of text, "ev: SubscribedButtonClick," identifies and categorizes which actions the user took on the Webpage ("ev:" is an abbreviation for event, and "SubscribedButtonClick" is the type of event). Thus, this identifies the user as having clicked a

specific button on the particular Webpage to submit search parameters.

87. The remaining lines of text identify: (i) the user as a patient seeking medical care from Defendant via www.lifestance.com; (ii) who is in the process of searching for a provider of online therapy; (iii) who specializes in psychiatry; and (iv) is located in New York, NY.

88. Finally, the last line of highlighted text ("GET"), demonstrates that Defendant's Pixel sent the user's communications, and the Private Information contained therein, alongside the user's personal identifiers including Facebook cookies. This is further evidenced by the images below, which were collected during the same browsing session as the previous image.



***Figures 6 & 7. Defendant's transmission to Facebook of patient's search parameters showing search terms and the patient's personal identifiers (datr and c_user fields).***

104. If the patient uses additional filters, such as Treatment Areas or Provider Gender, those search parameters are also automatically transmitted to Facebook by Defendant's Pixel.

105. For example, selecting "Alcohol and Drug Use Issues" from the "Treatment Areas" causes that information to be sent directly to Facebook, along with the patient's personal identifiers.


***Figure 8. An HTTP single communication session sent from the device to Facebook that reveals the user's search parameters and the patient's personal identifiers.***

106. Once a patient chooses a doctor or books an appointment, all of the information that patient has submitted is automatically sent directly to Facebook. The information transmitted to Facebook includes: (i) the patient's unique and persistent identifiers (including IP address, c_user ID and datr cookie values), (ii) the fact that the patient clicked on a specific provider's profile page, (iii) the patient's search parameters (demonstrating what filters they used, including doctor's specialty and patient's medical conditions), (iv) the patient's location filter and (v) appointment details.

107. Each time Defendant sends this activity data, it also discloses a patient's personally identifiable information alongside the contents of their communications.

108. A user who accesses Defendant's website while logged into Facebook will transmit the c_user cookie to Facebook, which contains that user's unencrypted Facebook ID, and other personal cookie values including the datr and fr cookies.

109. When accessing ww.lifestance.com, for example, Facebook receives as many as eight cookies:

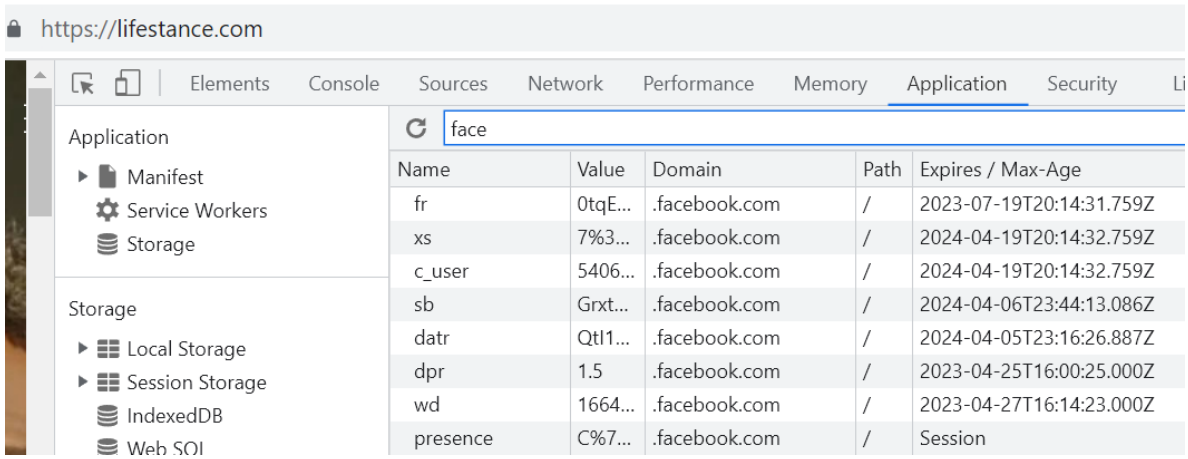


***Figure 9.***

112. When a visitor's browser has recently logged out of an account, Facebook compels the visitor's browser to send a smaller set of cookies[35]:

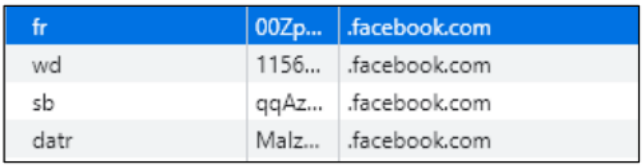


***Figure 10.***

113. The fr cookie contains, at least, an encrypted Facebook ID and browser identifier.[36] Facebook, at a minimum, uses the fr cookie to identify users.[37]

114. At each stage, Defendant also utilized the _fbp cookie, which attaches to a browser

---

[35] The screenshot below serves as an example and demonstrates the types of data transmitted during an HTTP single communication session. Not pictured here and in the preceding image is the _fbp cookie, which is transmitted as a first-party cookie.

[36] Data Protection Commissioner, *Facebook Ireland Ltd: Report of Re-Audit* (Sept. 21, 2012), p. 33, http://www.europe-v-facebook.org/ODPC_Review.pdf (last visited April 18, 2023).

[37] *Cookies & other storage technologies*, FACEBOOK.COM, https://www.facebook.com/policy/cookies/ (last visited April 18, 2023).

as a first-party cookie, and which Facebook uses to identify a browser and a user:[38]

| | | | | |
|---|---|---|---|---|
| _fbp | fb.1.1677811625287.507077028 | .lifestance.com | / | 2023-07-19T20:52:44.000Z |

***Figure 11.***

115. The fr cookie expires after 90 days unless the visitor's browser logs back into Facebook.[39] If that happens, the time resets, and another 90 days begins to accrue.

116. The _fbp cookie expires after 90 days unless the visitor's browser accesses the same website.[40] If that happens, the time resets, and another 90 days begins to accrue.

117. The Facebook Tracking Pixel uses both first- and third-party cookies. A first-party cookie is "created by the website the user is visiting"—i.e., Defendant.[41]

118. A third-party cookie is "created by a website with a domain name other than the one the user is currently visiting"—i.e., Facebook.[42]

119. The _fbp cookie is always transmitted as a first-party cookie. A duplicate _fbp cookie is sometimes sent as a third-party cookie, depending on whether the browser has recently logged into Facebook.

120. Facebook, at a minimum, uses the fr, _fbp, and c_user cookies to link to FIDs and corresponding Facebook profiles.

121. As shown in the above figures, Defendant sent these identifiers with the event data.

122. Plaintiffs never consented, agreed, authorized, or otherwise permitted Defendant to disclose their personally identifiable information and protected health information nor did she

---

[38] *Id.*

[39] *Id.*

[40] *Id.*

[41] *First-Party Cookie*, PCMAG.COM, https://www.pcmag.com/encyclopedia/term/first-party-cookie (last visited April 18, 2023). This is confirmable by using developer tools to inspect a website's cookies and track network activity.

[42] *Third-Party Cookie*, PCMAG.COM, https://www.pcmag.com/encyclopedia/term/third-party-cookie (last visited April 18, 2023). This is also confirmable by tracking network activity.

authorize any assistance with intercepting her communications.

123. Plaintiffs were never provided with any written notice that Defendant disclosed its Website users' PHI nor were they provided any means of opting out of such disclosures.

124. Despite this, Defendant knowingly and intentionally disclosed Plaintiffs' PHI to Facebook.

### *F. LifeStance Does Not Disclose That It Sends Private Information to Third Parties for Marketing Purposes.*

110. LifeStance represents to patients and visitors to its Website that it will only disclose PHI provided to it under certain circumstances, ***none of which apply here***.[43]

111. Defendant's privacy policy does ***not*** permit Defendant to use and disclose Plaintiffs' and Class Members' Private Information for marketing purposes. In fact, LifeStance acknowledges that it must obtain Users' "written authorization" to use or to disclose PHI; "[s]pecific, examples, of uses or disclosures that require written authorization include: Marketing activities (unless an exception applies)."[44]

112. Defendant violated its own privacy policy by unlawfully intercepting and disclosing Plaintiffs' and Class Members' Private Information to Facebook and third parties without adequately disclosing that it shared Private Information with third parties and without acquiring the specific patients' consent or authorization to share the Private Information.

113. The Pixel, which is embedded in and throughout the Website, collects search queries regarding users' personal information including their name and email, their medical conditions, treatment and/or specific providers. Even non-Facebook users can be individually identified via the information gathered on the Web Properties, like an IP address or personal device identifying information.[45]

---

[43] https://lifestance.com/privacy-policy/ (last visited April 15, 2023).

[44] *Id.*

[45] This is precisely the type of information for which HIPAA requires the use of de-identification techniques to protect patient privacy. *See* https://www.hhs.gov/hipaa/for-

### *G. LifeStance's Disclosure of PHI Without Informed Consent Violates HIPAA's Privacy Rule & OCR Guidance.*

114. Beyond Defendant's own policies, and those of Meta, the government has issued guidance warning that tracking code like Meta Pixel may come up against federal privacy law when installed on healthcare websites. The statement, titled *Use of Online Tracking Technologies By HIPAA Covered Entities And Business Associates* (the "Bulletin"), was recently issued by the HHS' Office for Civil Rights ("OCR").[46]

115. Healthcare organizations regulated under the HIPAA may use third-party tracking tools, such as Google Analytics or Meta Pixel, in a limited way, to perform analysis on data key to operations. They are not permitted, however, to use these tools in a way that may expose patients' protected health information to these vendors. The Bulletin explains:

> Regulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. ***For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.***[47]

116. The bulletin discusses the types of harm that disclosure may cause to the patient:

> An impermissible disclosure of an individual's PHI not only violates the Privacy Rule but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft, financial loss, ***discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI.*** Such disclosures can reveal incredibly sensitive information about an individual, ***including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment.*** While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology

---

professionals/privacy/special-topics/de-identification/index.html, HHS.GOV (last visited April 15, 2023).

[46] *Use Of Online Tracking Technologies By HIPAA Covered Entities And Business Associates*, HHS.GOV, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last visited April 15, 2023).

[47] *Id.* (emphasis added).

> vendors, ***because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI only as expressly permitted or required by the HIPAA Privacy Rule.***[48]

117. Plaintiffs and Class members face the precise risks the government is warning about as LifeStance has shared Plaintiffs' and Class Members' search terms about health conditions for which they seek doctors; their contacts with doctors to make appointments; the names of their doctors; the frequency with which they take steps to obtain healthcare for certain conditions; and where they seek medical treatment.

118. This information is, as described by the OCR bulletin, "highly sensitive." The Bulletin goes on to make clear how broad the government's view of protected information is:

> This information might include an individual's medical record number, home or email address, or dates of appointments, as well as an individual's IP address or geographic location, medical device IDs, ***or any unique identifying code.***[49]
>
> ***All such [individually identifiable health information ("IIHI")] collected on a regulated entity's website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, such as IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services.*** This is because, ***when a regulated entity collects the individual's IIHI through its website or mobile app, the information connects the individual to the regulated entity (i.e., it is indicative that the individual has received or will receive health care services or benefits from the covered entity), and thus relates to the individual's past, present, or future health or health care or payment for care.***[50]

119. LifeStance's disclosure of Plaintiffs' and Class Members' Private Information to entities like Facebook violated HIPAA's Privacy Rule, which defines "individually identifiable health information" as "a subset of health information, including demographic information collected from an individual" that is (1) "created or received by a health care provider;" (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

---

[48] *Id.* (emphasis added).

[49] *Id.* (emphasis added).

[50] *Id.* (emphasis added).

provision of health care to an individual;" and either (i) "identifies the individual;" or (ii) "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual." 45 C.F.R. § 160.103.

120. HIPAA prohibits health care providers from "us[ing] or disclos[ing] 'protected health information "except as permitted or required by" the HIPAA Privacy Rule. *See* 45 C.F.R. § 164.502.[51]

121. Consistent with this restriction, HHS has issued marketing guidance that provides, "[w]ith limited exceptions, the [Privacy] Rule requires an individual's written authorization before a use or disclosure of her or her [PHI] can be made for marketing . . . Simply put, a covered entity may not sell [PHI] to a business associate or any other third party for that party's own purposes. Moreover, covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list."[52]

122. Commenting on a June 2022 report discussing the use of the Meta Pixel by hospitals and medical centers, David Holtzman, a health privacy consultant and a former senior privacy adviser in HHS OCR, which enforces HIPAA, stated, "I am deeply troubled by what [the hospitals] are doing with the capture of their data and the sharing of it … It is quite likely a HIPAA violation."[53]

123. Defendant's placing a third-party tracking code on its Web Properties is a violation of Plaintiffs' and Class Members' privacy rights under HIPAA's Privacy Rule. While Plaintiffs does not bring a claim under HIPAA itself, this violation demonstrates LifeStance's

---

[51] Even the fact that an individual is receiving a medical service, *i.e.*, is a patient of a particular entity, can be PHI. The Department of Health and Human Services has instructed health care providers that, while identifying information alone is not necessarily PHI if it were part of a public source such as a phonebook because it is not related to health data, "[i]f such information was listed with health condition, health care provision or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI."

[52] *Marketing*, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/marketing/index.html, HHS.GOV (last visited April 15, 2023).

[53] '*Deeply Troubled*': *Security experts worry about Facebook trackers on hospital sites*, ADVISORY BOARD, https://www.advisory.com/daily-briefing/2022/06/17/data-trackers (last visited April 15, 2023).

wrongdoing relevant to other claims and establishes its duty to maintain patient privacy.

124. Tech companies are under particular scrutiny because they already have access to a massive trove of information about people, which they use to serve their own purposes. For instance, the health data Google collects could eventually help it micro-target advertisements to people with certain health conditions.

125. Policymakers are proactively calling for a revision and potential upgrade of the HIPAA privacy rules out of concern for what might happen as tech companies continue to march into the medical sector.[54]

126. Similarly, a Time Magazine article titled, *How your Medical Data Fuels A Hidden Multi-Billion Dollar Industry*, referenced the "growth of the big health data bazaar," in which patients' health information is sold:

> [T]he secondary market in information unrelated to a patient's direct treatment poses growing risks, privacy experts say. That's because clues in anonymized patient dossiers make it possible for outsiders to determine your identity, especially as computing power advances in the future.[55]

127. LifeStance gave away Plaintiffs' and Class Members' private communications and transactions on its Web Properties without permission. The unauthorized access to Plaintiffs' and Class Members' Private Information has diminished the value of that information, resulting in harm to Users, including Plaintiffs and Class Members.

### *H. Plaintiff's & Class Members' Expectation of Privacy*

136. Plaintiff and Class Members were aware of Defendant's duty of confidentiality when they sought medical services from Defendant.

137. Indeed, at all times when Plaintiff and Class Members provided their PII and PHI to Defendant, they each had a reasonable expectation that the information would remain private and that Defendant would not share the Private Information with third parties for a commercial

---

[54] *Id.*

[55] Adam Tanner, *How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry* (Jan. 9, 2017), TIME, https://time.com/4588104/medical-data-industry/ (last visited April 15, 2023).

purpose, unrelated to patient care.

***I. The Information LifeStance Discloses to Third Parties Is PHI.***

1. IP Addresses are Personally Identifiable Information

138. In addition to patient status, medical conditions, treatment, specific providers, appointment information and patient's unique and persistent Facebook ID, Defendant improperly disclosed patients' computer IP addresses to Facebook through the use of the Pixel.

139. An IP address is a number that identifies the address of a device connected to the Internet.

140. IP addresses are used to identify and route communications on the Internet.

141. IP addresses of individual Internet users are used by Internet service providers, Websites, and third-party tracking companies to facilitate and track Internet communications.

142. Facebook tracks every IP address ever associated with a Facebook user.

143. Facebook, Google and other third-party marketing companies track IP addresses for use in tracking and targeting individual homes and their occupants with advertising by using IP addresses.

144. Under HIPAA, an IP address is considered personally identifiable information.

145. HIPAA defines personally identifiable information to include "any unique identifying number, characteristic or code" and specifically lists the example of IP addresses. *See* 45 C.F.R. § 164.514 (2).

146. HIPAA further declares information as personally identifiable where the covered entity has "actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information." 45 C.F.R. § 164.514(2)(ii); See also, 45 C.F.R. § 164.514(b)(2)(i)(O).

147. Consequently, Defendant's disclosure of patients' IP addresses violated HIPAA and industry privacy standards.

2. Internet Cookies are Personally Identifiable Information

148. In the early years of the Internet, advertising on websites followed the same model as traditional newspapers. Just as a sporting goods store would choose to advertise in the sports

section of a traditional newspaper, advertisers on the early Internet paid for ads to be placed on specific web pages based on the type of content displayed on the web page.

149. Computer programmers eventually developed "cookies"—small text files that web servers can place on a person's web browser and computing device when that person's web browser interacts with the website server. Cookies can perform different functions, like saving a user's login or other site settings. Eventually, some cookies were designed to acquire and record an individual Internet user's communications and activities on websites across the Internet.

150. Cookies are designed to and, in fact, most often do operate as a means of identification for Internet users.

151. Cookies are protected personal identifiers under HIPAA. See 45 C.F.R. § 164.514(b)(2)(i)(H), (J), (M), (N), and (R).

152. In general, cookies are categorized by (1) duration and (2) party.

153. There are two types of cookies classified by duration:

154. "Session cookies" are placed on a user's computing device only while the user is navigating the website that placed and accesses the cookie. The user's web browser typically deletes session cookies when the user closes the browser.

155. "Persistent cookies" are designed to survive beyond a single Internet browsing session. The party creating the persistent cookie determines its lifespan. As a result, a persistent cookie can acquire and record a user's Internet communications for years and over dozens or hundreds of websites. Persistent cookies are sometimes called "tracking cookies."

156. Cookies are also classified by the party that uses the collected data.

157. "First-party cookies" are set on a user's device by the website with which the user is exchanging communications. For example, Rush sets a collection of its own cookies on patients' browsers when they visit any webpage on Rush's web properties. First-party cookies can be helpful to the user, server, and/or website to assist with security, log in, and functionality.

158. "Third-party cookies" are set on a user's device by website servers other than the website or server with which the user is exchanging communications. For example, the same

patient who visits www.rush.edu will also have cookies on their device from third parties, such as Facebook. Unlike first-party cookies, third-party cookies are not typically helpful to the user. Instead, third-party cookies are typically used for data collection, behavioral profiling, and targeted advertising.

159. Data companies like Facebook have developed methods for monetizing and profiting from cookies. These companies use third-party tracking cookies to help them acquire and record user data and communications in order to sell advertising that is customized to that person's communications and habits. To build individual profiles of Internet users, third party data companies assign each user a unique, or a set of unique identifiers to each user.

160. Traditionally, first- and third-party cookies were kept separate. An Internet security policy known as the same-origin policy required web browsers to prevent one web server from accessing the cookies of a separate web server. For example, although LifeStance can deploy source code that uses Facebook third-party cookies to help Facebook acquire and record the patient's communications, it is not permitted direct access to Facebook third-party cookie values. The reverse was also true: Facebook was not provided direct access to the values associated with first party cookies set by LifeStance.

161. Data companies have designed a way to hack around the same-origin policy so that third-party data companies gain access to first-party cookies.

162. Javascript source code developed by third-party data companies and placed on a webpage by a developer such as Rush can bypass the same-origin policy to send a first-party cookie value in a tracking pixel to the third-party data company. This technique is known as "cookie synching," and it allows two cooperating websites to learn each other's cookie identification numbers for the same user. Once the cookie synching operation is completed, the two websites can exchange any information they have collected and recorded about a user that is associated with a cookie identification number. The technique can also be used to track an individual who has chosen to deploy third-party cookie blockers.

163. Whenever a LifeStance patient uses Defendant's Website, LifeStance uses and causes the disclosure of patient cookie identifiers with each re-directed communication

described herein, including patient status, conditions, treatments sought, location, and appointment details.

164. Defendant's cookie disclosures include the deployment of cookie synching techniques that cause the disclosure of the first-party cookie values that LifeStance assigns to patients to be made to third parties.

## REPRESENTATIVE PLAINTIFFS' EXPERIENCES

***Plaintiff Montana Strong's Experience with LifeStance***

128. Plaintiff Strong initially became aware of LifeStance via an advertisement on Facebook.

129. Plaintiff Strong started receiving healthcare services from LifeStance in or about March of 2022 and continued such activity thereafter through early 2023.

130. Plaintiff Strong received those services via Defendant's Website, which she accessed on her phone and computer.

131. Plaintiff Strong used Defendant's Website to communicate with healthcare providers, research particular medical concerns and treatments, fill out forms, schedule and attend appointments and perform other tasks related to her specific medical inquiries and treatment.

132. As a condition of receiving Defendant's services, Plaintiff Strong disclosed her Private Information to Defendant on numerous occasions; but for her status as Defendant's patient, Plaintiff Strong would not have disclosed her Private Information to Defendant.

133. Plaintiff Strong reasonably expected that her communications with Defendant via the Website were confidential, solely between herself and Defendant and that such communications would not be transmitted to or intercepted by a third party.

134. However, and as a result of the Meta Pixel Defendant chose to install on its Website, Plaintiff Strong's Private Information was intercepted, viewed, analyzed and used by unauthorized third parties.

135. Defendant transmitted Plaintiff Strong's Facebook ID, computer IP address and other device and online identifiers to Facebook. Defendant also transmitted information such as

username and password; protected characteristics such as age, gender, race and ethnicity and health and medical information including medical history, the type of medical treatment sought, Plaintiffs' particular health condition, patient status and the fact that Plaintiffs attempted to or did book a medical appointment.

136. Plaintiff Strong never consented to the disclosure of or use of her Private Information by third parties or to Defendant enabling third parties, including Facebook, to access or interpret such information. Plaintiff Strong never consented to any third-parties' receipt or use of her Private Information.

137. Notwithstanding, through the Meta Pixel and similar technologies embedded on Defendant's Website, Defendant transmitted Plaintiff Strong's Private Information to, at a minimum, Facebook and likely many other third parties like Google, TikTok and others.

138. By making these disclosures without her consent, Defendant breached Plaintiff Strong's privacy and unlawfully disclosed her Private Information.

139. Defendant did not inform Plaintiff Strong that it had shared her Private Information with Facebook.

140. Plaintiff Strong used and continues to use the same devices to maintain and to access an active Facebook account throughout the relevant period for this case.

141. Plaintiff Strong has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future unauthorized disclosure(s).

142. Plaintiff Strong would consider using Defendant's services again and/or in greater frequency if she could be assured by Defendant that the violations set forth herein were no longer occurring.

***Plaintiff Debra Yick's Experience with LifeStance***

143. Plaintiff Debra Yick started receiving healthcare services from LifeStance in or about July of 2022 and continued such activity thereafter through early 2023.

144. Plaintiff Yick received those services via Defendant's Website, which she accessed on her phone and computer.

145. Plaintiff Yick used Defendant's Website to communicate with healthcare providers, research particular medical concerns and treatments, fill out forms, schedule and attend appointments and perform other tasks related to her specific medical inquiries and treatment.

146. As a condition of receiving Defendant's services, Plaintiff Yick disclosed her Private Information to Defendant on numerous occasions; but for her status as Defendant's patient, Plaintiff Yick would not have disclosed her Private Information to Defendant.

147. Plaintiff Yick reasonably expected that her communications with Defendant via the Website were confidential, solely between herself and Defendant and that such communications would not be transmitted to or intercepted by a third party.

148. However, and as a result of the Meta Pixel Defendant chose to install on its Website, Plaintiff Yick's Private Information was intercepted, viewed, analyzed and used by unauthorized third parties.

149. Defendant transmitted Plaintiff Yick's Facebook ID, computer IP address and other device and online identifiers to Facebook. Defendant also transmitted information such as username and password; protected characteristics such as age, gender, race and ethnicity and health and medical information including medical history, the type of medical treatment sought, Plaintiffs' particular health condition, patient status and the fact that Plaintiffs attempted to or did book a medical appointment.

150. Plaintiff Yick never consented to the disclosure of or use of her Private Information by third parties or to Defendant enabling third parties, including Facebook, to access or interpret such information. Plaintiff Yick never consented to any third-parties' receipt or use of her Private Information.

151. Notwithstanding, through the Meta Pixel and similar technologies embedded on Defendant's Website, Defendant transmitted Plaintiff Yick's Private Information to, at a minimum, Facebook and likely many other third parties like Google, TikTok and others.

152. By making these disclosures without her consent, Defendant breached Plaintiff Yick's privacy and unlawfully disclosed her Private Information.

153. Defendant did not inform Plaintiff Yick that it had shared her Private Information with Facebook.

154. Plaintiff Yick used and continues to use the same devices to maintain and to access an active Facebook account throughout the relevant period for this case.

155. Plaintiff Yick has a continuing interesting in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future unauthorized disclosure(s).

156. Plaintiff Yick would consider using Defendant's services again and/or in greater frequency if she could be assured by Defendant that the violations set forth herein were no longer occurring.

## TOLLING

157. Any applicable statute of limitations has been tolled by the "delayed discovery" rule as Plaintiffs did not know (and had no way of knowing) that their Private Information was unlawfully disclosed because Defendant did (and has) not disclosed that information. Alternatively, applicable statute of limitations has been tolled by other applicable rules or doctrines.

## CLASS ACTION ALLEGATIONS

158. Plaintiffs bring this action on behalf of themselves and on behalf of various classes of persons similarly situated, as defined below, pursuant to Rule 23(b)(2), 23(b)(3) and 23(c)(4) of the Federal Rules of Civil Procedure.

159. The Nationwide Class that Plaintiffs seek to represent is defined as:

> All individuals residing in the United States whose Private Information was disclosed to a third party without authorization or consent through the Pixel on Defendant's Website.

160. The California Class that Plaintiff Yick seeks to represent is defined as:

> All individuals residing in the State of California whose Private Information was disclosed to a third party without authorization or consent through the Pixel on Defendant's Website.

161. The New York Class that Plaintiff Strong seeks to represent is defined as:

> All individuals residing in the State of New York whose Private

Information was disclosed to a third party without authorization or consent through the Pixel on Defendant's Website and Web Properties.

162. The Nationwide Class, the California Class and the New York Class are referred to collectively as the "Classes." Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign and any Judge who adjudicates this case, including their staff and immediate family.

163. Plaintiffs reserve the right to modify or amend the definition of the proposed Classes before the Court determines whether certification is appropriate.

164. **Numerosity, Fed R. Civ. P. 23(a)(1).** The members of the Classes are so numerous that joinder of all them is impracticable. Upon information and belief, there are over one million individuals whose Private Information may have been improperly accessed by Facebook. The members of each Class are ascertainable and identifiable from Defendant's records.

165. **Commonality & Predominance, Fed. R. Civ. P. 23(a)(2) and (b)(3).** Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant has a duty to protect the PII and PHI of Plaintiffs and Class Members;

b. Whether Defendant owes a duty to not disclose the PII and PHI of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendant violated its privacy policy by disclosing the PII and PHI of Plaintiffs and Class Members to Facebook, Google, and/or other third parties.

d. Whether Defendant adequately, promptly and accurately informed Plaintiffs and Class Members that their PII and PHI would be disclosed to third parties;

e. Whether Defendant violated the law by failing to promptly notify

Plaintiffs and Class Members that their PII and PHI had been compromised;

f. Whether Defendant adequately addressed and fixed the practices which permitted the disclosure of patient PHI and PII;

g. Whether Defendant engaged in unfair, unlawful or deceptive practices by failing to safeguard the PII and PHI of Plaintiffs and Class Members;

h. Whether Defendant violated consumer protection statutes invoked herein;

i. Whether Plaintiffs and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

j. Whether Defendant knowingly made false representations as to its data security and/or privacy policy practices;

k. Whether Defendant knowingly omitted material representations with respect to its data security and/or privacy policy practices; and

l. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of Defendant's disclosure of their PII and PHI.

166. **Typicality, Fed. R. Civ. P. 23(a)(3).** Plaintiffs' claims are typical of those of other Class Members because all had their Private Information compromised as a result of Defendant's use of the Meta Pixel and due to Defendant's misfeasance. Plaintiffs present common claims on behalf of the absent members of the Classes that are not unique but capable of proof by applying common evidence regarding common business practices and policies to common legal theories and claims.

167. **Adequacy, Fed. R. Civ. P. 23(a)(4).** Plaintiffs will fairly and adequately represent and protect the interests of Class Members in that Plaintiffs have no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiffs seek no relief

that is antagonistic or adverse to the Class Members, and the infringement of rights and the damages Plaintiffs have suffered are typical of other Class Members. Plaintiffs have also retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

168. **Superiority and Manageability, Fed. R. Civ. P. 23(b)(3).** Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently and without the unnecessary duplication of evidence, effort and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members who could not individually afford to litigate a complex claim against a large corporation, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, such individual actions would still be economically impractical and impose a burden on the courts.

169. **Policies Generally Applicable to the Class.** This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly, and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

170. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would otherwise gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that

would be recovered; proof of a common course of conduct to which Plaintiffs was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

171. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

172. **Ascertainability & Notice**. Membership in the Classes can be determined by objective records maintained by Defendant and adequate notice can be given to Class Members directly using information maintained in Defendant's records.

173. **Class-wide Injunctive Relief, Fed. R. Civ. P. 23(b)(2).** Unless a Class-wide injunction is issued, Defendant may continue to fail to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the practices complained of herein, and Defendant may continue to act unlawfully as set forth in this Complaint as Defendant has acted or refused to act on grounds generally applicable to the Class. Accordingly, final injunctive or corresponding declaratory relief with regard to the Class as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

174. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- Whether Defendant owes a legal duty to not disclose Plaintiffs' and Class Members' Private Information;
- Whether Defendant owes a legal duty to not disclose Plaintiffs' and Class Members' Private Information under Defendant's privacy policy;
- Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and

safeguarding their Private Information;

- Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;
- Whether Defendant adequately and accurately informed Plaintiffs and Class Members that their Private Information would be disclosed to third parties;
- Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information disclosed to third parties and
- Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

**ARIZONA LAW SHOULD APPLY TO PLAINTIFFS' & CLASS MEMBERS' COMMON LAW CLAIMS**

175. The State of Arizona has a significant interest in regulating the conduct of businesses operating within its borders.

176. Arizona, which seeks to protect the rights and interests of Arizona and all residents and citizens of the United States against a company headquartered and doing business in Arizona, has a greater interest in the claims of Plaintiffs and the Classes than any other state and is most intimately concerned with the claims and outcome of this litigation.

177. The principal place of business and headquarters of LifeStance, located in Scottsdale, Arizona, is the "nerve center" of its business activities—the place where its high-level officers direct, control and coordinate its activities, including major policy, financial and legal decisions.

178. Upon information and good faith belief, Defendant's actions and corporate decisions surrounding the allegations made in the Complaint were made from and in Arizona.

179. Defendant's breaches of duty to Plaintiffs and Class Members emanated from Arizona.

180. Application of Arizona law to the Classes with respect to Plaintiffs' and the Classes' common law claims is neither arbitrary nor fundamentally unfair because, further to choice of law principles applicable to this action, the common law of Arizona applies to the

nationwide common law claims of all Class members. Additionally, given Arizona's significant interest in regulating the conduct of businesses operating within its borders, and that Arizona has the most significant relationship to Defendant, as it is headquartered in Arizona, there is no conflict in applying Arizona law to non-resident consumers such as Plaintiffs and the Class members.

181. Alternatively and/or in addition to Arizona law, the laws set forth below apply to the conduct described herein.

## CLAIMS FOR RELIEF

## COUNT I

### VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT
### Cal. Penal Code §§ 630, *et. Seq*.
### (By Plaintiff Yick on Behalf of the California Class)

182. Plaintiff Yick repeats the allegations contained in the paragraphs above as if fully set forth herein and brings this count individually and on behalf of the California Class.

183. The California Invasion of Privacy Act ("CIPA") is codified at California Penal Code §§ 630 to 638.

184. CIPA represents a fundamental policy of the state of California which cannot be waived or contracted out of.

185. CIPA begins with its statement of purpose.

> The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.

CAL. PENAL CODE § 630.

186. California Penal Code § 631(a) provides, in pertinent part:

> Any person who, by means of any machine, instrument, or contrivance, or in any other manner . . . willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit

> or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars ($2,500)[.]

187. Simply put, a defendant must show it had the consent of ***all*** parties to a communication.

188. At all relevant times, Defendant aided, employed, agreed with, and conspired with Facebook to track and intercept Plaintiffs' and Class Members' internet communications while using Defendant's Website.

189. These communications were intercepted by a third party during the communications and without the knowledge, authorization or consent of Plaintiffs and Class Members.

190. Defendant intentionally inserted an electronic device that, without the knowledge and consent of Plaintiffs and Class members, recorded and transmitted their confidential communications with Defendant to a third party.

191. Defendant willingly facilitated and aided Facebook's interception and collection of Plaintiffs' and Class Members' Private Information by embedding the Pixel(s) on the Website, thereby assisting Facebook's eavesdropping.

192. The following items constitute "machine[s], instrument[s], or contrivance[s]" under the CIPA, and even if they do not, the Pixel falls under the broad catch-all category of "any other manner":

a. The computer codes and programs Facebook used to track Plaintiffs' and Class Members' communications while they were navigating the Website;

b. Plaintiffs' and Class Members' browsers;

c. Plaintiffs' and Class Members' computing and mobile devices;

d. Facebook's web and ad servers;

e. The web and ad servers from which Facebook tracked and intercepted Plaintiffs' and Class Members' communications

while they were using a web browser to access or navigate the Website;

f. The computer codes and programs used by Facebook to effectuate its tracking and interception of Plaintiffs' and Class Members' communications while they were using a browser to visit the Website; and

g. The plan Facebook carried out to effectuate its tracking and interception of Plaintiffs' and Class Members' communications while they were using a web browser or mobile application to visit the Web Properties.

193. Defendant fails to disclose to Users that it is using the Pixel to track and automatically and simultaneously transmit highly sensitive personal communications to a third party. Defendant is necessarily aware that these communications are confidential as its Website Notice of Privacy Practices acknowledges the confidential nature of private medical information and disclaims that it is being shared with unidentified third parties without Plaintiffs' and Class Members' express authorization.

194. The patient communication information that Defendant transmits while using the Pixel constitutes protected health information.

195. As demonstrated herein, Defendant violates CIPA by aiding and permitting third parties to receive its patients' online communications in real time through its Web Properties without their consent.

196. By disclosing Plaintiffs' and Class Members' private health information, Defendant violated Plaintiffs' and Class Members' statutorily protected right to privacy.

197. As a result of the above violations and pursuant to CIPA Section 637.2, Defendant is liable to Plaintiffs and Class Members for treble actual damages related to their loss of privacy in an amount to be determined at trial, or for statutory damages in the amount of $5,000 per violation. Section 637.2 specifically states that "[i]t is not a necessary prerequisite to an action pursuant to this section that the Plaintiffs has suffered, or be threatened with, actual damages."

198. Under the statute, Defendant is also liable for reasonable attorney's fees, litigation costs, injunctive and declaratory relief, and punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by the Defendant in the future.

199. Based on the foregoing, Plaintiffs and California Class Members seek all other

relief as the Court may deem just and proper, including all available monetary relief, injunctive and declaratory relief, any applicable penalties, and reasonable attorneys' fees and costs.

## COUNT II

### VIOLATION OF THE CONFIDENTIALITY OF MEDICAL INFORMATION ACT
### Cal. Civ. Code §§ 56, *et seq*.
### (By Plaintiff Yick on behalf of the California Class)

200. Plaintiff Yick repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the California Class.

201. The California Confidentiality of Medical Information Act, California Civil Code §§ 56, et seq. ("CMIA") prohibits health care providers from disclosing medical information relating to their patients without patient authorization.

202. "Medical information" refers to "any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care . . . regarding a patient's medical history, mental or physical condition, or treatment. 'Individually Identifiable' means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual[.]" Cal. Civ. Code § 56.05.

203. Defendant is a "provider of health care" as defined by California Civil Code § 56.06(b).

204. Plaintiffs and Class Members are patients, and, as a health care provider, Defendant has an ongoing obligation to comply with the CMIA's requirements.

205. As set forth above, device identifiers, web URLs, Internet Protocol (IP) addresses and other characteristics that can uniquely identify Plaintiffs and Class Members are transmitted to Defendant in combination with patient medical conditions, medical concerns, treatment(s) sought by the patients, medical history and other medical information. This is protected health information under the CMIA.

206. This private medical information is intercepted and transmitted to Facebook via Defendant's use of enabling software into its Website. Facebook ID is also an identifier

sufficient to allow identification of an individual. Along with patients' Facebook ID, Defendant discloses to Facebook several pieces of information regarding patient use of its Web Properties, including but not limited to the following: patient medical conditions, medical concerns, treatment(s) sought by the patients, medical specialty of the doctor(s) searched for and selected by patients and appointment information.

207. The information described above constitutes medical information pursuant to the CMIA because it is patient information derived from a provider of health care regarding patients' medical treatment and physical condition, and this medical information is linked with individually identifying information. *See* CAL. CIV. CODE § 56.05(i).

208. As demonstrated herein, Defendant fails to obtain its patients' authorization for the disclosure of medical information and fails to disclose in its Privacy Policy (available at: https://lifestance.com/privacy-policy/)(last visited April 18, 2023) that it shares protected health information with Facebook or other third parties for marketing purposes.

209. Pursuant to CMIA Section 56.11, a valid authorization for disclosure of medical information must be: (1) "Clearly separate from any other language present on the same page and is executed by a signature which serves no other purpose than to execute the authorization;" (2) signed and dated by the patient or her representative; (3) state the name and function of the third party that receives the information; and (4) state a specific date after which the authorization expires. Further, the Website Notice of Privacy Practices does not require consumers to agree to them by selecting or clicking a "checkbox" presented in a sufficiently conspicuous manner to put Plaintiffs on notice of them. Accordingly, the information set forth in Defendant's Website Privacy Notice do not qualify as a valid authorization.

210. As described above, Defendant is violating the CMIA by disclosing its patients' medical information to Facebook along with the patients' individually identifying information. Accordingly, Plaintiffs and Class Members seek all relief available for Defendant's CMIA violations.

211. Based on the foregoing, Plaintiffs and Class Members seek nominal damages, compensatory damages, punitive damages, attorneys fees and costs of litigation for Defendant's

violation(s) of the CMIA.

## COUNT III

### VIOLATIONS OF ELECTRONIC COMMUNICATIONS PRIVACY ACT
### 18 U.S.C. § 2511(1), *et seq*.
### Unauthorized Interception, Use and Disclosure
### (By Plaintiffs Strong and Yick on behalf of the Nationwide Class)

212. Plaintiffs repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and bring this claim individually and on behalf of the proposed Nationwide Class.

213. The ECPA protects both sending and receipt of communications.

214. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

215. The transmissions of Plaintiffs' PII and PHI to Defendant's Website qualifies as a "communication" under the ECPA's definition of 18 U.S.C. § 2510(12).

216. Electronic Communications. The transmission of PII and PHI between Plaintiffs and Class Members and Defendant's Web Properties with which they chose to exchange communications are "transfer[s] of signs, signals, writing, . . . data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(2).

217. Content. The ECPA defines content, when used with respect to electronic communications, to "include[] ***any information concerning the substance, purport, or meaning of that communication***." 18 U.S.C. § 2510(8) (emphasis added).

218. Interception. The ECPA defines an interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device" and "contents . . . include any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(4), (8).

219. Electronical, Mechanical, or Other Device. The ECPA defines "electronic,

mechanical, or other device" as "any device … which can be used to intercept a[n] … electronic communication[.]" 18 U.S.C. § 2510(5).

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

a. Plaintiffs' and Class Members' browsers;

b. Plaintiffs' and Class Members' computing devices;

c. Defendant's web-servers; and,

d. The Pixel Code deployed by Defendant to effectuate sending and acquiring patient communications.

221. By utilizing and embedding the Pixel on its Web Properties, Defendant intentionally intercepted, endeavored to intercept, and/or procured another person to intercept, the electronic communications of Plaintiffs and Class Members, in violation of 18 U.S.C. § 2511(1)(a).

222. Specifically, Defendant intercepted Plaintiffs' and Class Members' electronic communications via the Meta Pixel, which tracked, stored, and unlawfully disclosed Plaintiffs' and Class Members' Private Information to third parties such as Facebook.

223. Defendant intercepted communications that include, but are not limited to, communications to/from Plaintiffs and Class Members regarding PII and PHI, treatment, medication, and scheduling.

224. By intentionally disclosing or endeavoring to disclose Plaintiffs' and Class Members' electronic communications to affiliates and other third parties, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

225. By intentionally using, or endeavoring to use, the contents of Plaintiffs' and Class Members' electronic communications, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

226. Unauthorized Purpose. Defendant intentionally intercepted the contents of

Plaintiffs' and Class Members' electronic communications for the purpose of committing a tortious act in violation of the Constitution or laws of the United States or of any State – namely, invasion of privacy, among others.

227. Defendant used the wire or electronic communications to increase its profit margins. Defendant specifically used the Pixel to track and utilize Plaintiffs' and Class Members' PII and PHI for financial gain.

228. Defendant was not acting under color of law to intercept Plaintiffs' and the Class Members' wire or electronic communication.

229. Plaintiffs and Class Members did not authorize Defendant to acquire the content of their communications for purposes of invading Plaintiffs' privacy via the Pixel tracking code.

230. Any purported consent that Defendant received from Plaintiffs and Class Members was not valid.

231. In sending and in acquiring the content of Plaintiffs' and Class Members' communications relating to the browsing of Defendant's Website, Defendant's purpose was tortious, criminal, and designed to violate federal and state legal provisions including a knowing intrusion into a private place, conversation, or matter that would be highly offensive to a reasonable person.

232. A person who violates § 2511(1)(a) is liable for $10,000 in statutory damages to any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used.

233. For the same reasons as set forth above for Plaintiffs' CIPA Claims, Defendant is liable to Plaintiffs and Class Members for violations of the ECPA.

234. Based on the foregoing, Plaintiffs and Nationwide Class Members seek all other relief as the Court may deem just and proper, including all available monetary relief, injunctive and declaratory relief, any applicable penalties, and reasonable attorneys' fees and costs.

## COUNT IV

**VIOLATIONS OF ELECTRONIC COMMUNICATIONS PRIVACY ACT**
**18 U.S.C. § 2511(3)(a), *et seq*.**
**Unauthorized Divulgence by Electronic Communications Service**
**(By Plaintiffs Strong and Yick on behalf of the Nationwide Class)**

235. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully set forth herein and bring this claim individually and on behalf of the Nationwide Class.

236. The ECPA Wiretap statute provides that "a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient." 18 U.S.C. § 2511(3)(a).

237. Electronic Communication Service. An "electronic communication service" is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

238. Defendant's Web Properties are electronic communication services. The Web Properties provide Users the ability to send or receive electronic communications. In the absence of Defendant's Web Properties, internet users could not send or receive communications regarding Plaintiffs' and Class Members' PII and PHI.

239. Intentional Divulgence. Defendant intentionally utilized the Tracking Pixel and was, or should have been aware, that it could divulge Plaintiffs' and Class Members' PII and PHI.

240. While in Transmission. Upon information and belief, divulgence of the contents of Plaintiffs' and Class Members' communications was contemporaneous with their exchange with Defendant's Web Properties, to which they directed their communications.

241. Defendant divulged the contents of Plaintiffs' and Class Members' communications to Facebook or other third parties without Plaintiffs' and Class Members' consent and/or authorization.

242. Exceptions do not apply. In addition to the exception for communications directly to an ECS or an agent of an ECS, the Wiretap Act states that "[a] person or entity providing electronic communication service to the public may divulge the contents of any such communication as follows:

a. "as otherwise authorized in section 2511(2)(a) or 2517 of this title;"

b. "with the lawful consent of the originator or any addressee or intended recipient of such communication;"

c. "to a person employed or authorized, or whose facilities are used, to forward such communication to its destination;" or

d. "which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency." 18 U.S.C. § 2511(3)(b).

243. Section 2511(2)(a)(i) provides: "It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks."

244. Defendant's divulgence of the contents of Plaintiffs' and Class Members' communications on Defendant's Web Properties to a third party was not authorized by 18 U.S.C. § 2511(2)(a)(i) in that it was neither: (1) a necessary incident to the rendition of Defendant's service; nor (2) necessary to the protection of the rights or property of Defendant.

245. Defendant's divulgence of the contents of user communications on Defendant's browser through the Pixel code was not done "with the lawful consent of the originator or any addresses or intended recipient of such communication[s]." As alleged above: (a) Plaintiffs and Class Members did not authorize Defendant to divulge the contents of their communications; and (b) Defendant did not procure the "lawful consent" from the Websites or apps with which

Plaintiffs and Class Members were exchanging information.

246. Moreover, Defendant divulged the contents of Plaintiffs' and Class Members' communications through the Meta Pixel to individuals who are not "person[s] employed or whose facilities are used to forward such communication to its destination."

247. The contents of Plaintiffs' and Class Members' communications did not appear to pertain to the commission of a crime and Defendant did not divulge the contents of their communications to a law enforcement agency.

248. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages; preliminary and other equitable or declaratory relief as may be appropriate; and reasonable attorneys' fees and other litigation costs reasonably incurred.

249. A person who violates § 2511(3)(a) is liable for $10,000 in statutory damages to any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used.

250. For the same reasons as set forth above for Plaintiffs' CIPA Claims, Defendant is liable to Plaintiffs and Class Members for violations of the ECPA.

251. Based on the foregoing, Plaintiffs and Nationwide Class Members seek all other relief as the Court may deem just and proper, including all available monetary relief, injunctive and declaratory relief, any applicable penalties, and reasonable attorneys' fees and costs.

.

## COUNT V

### VIOLATION OF THE UNFAIR COMPETITION LAW
### Cal. Bus. & Prof. Code § 17200, *et seq.* – Unlawful Business Practices
### (By Plaintiff Yick on behalf of the California Class)

252. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the California Class.

253. Plaintiff Yick, California Class Members and Defendant are each a "person" under Cal. Bus. & Prof. Code § 17201.

254. The acts, omissions and conduct of Defendant as alleged herein constitute "business practices" within the meaning of the UCL.

255. California Business and Professions Code §§ 17201, *et seq.*, prohibits acts of unfair competition, which includes unlawful business practices.

256. Plaintiff Yick brings her claim for injunctive relief as she has no confidence that Defendant has altered its privacy practices and she may wish to use Defendant's services in the future.

257. Plaintiff Yick brings her claim for restitution in the alternative to her claims for damages.

258. Defendant engaged in unlawful business practices by disclosing Plaintiff Yick's and California Class Members' Private Information to unrelated third parties, including Facebook, without prior consent in violation of the consumer protection and privacy statutes alleged herein.

259. Defendant's unlawful acts and practices include violations of Plaintiff Yick's and Class Member's constitutional rights to privacy; Cal. Penal Code §§ 630, *et. seq.* ; Cal. Civ. Code §§ 56, *et. seq.* ; 18 U.S.C. § 2511(1), *et seq.*; 18 U.S.C. § 2511(3)(a), *et seq.*; and 18 U.S.C. § 1030, *et seq.*

260. Because Defendant is in the business of providing medical and mental healthcare services, Plaintiff Yick and California Class Members relied on Defendant to advise them of any potential disclosure of their private information.

261. Plaintiff Yick and California Class Members were entitled to assume (and did assume) that Defendant would take appropriate measures to keep their private information private and confidential.

262. Plaintiff Yick viewed and relied upon Defendant's representations in its privacy policies concerning the confidentiality of information provided by patients like Plaintiff Yick and California Class Members to Defendant.

263. Defendant's failure to disclose that it was sharing Private Information with third-parties constitutes a material omission of fact.

264. Defendant was in sole possession of and had a duty to disclose the material information that Plaintiff Yick's and California Class Members' Private Information was being

shared with a third party.

265. Defendant also had a duty to disclose the material information that Plaintiff Yick's and California Class Members' Private Information was being shared with a third party as: a) Defendant had superior knowledge of such facts and Plaintiff Yick and California Class Members had no other way to obtain the information; b) by reason of its status as a provider of medical and mental healthcare services, Defendant was in a special relationship with Plaintiff Yick and California Class Members - Medical providers have a duty to keep patients' non-public medical information completely confidential; c) the facts not disclosed relate to health and safety of Plaintiff Yick and California Class Members; d) Defendant made certain affirmative statements regarding its privacy policy but failed to disclose all material facts (including that it was sharing Private Information with third-parties as described herein) making its partial disclosures misleading.

266. Had Defendant disclosed that it shared Private Information with third parties, Plaintiff Yick would not have used Defendant's services or would have paid considerably less for those services.

267. The harm caused by Defendant's conduct outweighs any potential benefits attributable to such conduct and there were reasonably available alternatives to further Defendant's legitimate business interests other than the conduct described herein.

268. As a direct result of their reliance on Defendant's representations that it would keep personal information confidential, Plaintiffs and California Class Members shared highly sensitive information through their use of the Website, causing them to suffer damages when Defendant disclosed that information to a third party.

269. Plaintiff Yick requests appropriate injunctive and declaratory relief against the continuation of the practices described herein and complained of. Such relief will create a pubic benefit. Plaintiff Yick separately seeks public injunctive relief on behalf of the general public of California who have yet to deal with Defendant in the manner described herein, but are likely to in the future, and therefore, are in need of protection provided by the public injunctive relief sought. Such public injunctive relief will create additional public benefits.

270. As a direct result of Defendant's violations of the UCL, Plaintiff Yick and California Class Members have suffered injury in fact and lost money or property including, but not limited to, payments to Defendant and/or other valuable consideration, such as access to their private and personal data. The unauthorized access to Plaintiff Yick's and California Class Members' private and personal data also diminished the value of that information.

271. As a direct result of its unlawful practices, Defendant has been unjustly enriched and should be required to make restitution to Plaintiff Yick and California Class Members pursuant to §§ 17203 and 17204 of the California Business & Professions Code, disgorgement of all profits accruing to Defendant because of its unlawful business practices, declaratory relief, attorney's fees and costs (pursuant to Cal. Code Civ. Proc. §1021.5) and injunctive or other equitable relief.

## COUNT VI

### VIOLATION OF THE UNFAIR COMPETITION LAW ("UCL")
### Cal. Bus. & Prof. Code § 17200, *et seq*. – Unfair Prong
### (By Plaintiff Yick on behalf of the California Class)

272. Plaintiff Yick repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the California Class.

273. Defendant engaged in unfair business practices by disclosing Plaintiff Yick's and California Class Members' Private Information to unrelated third parties, including Facebook, without prior consent despite its promises to keep such information confidential.

274. Defendant's unfair business practices included widespread violations of Plaintiff Yick's and California Class Members' rights to privacy, including its failure to inform the public that using its Website would result in disclosing very private information to a third party.

275. Because Defendant is in the business of providing medical and mental healthcare services, Plaintiff Yick and California Class Members relied on Defendant to advise them of any potential disclosure of their Private Information.

276. Plaintiff Yick and California Class Members were entitled to assume, and did assume, that Defendant would take appropriate measures to keep their Private Information

secure and confidential.

277. Plaintiff Yick viewed and relied upon Defendant's representations in its privacy policies concerning the confidentiality of information provided by patients to Defendant.

278. Defendant was in sole possession of and had a duty to disclose the material information that Plaintiff Yick's and Class Members' private information was being shared with a third party.

279. Had Defendant disclosed that it shared Private Information with third parties, Plaintiff Yick would not have used Defendant's services or would have paid considerably less for those services.

280. The harm caused by the Defendant's conduct outweighs any potential benefits attributable to such conduct and there were reasonably available alternatives to further Defendant's legitimate business interests other than Defendant's conduct described herein.

281. Defendant's acts, omissions and conduct also violate the unfair prong of the UCL because those acts, omissions and conduct offended public policy (including the aforementioned federal and state privacy statutes and state consumer protection statutes, such as HIPAA and CIPA, the ECPA, and CFAA, and constitute immoral, unethical, oppressive, and unscrupulous activities that caused substantial injury, including to Plaintiff Yick and California Class Members.

282. As a direct result of their reliance on Defendant's representations that it would keep personal information confidential, Plaintiff Yick and California Class Members shared highly sensitive information through their use of the Website, causing them to suffer damages when Defendant disclosed that information to a third party.

283. As a direct result of Defendant's violations of the UCL, Plaintiff Yick and California Class Members have suffered injury in fact and lost money or property, including but not limited to payments to Defendant and/or other valuable consideration. The unauthorized access to Plaintiff Yick's and California Class Members' private and personal data also diminished the value of that information.

284. As a direct result of its unfair practices, Defendant has been unjustly enriched and

should be required to make restitution to Plaintiff Yick and California Class Members pursuant to §§ 17203 and 17204 of the California Business & Professions Code, disgorgement of all profits accruing to Defendant because of its unlawful business practices, declaratory relief, attorney's fees and costs (pursuant to Cal. Code Civ. Proc. §1021.5) and injunctive or other equitable relief.

## COUNT VII

## VIOLATION OF ARIZONA CONSUMER FRAUD ACT, A.R.S. §44-1521 *et seq.*
## (On behalf of Plaintiffs & the Nationwide Class)

285. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the Nationwide Class.

286. The Arizona Consumer Fraud Act, A.R.S. 44-1521 *et seq.,* prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the state of Arizona.

287. A.R.S. § 44-1522 provides in pertinent part:

> (a) The act, use or employment by any person of any deception, deceptive or unfair act or practice, fraud, false pretense, false promise, misrepresentation, or concealment, suppression or omission of any material fact with intent that others rely on such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise whether or not any person has in fact been misled, deceived or damaged thereby, is declared to be an unlawful practice.. By the acts and conduct alleged herein, Defendant was selling or advertising merchandise as those terms are defined in A.R.S. § 44-1521.

288. By the acts and conduct alleged herein, Defendant committed unfair or deceptive acts and practices in and from Arizona, in violation of the Arizona Consumer Fraud Act, by:

a. promising to maintain the privacy and security of Plaintiffs' and Class Members' protected health information as required by law;

b. installing the Facebook Pixel to operate as intended and transmit Plaintiffs' and Class Members' Private Information without their authorization to Facebook;

c. failing to disclose or omitting material facts to Plaintiffs and Class Members regarding the disclosure of their Private Information to Facebook;

d. failing to take proper action to ensure the Pixel was configured

to prevent unlawful disclosure of Plaintiffs' and Class Members' Private Information;

e. unlawfully disclosing Plaintiffs' and Class Members' Private Information to Facebook.

289. Defendant knew or should have known that its conduct was of the nature prohibited by A.R.S. § 44-1522, *et seq.*

290. Defendant's actions also constitute deceptive and unfair acts or practices because Defendant knew it failed to disclose to Plaintiffs and Class Members that their healthcare related communications via the Website would be disclosed to Facebook.

291. Defendant's actions also constitute deceptive and unfair acts or practices because Defendant intended that Plaintiffs and Class Members rely on its deceptive and unfair acts and practices and the concealment and omission of material facts in connection with Defendant's offering of goods, merchandise and services.

292. Specifically, Defendant was aware that Plaintiffs and Class Members depended and relied upon it to keep their communications confidential and Defendant instead disclosed that information to Facebook.

293. Contrary to its duties as a medical provider and its express promises of confidentiality, Defendant deployed the Pixel to disclose and transmit Plaintiffs' personally identifiable, non-public medical information, and the contents of her communications exchanged with Defendant to third parties, *i.e.*, Facebook.

294. Defendant's disclosures of Plaintiffs' and Class Members' Private Information were made without their knowledge, consent, or authorization, and were unprivileged.

295. The harm arising from a breach of provider-patient confidentiality includes erosion of the essential confidential relationship between the healthcare provider and the patient.

296. Defendant willfully, knowingly, intentionally, and voluntarily engaged in the aforementioned acts when it incorporated the Facebook Pixel with knowledge of the Pixel's purpose and functionality.

297. The harm described herein could not have been avoided by Plaintiffs and Class Members through the exercise of ordinary diligence.

298. As a result of Defendant's actions, Plaintiffs and Nationwide Class Members have suffered harm and injury.

299. Defendant's conduct complained of is ongoing. Injunctive and declaratory relief is necessary and appropriate to prevent further violations.

300. Plaintiffs and Nationwide Class Members have been damaged as a direct and proximate result of Defendant's invasion of their privacy and are entitled to just compensation, including monetary damages.

301. Plaintiffs and Nationwide Class Members seek appropriate relief for these injuries, including but not limited to damages that will reasonably compensate Plaintiffs and Nationwide Class Members for the harm to their privacy interests as a result of Defendant's violation of the Arizona Consumer Fraud Act.

302. Plaintiffs and Nationwide Class Members seek all other relief as the Court may deem just and proper, including all available monetary relief, injunctive and declaratory relief, any applicable penalties, and reasonable attorneys' fees and costs.

## COUNT VIII

### VIOLATIONS OF NEW YORK GENERAL BUSINESS LAW
### N.Y. Gen. Bus. Law § 349, *et seq.*
### (On Behalf of Plaintiff Strong & the New York Subclass)

303. Plaintiff Strong fully incorporates by reference all of the above paragraphs, as though fully set forth herein and brings this claim individually and on behalf of the New York Class.

304. New York General Business Law § 349 prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the state of New York.

305. GBL §349(a) provides:

> (a) Deceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state are hereby declared unlawful.

306. By reason of the conduct alleged herein, Defendant engaged in unlawful practices

within the meaning of the N.Y. Gen. Bus. Law § 349.

307. The conduct alleged herein are "acts or practices in the conduct of any business" within the meaning of the N.Y. Gen. Bus. Law § 349.

308. By the acts and conduct alleged herein, Defendant committed deceptive acts and practices in violation of the N.Y. Gen. Bus. Law § 349, by:

a. promising to maintain the privacy and security of Plaintiffs' and Class Members' protected health information as required by law;

b. installing the Facebook Pixel to operate as intended and transmit Plaintiffs' and Class Members' Private Information without their authorization to Facebook;

c. failing to disclose or omitting material facts to Plaintiffs and Class Members regarding the disclosure of their Private Information to Facebook;

d. failing to take proper action to ensure the Pixel was configured to prevent unlawful disclosure of Plaintiffs' and Class Members' Private Information and

e. unlawfully disclosing Plaintiffs' and Class Members' Private Information to Facebook.

309. Defendant knew or should have known that its conduct was of the nature prohibited by N.Y. Gen. Bus. Law § 349.

310. Defendant's actions also constitute deceptive and unfair acts or practices because Defendant knew it failed to disclose to Plaintiff Strong and New York Class Members that their healthcare related communications via the Website would be disclosed to Facebook.

311. Defendant's actions also constitute deceptive and unfair acts or practices because Defendant intended that Plaintiff Strong and New York Class Members rely on its deceptive and unfair acts and practices and the concealment and omission of material facts in connection with Defendant's offering of goods, merchandise and services.

312. Specifically, Defendant was aware that Plaintiff Strong and New York Class Members depended and relied upon it to keep their communications confidential and Defendant instead disclosed that information to Facebook.

313. Contrary to its duties as a medical provider and its express promises of confidentiality, Defendant deployed the Pixel to disclose and transmit Plaintiff Strong's

personally identifiable, non-public medical information, and the contents of her communications exchanged with Defendant to third parties, *i.e.*, Facebook.

314. Defendant's disclosures of Plaintiff Strong's and New York Class Members' Private Information were made without their knowledge, consent, or authorization, and were unprivileged.

315. The harm arising from a breach of provider-patient confidentiality includes erosion of the essential confidential relationship between the healthcare provider and the patient.

316. Defendant willfully, knowingly, intentionally, and voluntarily engaged in the aforementioned acts when it incorporated the Facebook Pixel with knowledge of the Pixel's purpose and functionality.

317. The harm described herein could not have been avoided by Plaintiff Strong and New York Class Members through the exercise of ordinary diligence.

318. As a result of Defendant's actions, Plaintiff Strong and New York Class Members have suffered harm and injury.

319. Defendant's conduct complained of is ongoing. Injunctive and declaratory relief is necessary and appropriate to prevent further violations.

320. Plaintiff Strong and New York Class Members have been damaged as a direct and proximate result of Defendant's invasion of their privacy and are entitled to just compensation, including monetary damages.

321. Plaintiff Strong and New York Class Members seek appropriate relief for these injuries, including but not limited to damages that will reasonably compensate Plaintiffs and New York Class Members for the harm to their privacy interests as a result of Defendant's violation of the N.Y. Gen. Bus. Law § 349.

322. Based on the foregoing, Plaintiff Strong and New York Class Members seek all other relief as the Court may deem just and proper, including all available monetary relief, injunctive and declaratory relief, any applicable penalties, and reasonable attorneys' fees and costs.

## COUNT IX

### COMMON LAW INVASION OF PRIVACY – INTRUSION UPON SECLUSION
**(By Plaintiffs Strong and Yick on behalf of the Nationwide Class)**

323. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the Nationwide Class.

324. Plaintiffs and Nationwide Class Members had a reasonable expectation of privacy in their communications with Defendant via its Website and the communication platforms and services therein.

325. Plaintiffs and Nationwide Class Members communicated sensitive and protected medical information and individually identifiable information that they intended for only Defendant to receive and that they understood Defendant would keep private.

326. Defendant's disclosure of the substance and nature of those communications to third parties without the knowledge and consent of Plaintiffs and Nationwide Class Members is an intrusion on Plaintiffs' and Nationwide Class Members' solitude or seclusion.

327. Plaintiffs and Nationwide Class Members had a reasonable expectation of privacy because Defendant's Web Notice of Privacy Practices states that they can expect such privacy.

328. Moreover, Plaintiffs and Nationwide Class Members have a general expectation that their communications regarding healthcare with their healthcare providers will be kept confidential.

329. Defendant's disclosure of private medical information coupled with individually identifying information is highly offensive to the reasonable person.

330. As a result of Defendant's actions, Plaintiffs and Nationwide Class Members have suffered harm and injury, including but not limited to an invasion of their privacy rights.

331. Plaintiffs and Nationwide Class Members have been damaged as a direct and proximate result of Defendant's invasion of their privacy and are entitled to just compensation, including monetary damages.

332. Based on the foregoing, Plaintiffs and Nationwide Class Members seek appropriate relief for these injuries, including but not limited to damages that will reasonably

compensate Plaintiffs and Nationwide Class Members for the harm to their privacy interests as a result of the intrusion(s) upon Plaintiffs' and Nationwide Class Members' privacy.

333. Based on the foregoing, Plaintiffs and Nationwide Class Members seek all other relief as the Court may deem just and proper.

## COUNT X

### BREACH OF CONFIDENCE
### (By Plaintiffs Strong & Yick on behalf of the Nationwide Class)

334. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully set forth herein and bring this claim individually and on behalf of the Nationwide Class.

335. Medical providers have a duty to keep patients' non-public medical information completely confidential.

336. Plaintiffs and Nationwide Class Members had reasonable expectations of privacy in their communications exchanged with Defendant, including communications exchanged on Defendant's Website, because Defendant is in the business of providing medical and mental health care.

337. Plaintiffs' and Nationwide Class Members' reasonable expectations of privacy in the communications exchanged with Defendant are further supported by Defendant's express promises in its Privacy Policies.

338. In breach of its duties as a medical provider and its express promises of confidentiality, Defendant deployed the Meta Pixel to disclose and transmit Plaintiffs' and Nationwide Class Members' Private Information and the contents of private healthcare communications exchanged with Defendant to third parties, including Facebook.

339. Defendant's disclosures of Plaintiffs' and Nationwide Class Members' Private Information were made without their knowledge, consent or authorization, and were unprivileged.

340. As a direct result of Defendant's breach of provider-patient confidentiality, Defendant eroded the essential confidential relationship between a healthcare provider and patient.

341. As a direct and proximate cause of Defendant's unauthorized disclosures of patient personally identifiable, non-public medical information and communications, Plaintiffs and Nationwide Class members were damaged, including the following:

a. Sensitive and confidential information that Plaintiffs and Nationwide Class Members intended to remain private is no longer private;

b. Defendant eroded the essential confidential nature of the provider-patient relationship;

c. Defendant took something of value from Plaintiffs and Nationwide Class Members and derived benefit therefrom without Plaintiffs' and Nationwide Class Members' knowledge or informed consent and without compensating Plaintiffs and Nationwide Class Members for the data;

d. Plaintiffs and Nationwide Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality;

e. Defendant's actions diminished the value of Plaintiffs' and Nationwide Class Members' Private Information and

f. Defendant's actions violated the property rights Plaintiffs and Nationwide Class Members have in their Private Information.

**342.** Based on the foregoing, Plaintiffs and Nationwide Class Members are therefore entitled to general damages for invasion of their rights in an amount to be determined by a jury and nominal damages for each independent violation.

**WHEREFORE**, Plaintiffs Montana Strong and Debra Yick respectfully pray for judgment in their favor and against Defendant LifeStance as follows on all Counts where such relief is applicable:

A. For an Order certifying the Classes (as defined herein) and appointing Plaintiffs as Class Representatives and Plaintiffs' counsel as Class Counsel;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage and safety, and to disclose with

specificity the type of PII and PHI disclosed to third parties;

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

E. For an award of actual damages, compensatory damages, statutory damages and statutory penalties, in an amount to be determined, as allowable by law;

F. For an award of punitive damages, as allowable by law;

G. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

H. Pre- and post-judgment interest on any amounts awarded and

I. Such other and further relief as this Honorable Court may deem just and proper.

**DEMAND FOR JURY TRIAL**

Plaintiffs Montana Strong and Debra Yick hereby demand that this matter be tried to a jury on all Counts that permit trial by jury.

Respectfully submitted,

**ZIMMERMAN REED LLP**

Dated: April 21, 2023

By: s/ Hart L. Robinovitch

Hart L. Robinovitch (AZ SBN 020910)
14646 North Kierland Blvd., Suite 145
Scottsdale, AZ 85254
Telephone: (480) 348-6400
Facsimile: (480) 348-6415
Email: hart.robinovitch@zimmreed.com

**ALMEIDA LAW GROUP LLC**
David S. Almeida (*pro hac vice forthcoming*)
Elena A. Belov (*pro hac vice* forthcoming)
849 W. Webster Avenue
Chicago, Illinois 60614
Tel: (312) 576-3024
david@almeidalawgroup.com
elena@almeidalawgroup.com

*Attorneys for Plaintiffs & the Classes*

# ClassAction.org