

1 Hart L. Robinovitch (AZ SBN 020910)
2 Ryan J. Ellersick (AZ SBN 038805)
3 **ZIMMERMAN REED LLP**
4 14648 N. Scottsdale Road, Suite 130
5 Scottsdale, AZ 85254
6 Telephone: (480) 348-6400
7 Facsimile: (480) 348-6415
8 hart.robinovitch@zimmreed.com
9 ryan.ellersick@zimmreed.com

6 David S. Almeida (*pro hac vice*)
7 Elena A. Belov (*pro hac vice*)
8 **ALMEIDA LAW GROUP LLC**
9 849 W. Webster Avenue
10 Chicago, Illinois 60614
11 Tel: (312) 576-3024
12 david@almeidalawgroup.com
13 elena@almeidalawgroup.com

11 *Attorneys for Plaintiffs & the Classes*

12
13 **IN THE UNITED STATES DISTRICT COURT**
14 **DISTRICT OF ARIZONA**

15 Montana Strong and Debra Yick,
16 *individually and on behalf of all others*
17 *similarly situated,*

17 Plaintiffs,

18 v.

19 LifeStance Health Group, Inc. d/b/a
20 LifeStance, a Delaware corporation,

21 Defendant.

Case No. 2:23-cv-00682

**THIRD AMENDED CLASS
ACTION COMPLAINT**

JURY TRIAL DEMANDED

REDACTED

THIRD AMENDED CLASS ACTION COMPLAINT

Plaintiffs 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.

The Sensitive Nature of LifeStance’s Mental Health Website.

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

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 Jan. 16, 2024) (“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 Jan. 16, 2024).

1 data—and especially mental health data²—is some of the most valuable and
2 controversial.³

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

6 5. These mental health websites and applications (“apps”) are a data harvesting
7 bonanza as “[n]early all the apps reviewed gobble up users’ personal data . . . Further,
8 some apps harvest additional data from third-party platforms (like Facebook), elsewhere
9 on users’ phones, or data brokers.”⁵

10 6. These telehealth companies are collecting, in some instances, “ultra-
11 sensitive personal data” about patients ranging from those seeking information about their
12 reproductive rights and options, those seeking information regarding their addictions and
13 . . . those seeking mental health counseling.⁶

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

19 ³ Protected and highly sensitive medical information collected by healthcare entities
20 includes many categories, from intimate details of an individual’s conditions, symptoms,
21 diagnoses and treatments to personally identifying information to unique codes which
22 can identify and connect individuals to the collecting entity. *See* Molly Osberg & Dhruv
23 Mehrotra, *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 Jan. 16, 2024).

24 ⁴ *See, e.g., Top Mental Health and Prayer Apps Fail Spectacularly at Privacy,*
25 *Security*, MOZILLA (May 2, 2022), available at
26 <https://foundation.mozilla.org/en/blog/top-mental-health-and-prayer-apps-fail-spectacularly-at-privacy-security/> (last visited Jan. 16, 2024).

27 ⁵ *Id.* (stating that “others are taking advantage of this. Silicon Valley investors are
28 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 *See* 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

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

from getting an abortion. It can be used to build anti-abortion ad campaigns – and spread misinformation about reproductive 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 Jan. 16, 2024).

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 Jan. 16, 2024) (“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).

LifeStance Collects a Significant Amount of Private Information.

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 telemedicine offering.”⁹

11. 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.

12. 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.

13. In order to market and to provide these services, 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 on the Website.¹⁰

14. 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.

⁹ <https://lifestance.com/why-lifestance> (last visited Jan. 16, 2024); *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 Jan. 16, 2024).

¹⁰ *See* <https://lifestance.com/privacy-policy/> (last visited Jan. 16, 2024).

LifeStance Utilized Tracking Technologies to Monetize Users' Private Information.

15. 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 (collectively, “Pixel Information Recipients”) without the informed consent of its Users.

16. Invisible to the naked eye, pixels—which are configured by the website owner, here, LifeStance—collect and transmit information from Users’ browsers to unauthorized third parties.

17. The Facebook Pixel, installed and configured by LifeStance, is a piece of code that “tracks the people and [the] type of actions they take” as they interact with a website,¹¹ including how long a person spends on a particular web page, which buttons the person clicks, which pages they view and the text or phrases they type into various portions of the website (such as a general search bar, chat feature or text box).

18. The Private Information illegally sent to these third parties is, in turn, associated with other information to create very fulsome user profiles that are mined for marketing and other commercial purposes.

19. For example, in the case of information collected by LifeStance and sent to Facebook, such information is then linked to Users’ unique Facebook user ID (“Facebook ID” or “FID”) which allows Facebook and other third parties to personally identify those Users and associates their Private Information with their Facebook profiles.¹²

¹¹ *Retargeting*, <https://www.facebook.com/business/goals/retargeting> (last visited Jan. 11, 2024).

¹² The Facebook ID is a string of numbers Facebook uses to identify and connect to a User’s Facebook profile. Facebook creates a Facebook ID automatically, whether or not you choose to create a username. See <https://www.facebook.com/help/211813265517027> (last accessed January 10, 2024). Thus Facebook, which creates and maintains the Facebook ID directly connected to a

20. As a result, there is no anonymity in the information disclosed to Facebook for marketing and analytics purposes; that is, the Pixel collects and discloses a substantial “data packet” coupled with the FID so that LifeStance can, among other things, send targeted advertisements to Users based on their sensitive and protected Private Information. LifeStance also uses this impermissibly obtained data for analytics purposes to gain additional insights into how its patients use its Website.¹³

21. LifeStance tracks, collects and divulges data even on people who do not have a Facebook account or have deactivated their Facebook accounts, and these individuals can find themselves in an even worse situation because when their Private Information is sent to Facebook, they cannot clear past activity or disconnect the collection of future activity since they do not have an account (or an active account).¹⁴

22. When a User uses LifeStance’s Website where tracking technologies, such as the Pixel are present, the Pixel transmits the contents of their communications to Facebook including, but not limited to: (i) accessing the telehealth waiting rooms; (ii) the state where a User was located when accessing the telehealth waiting rooms; (iii) searches for medical services and treatments sought; (iv) searches for therapists; (v) the text of URLs visited by the User and (vi) other information that qualifies as PII and PHI under

User’s Facebook account, utilizes the Facebook ID to personally identify each User whose Private Information is disclosed to it.

¹³ While gaining additional insights into its User base is not a bad thing necessarily, LifeStance unquestionably was required to inform its Users that it had deployed tracking technologies on its Website so that those Users could make an informed decision as to whether they wanted their information to be collected, disclosed and used in this manner. The OCR Bulletin is instructive: “disclosures of PHI to tracking technology vendors for marketing purposes, ***without individuals’ HIPAA-compliant authorizations***, would constitute impermissible disclosures.” See OCR Bulletin, *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> (emphasis added) (last visited Jan. 17, 2024).

¹⁴ See *Shadow profiles: Facebook has information you didn’t have over* (April 11, 2018), <https://www.cnet.com/news/privacy/shadow-profiles-facebook-has-information-you-didnt-hand-over/> (last visited Jan. 15, 2024).

1 federal and state laws.¹⁵

2 23. Operating as designed and as implemented by LifeStance, the Pixel
3 disclosed information that allows a third party (e.g., Facebook) to know when and where
4 a specific patient was seeking confidential medical care, for what mental health condition
5 and the precise care they sought or received. Facebook, in turn, sells Users' Private
6 Information to third-party marketers who geo-target Plaintiffs' and Class Members' Meta
7 accounts based on that Private Information.

8 **LifeStance Derives Significant Value from Users' Private Information**

9 24. While the information captured and disclosed without permission may vary
10 depending on the pixel(s) embedded, these "data packets" can be extensive in that they
11 collect and transmit the contents of Users' communications and numerous other pieces
12 of information including, but not limited to: (i) the User's first and last name, (ii) the
13 User's date of birth; (iii) the User's email address, phone number and other personal
14 information; (iv) when a User accesses the Website; (v) medical services and treatments
15 sought; (vi) scheduling of appointments; (vii) accessing and viewing the appointment
16 portal; (viii) the text of URLs visited by the User and (ix) other information that qualifies
17 as PII and PHI under federal and state laws.

18 25. The data in the "data packets" is then linked to the User's unique Facebook
19 ID and their specific internet protocol ("IP") address, which is itself protected information
20 under the Health Insurance Portability and Accountability Act ("HIPAA").¹⁶

21 _____
22 ¹⁵ While this Amended Complaint primarily focuses on how LifeStance embedded
23 the Meta Pixel on its Website to collect and disclose Users' Private Information, other
24 secret tracking technologies embedded by LifeStance—such as Google Tag Manager,
25 Invoca, Heap Analytics and Pardot Analytics—also collect such Private Information and
26 the respective tech companies have the capability to link it to specific user profiles they
27 have built.

28 ¹⁶ The HIPAA privacy rule sets forth policies to protect all individually identifiable
health information that is held or transmitted, and there are approximately 18 HIPAA
Identifiers that are considered PII. This information can be used to identify, contact or
locate a single person or can be used with other sources to identify a single individual.
These HIPAA Identifiers, as relevant here, include names, dates related to an individual,
email addresses, device identifiers, web URLs and IP addresses. *See Guidance regarding
Methods for De-identification of Protected Health Information in Accordance with the*

1 26. LifeStance went to these lengths to obtain sensitive Private Information
2 because its patients would **not** provide it if they were informed and given a choice.

3 27. Thus, by deciding to use the Pixel (and other tracking technologies) to
4 collect Users' Private Information, LifeStance was unjustly enriched in that it acquired
5 highly sensitive information that it would not be able to obtain otherwise or for which it
6 would have to pay significantly. LifeStance also uses this impermissibly obtained data
7 for analytics purposes to gain additional insights into how its patients use its Website.

8 **LifeStance's Disclosure of Private Information Without Consent Violates the Law.**

9 28. Users of LifeStance's Website thought they were communicating *only* with
10 their trusted healthcare providers. But by employing third-party trackers—which obtain
11 detailed information about its patients' medical information—LifeStance effectively
12 bartered their Private Information for more detailed analytics of its Users to increase its
13 revenues and profits.

14 29. Healthcare patients simply do not anticipate that their trusted healthcare
15 provider will send Private Information collected via its web pages to an undisclosed third
16 party—let alone Facebook, which has a sordid history of privacy violations in pursuit of
17 ever-increasing advertising revenue—without their informed and express consent.¹⁷

18 30. Simply put (and as detailed herein), covered entities such as LifeStance are
19 **not** permitted to use tracking technology tools (like pixels) in a way that exposes patients'
20 Private Information to any third-party without express and informed consent from each
21 patient.

22 _____
23 *Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule,*
24 [https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-](https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html)
[identification/index.html](https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html) (last visited Jan. 11, 2024).

25 ¹⁷ This Court will not have to look far to find evidence of Meta's violations of privacy
26 laws. In May of this year, for example, the European Union fined Meta "a record-
27 breaking" \$1.3 billion for violating EU privacy laws. *See* Hanna Ziady, *Meta slapped*
28 *with record \$1.3 billion EU fine over data privacy,*
<https://www.cnn.com/2023/05/22/tech/meta-facebook-data-privacy-eu-fine/index.html>
(last accessed Jan, 15, 2024).

31. As recognized by both the Federal Trade Commission (“FTC”) and the Office for Civil Rights (“OCR”) of the Department of Health and Human Services (“HHS”), healthcare companies’ use of tracking technologies to collect and divulge their patients’ sensitive and confidential information is an extremely serious data security and privacy issue:

In today’s surveillance economy, the consumer is often the product. Consumer data powers the advertising machine that goes right back to the consumer. *But when companies use consumers’ sensitive health data for marketing and advertising purposes, such as by sending that data to marketing firms via tracking pixels on websites or software development kits on apps, watch out.*¹⁸

32. Similarly, OCR is clear that “[r]egulated 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.”¹⁹

33. This is precisely the conduct that LifeStance is engaging in, as these tracking codes are *not* required for LifeStance’s Site to operate; instead, they collect data that is later used for marketing, remarketing and advertising purposes by LifeStance and third parties to whom it is disclosed.

34. The facts of this unauthorized interception of Plaintiffs’ Private Information are overwhelmingly offensive; as noted by the Honorable William Orrick in a case pending against Facebook’s parent company concerning the use of Pixel tracking on hospital websites, consumers “would be shocked” to learn of the scope and nature of the

¹⁸ See Elisa Jillison, *Protecting the privacy of health information: A Baker’s dozen takeaways from FTC cases*, the FTC Business Blog (July 25, 2023) (emphasis added), available at <https://www.ftc.gov/business-guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-ftc-cases> (last visited Jan. 9, 2024).

¹⁹ See OCR Bulletin, *supra* note 13.

1 information collected.²⁰

2 35. LifeStance’s obligation to protect and secure the Private Information
3 entrusted to it is **not** new as the Office for Civil Rights at the U.S. Department of Health
4 and Human Services recently **reminded** HIPAA-regulated entities, in its *Use of Online*
5 *Tracking Technologies by HIPAA Covered Entities and Business Associates* bulletin that
6 such tracking and disclosures are **not** permitted under HIPAA.

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

10 Identifying information alone, such as personal names,
11 residential addresses, or phone numbers, would not necessarily
12 be designated as PHI. For instance, if such information was
13 reported as part of a publicly accessible data source, such as a
14 phone book, then this information would not be PHI because it
15 is not related to health 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.***²¹

16 37. Despite numerous warnings from federal regulators (not to mention several
17 FTC enforcement actions against telehealth companies for similar conduct) about the data

18 ²⁰ See *Doe v. Meta Platforms Inc.* (N.D. Cal., No. 3:2022cv03580) ECF No. 141; see
19 also [https://www.law360.com/articles/1548383/facebook-health-tracking-claim-
shocking-if-true-judge-says](https://www.law360.com/articles/1548383/facebook-health-tracking-claim-shocking-if-true-judge-says). Indeed, the HHS Bulletin noted that “because of the
20 proliferation of tracking technologies collecting sensitive information, now more than
21 ever, it is critical for regulated entities to ensure that they disclose PHI [personal health
information] **only** as expressly permitted or required by the HIPAA Privacy Rule.”

22 ²¹ *Guidance regarding Methods for De-identification of Protected Health*
23 *Information in Accordance with the Health Insurance Portability and Accountability Act*
24 *(HIPAA) Privacy Rule*, [https://www.hhs.gov/hipaa/for-professionals/privacy/special-
topics/de-identification/index.html](https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html), HHS.GOV (last visited Oct. 9, 2023) (noting that
25 “HIPAA Identifiers” include name; address (all geographic subdivisions smaller than
26 state, including street address, city county, and zip code); all elements (except years) of
27 dates related to an individual (including birthdate, admission date, discharge date, date of
28 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).

1 privacy risks of using third-party tracking technologies,²² LifeStance put tracking
 2 technologies on its Site in order to acquire and transmit Users' Private Information
 3 without their informed consent.

4 38. As detailed herein, LifeStance owed common law, statutory and regulatory
 5 duties to keep Users' Private Information safe, secure and confidential. LifeStance
 6 breached those duties and obligations by, *inter alia*: (i) failing to adequately review its
 7 marketing programs to ensure its Site was safe and secure; (ii) failing to remove or
 8 disengage technology that was known and designed to share Users' Private Informtion;
 9 (iii) failing to obtain the prior written consent of Users to disclose their Private
 10 Information to Facebook and/or others before doing so; (iv) failing to take steps to block
 11 the transmission of Users' Private Information through Facebook Pixels; (v) failing to
 12 warn Users that their Private Information was being shared with third parties without
 13 express consent and (vi) otherwise failing to design and monitor its Site to maintain the
 14 security, confidentiality and integrity of patient Private Information.

15 **LifeStance Has Not Informed Users of Its Use of Tracking Technologies on its Site.**

16 39. Despite incorporating the Facebook Pixel (and other tracking technologies)
 17 into its Site and servers, LifeStance has—to *this day*—not disclosed to Users that it
 18 divulged their sensitive and confidential Private Information with Facebook, which has a
 19 sordid history of privacy violations.²³

20
 21 ²² See, e.g., Heather Landi, *Regulators Warn Hospitals and Telehealth Companies*
 22 *about privacy risks of Meta, Google Tracking Tech*, FIERCE HEALTHCARE (July 21, 2023),
 23 [https://www.fiercehealthcare.com/health-tech/regulators-warn-hospitals-and-telehealth-](https://www.fiercehealthcare.com/health-tech/regulators-warn-hospitals-and-telehealth-companies-about-privacy-risks-meta-google)
 24 [companies-about-privacy-risks-meta-google](https://www.fiercehealthcare.com/health-tech/regulators-warn-hospitals-and-telehealth-companies-about-privacy-risks-meta-google) (last visited Jan. 15, 2024) (noting that the
 FTC and the OCR issued a rare joint release announcing that 130 hospital systems and
 telehealth providers received a letter warning them about the data privacy and security
 risks related to the use of online tracking technologies integrated into their websites or
 mobile apps).

25 ²³ This Court will not have to look far to find evidence of Meta's violations of privacy
 26 laws. Just in May of last year, for instance, the European Union fined Meta "a record-
 27 breaking" \$1.3 billion for violating EU privacy laws. See Hanna Ziady, *Meta slapped*
 28 *with record \$1.3 billion EU fine over data privacy*,
<https://www.cnn.com/2023/05/22/tech/meta-facebook-data-privacy-eu-fine/index.html>
 (last visited Jan. 9, 2024).

40. That is, in recent months and in stark contrast to LifeStance, several medical providers that used the Facebook Pixel in a similar way have provided their patients with notice that their Private Information was transmitted to third parties.²⁴

41. Here, not only has LifeStance declined to report its (virtually identical) unauthorized disclosures, it continues to disclose Users' Private Information to third parties through tools such as Google Tag Manager.

LifeStance's Conduct Caused Concrete & Demonstrable Harm to Users

42. 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.

43. 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 Website to maintain the security, confidentiality and integrity of

²⁴ See, e.g., *Cerebral, Inc. Notice of HIPAA Privacy Breach*, available at https://cerebral.com/static/hippa_privacy_breach-4000c6eb21449c2ecd8bd13706750cc2.pdf (last visited Jan. 9, 2024); *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 Jan. 9, 2024); *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 Jan. 9, 2024).

1 patient Private Information.

2 44. The information intercepted by the Pixel and third-party tracking
3 technologies is used to build incredibly fulsome and robust marketing profiles for
4 individual Users and create targeted advertisements based on the medical conditions and
5 other Private Information disclosed. Despite the clear and unequivocal prohibition on the
6 disclosure of PHI without consent, LifeStance chose to use the Pixel and other tracking
7 technology data for marketing purposes to bolster its revenue.

8 45. Simply put, LifeStance put its profit over its patients' privacy rights.

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

15 47. Plaintiffs seek, on behalf of themselves and a class of similarly situated
16 persons, to remedy these harms and therefore assert the following statutory and common
17 law claims against LifeStance: (i) Violation of the California Invasion of Privacy Act,
18 Cal. Penal Code §§ 630, *et seq.*; (ii) Violation of the California Confidentiality of
19 Medical Information Act, Cal. Civ. Code §§ 56, *et seq.*; (iii) Violation of Electronic
20 Communications Privacy Act, 18 U.S.C. § 2511(1), *et seq.*, Unauthorized Interception,
21 Use and Disclosure; (iv) Violation of The Unfair Competition Law, Cal. Bus. & Prof.
22 Code § 17200, *et seq.*—Unlawful Business Practices; (v) Violation of The Unfair
23 Competition Law ("UCL"), Cal. Bus. & Prof. Code § 17200, *et seq.*—Unfair Prong; (vi)
24 violation of A.R.S. §44-1521 *et seq.* (vii) Violation of New York General Business Law
25 § 349, *et seq.* and (viii) Common Law Invasion of Privacy—Intrusion Upon Seclusion.

26 **THE PARTIES**

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

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

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

6 **JURISDICTION & VENUE**

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

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

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

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

24 **FACTUAL ALLEGATIONS**

25 ***A. Federal Regulators Make Clear that the Use of Tracking Technologies to*** 26 ***Collect & Divulge Private Information Without Informed Consent is Illegal.***

27 55. This surreptitious collection and divulgence of Private Information is an
28 extremely serious data security and privacy issue. Both the FTC and HHS have—in

1 recent months—reiterated the importance of and necessity for data security and privacy
2 concerning health information.

3 56. For instance, the FTC recently published a bulletin entitled *Protecting the*
4 *privacy of health information: A baker’s dozen takeaways from FTC cases*, in which it
5 noted that “[h]ealth information is not just about medications, procedures, and diagnoses.
6 ***Rather, it is anything that conveys information—or enables an inference—about a***
7 ***consumer’s health.*** Indeed, [recent FTC enforcement actions
8 involving] *Premom, BetterHelp, GoodRx and Flo Health make clear that the fact that a*
9 ***consumer is using a particular health-related app or website—one related to mental***
10 ***health or fertility, for example—or how they interact with that app (say, turning***
11 ***‘pregnancy mode’ on or off) may itself be health information.***”²⁵

12 57. The FTC is unequivocal in its stance as it informs—in no uncertain terms—
13 healthcare companies that they should ***not*** use tracking technologies to collect sensitive
14 health information and disclose it to various platforms without informed consent.

15 58. The federal government is taking these violations of health data privacy and
16 security seriously as recent high-profile FTC settlements against several telehealth
17 companies evidence.

18 59. For example, earlier this year, the FTC imposed a \$1.5 million penalty on
19 GoodRx for violating the FTC Act by sharing its customers’ sensitive PHI with
20 advertising companies and platforms, including Facebook, Google and Criteo. The FTC
21 also reached a \$7.8 million settlement with the online counseling service BetterHelp,
22 resolving allegations that the company shared customer health data with Facebook and
23 Snapchat for advertising purposes. Likewise, the FTC reached a settlement with Flo
24 Health, Inc. related to information about fertility and pregnancy that Flo fertility-tracking
25 app was improperly sharing with Facebook, Google and other third parties. And Easy
26 Healthcare was ordered to pay a \$100,000 civil penalty for violating the Health Breach

27
28 ²⁵ See *Protecting the privacy of health information: A Baker’s dozen takeaways from FTC cases*, *supra* note 18.

1 Notification Rule when its ovulation tracking app Premon shared health data for
2 advertising purposes.²⁶

3 60. Even more recently, in July 2023, federal regulators sent a letter to
4 approximately 130 healthcare providers warning them about using online tracking
5 technologies that could result in unauthorized disclosures of Private Information to third
6 parties. The letter highlighted the “risks and concerns about the use of technologies, such
7 as the Meta/Facebook Pixel and Google Analytics, that can track a user’s online
8 activities,” and warned about “[i]mpermissible disclosures of an individual’s personal
9 health information to third parties” that could “result in a wide range of harms to an
10 individual or others.” According to the letter, “[s]uch disclosures can reveal sensitive
11 information including health conditions, diagnoses, medications, medical treatments,
12 frequency of visits to health care professionals, where an individual seeks medical
13 treatment, and more.”²⁷

14 61. HHS has made clear that “*disclosures of PHI to tracking technology*
15 *vendors for marketing purposes, without individuals’ HIPAA-compliant*
16 *authorizations, would constitute impermissible disclosures.*”²⁸

17 62. The OCR Bulletin *reminds* healthcare organizations regulated under the
18 HIPAA that they may use third-party tracking tools, such as Google Analytics or Pixels

19 ²⁶ See How FTC Enforcement Actions Will Impact Telehealth Data Privacy,
20 [https://healthitsecurity.com/features/how-ftc-enforcement-actions-will-impact-](https://healthitsecurity.com/features/how-ftc-enforcement-actions-will-impact-telehealth-data-privacy)
21 [telehealth-data-privacy](https://healthitsecurity.com/features/how-ftc-enforcement-actions-will-impact-telehealth-data-privacy) (last visited Jan. 9, 2024); see also Allison Grande, *FTC Targets*
22 *GoodRx In 1st Action Under Health Breach Rule*, Law360 (Feb. 1, 2023), available at
23 [www.law360.com/articles/1571369/ftc-targets-goodrx-in-1st-action-under-health-](https://www.law360.com/articles/1571369/ftc-targets-goodrx-in-1st-action-under-health-breach-rule?copied=1)
24 [breach-rule?copied=1](https://www.law360.com/articles/1571369/ftc-targets-goodrx-in-1st-action-under-health-breach-rule?copied=1) (“The Federal Trade Commission signaled it won’t hesitate to
25 wield its full range of enforcement powers when it dinged GoodRx for allegedly sharing
26 sensitive health data with advertisers, teeing up a big year for the agency and boosting
27 efforts to regulate data privacy on a larger scale.”); [https://www.ftc.gov/news-](https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-gives-final-approval-order-banning-betterhelp-sharing-sensitive-health-data-advertising)
28 [events/news/press-releases/2023/07/ftc-gives-final-approval-order-banning-betterhelp-](https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-gives-final-approval-order-banning-betterhelp-sharing-sensitive-health-data-advertising)
[sharing-sensitive-health-data-advertising](https://www.ftc.gov/news-events/news/press-releases/2023/05/ovulation-tracking-app-premom-will-be-barred-sharing-health-data-advertising-under-proposed-ftc); [https://www.ftc.gov/news-](https://www.ftc.gov/news-events/news/press-releases/2023/05/ovulation-tracking-app-premom-will-be-barred-sharing-health-data-advertising-under-proposed-ftc)
[events/news/press-releases/2023/05/ovulation-tracking-app-premom-will-be-barred-sharing-health-data-](https://www.ftc.gov/news-events/news/press-releases/2023/05/ovulation-tracking-app-premom-will-be-barred-sharing-health-data-advertising-under-proposed-ftc)
[advertising-under-proposed-ftc](https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google) (last visited Jan. 9, 2024); [https://www.ftc.gov/news-](https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google)
[events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-](https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google)
[shared-sensitive-health-data-facebook-google](https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google) (last visited Jan. 9, 2024).

²⁷ See OCR Bulletin, *supra*, note 13.

²⁸ *Id.*

1 *only in a limited way*, to perform analysis on data key to operations. They are not
 2 permitted, however, to use these tools in a way that may expose patients' PHI to these
 3 vendors.²⁹

4 63. The OCR Bulletin discusses the harms that disclosure may cause patients:
 5 An impermissible disclosure of an individual's PHI not only
 6 violates the Privacy Rule but also may result in a wide range of
 7 additional harms to the individual or others. For example, an
 8 impermissible disclosure of PHI may result in identity theft,
 9 financial loss, ***discrimination, stigma, mental anguish, or***
 10 ***other serious negative consequences to the reputation, health,***
 11 ***or physical safety of the individual or to others identified in***
 12 ***the individual's PHI***. Such disclosures can reveal incredibly
 13 sensitive information about an individual, ***including***
 14 ***diagnoses, frequency of visits to a therapist or other health***
 15 ***care professionals, and where an individual seeks medical***
 16 ***treatment***. While it has always been true that regulated entities
 17 may not impermissibly disclose PHI to tracking technology
 18 vendors, ***because of the proliferation of tracking technologies***
 19 ***collecting sensitive information, now more than ever, it is***
 20 ***critical for regulated entities to ensure that they disclose PHI***
 21 ***only as expressly permitted or required by the HIPAA Privacy***
 22 ***Rule***.³⁰

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

28 65. Moreover, investigative journalists have published several reports detailing
 the seemingly ubiquitous use of tracking technologies on the digital properties of
 hospitals, health care providers and telehealth companies to monetize their Users' Private
 Information.

66. For instance, THE MARKUP reported that 33 of the largest 100 hospital

²⁹ See *id.*

³⁰ *Id.* (emphasis added).

1 systems in the country utilized the Meta Pixel to send Facebook a packet of data whenever
2 a person clicked a button to schedule a doctor's appointment.³¹

3 67. And, in the aptly titled report "*Out of Control*": *Dozens of Telehealth*
4 *Startups Sent Sensitive Health Information to Big Tech Companies*, a joint investigation
5 by STAT and THE MARKUP of 50 direct-to-consumer telehealth companies reported that
6 telehealth companies or virtual care websites were providing sensitive medical
7 information they collect to the world's largest advertising platforms.³²

8 68. Many telehealth sites had at least one tracker—from Meta, Google, TikTok,
9 Bing, Snap, Twitter, LinkedIn or Pinterest—that collected patients' answers to medical
10 intake questions.³³ These pixels are snippets of code that track internet and app users as
11 they navigate through a website, logging which pages they visit, which buttons they click
12 and certain information they enter into forms. In exchange for installing the pixels, third
13 party platforms (e.g., Facebook and Google) provide website owners analytics about the
14 advertisements they have placed as well as tools to target people who have visited their
15 websites.

16 69. Many healthcare sites had at least one tracker—from Meta, Google, TikTok,
17 Bing, Snap, Twitter, LinkedIn and/or Pinterest—that collected patients' answers to
18 medical intake questions.

19 **B. The Tracking Pixels.**

21 ³¹ See Todd Feathers, Simon Fondrie-Teitler, Angie Waller & Surya Mattu,
22 *Facebook is Receiving Sensitive Medical Information from Hospital Websites*, THE
MARKUP, <https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites> (last visited Jan. 9, 2024).

23 ³² Todd Feathers, Katie Palmer (STAT) & Simon Fondrie-Teitler, "*Out Of Control*":
24 *Dozens of Telehealth Startups Sent Sensitive Health Information to Big Tech Companies*:
25 *An investigation by The Markup and STAT found 49 out of 50 telehealth websites sharing*
health data via Big Tech's tracking tools (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 Jan. 9, 2024).

26 ³³ See *id.* (noting, "[t]rackers on 25 sites, including those run by industry leaders
27 Hims & Hers, Ro, and Thirty Madison, told at least one big tech platform that the user
28 had added an item like a prescription medication to their cart, or checked out with a
subscription for a treatment plan").

70. Tracking tools³⁴ 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.³⁵

71. Pixels are routinely used to target specific customers by utilizing data to build profiles for the purposes of retargeting, for example, serving online advertisements to people who have previously engaged with a business's website—and other marketing.

72. Here, a User's web browser executed the Pixels via instructions within each webpage of LifeStance's Website to communicate certain information (within parameters set by LifeStance) directly to the corresponding Pixel Information Recipients—at the same time as the User's browser is sending this information to LifeStance.

73. The Pixels can also share the Users' identifying information for easy tracking via “cookies”³⁶ stored on their computer by any of the Pixel Information Recipients with whom they have an account. For example, Facebook stores or updates a Facebook-specific cookie every time a person accesses their Facebook account from the same web browser.

74. The Pixel can access this cookie and send certain identifying information

³⁴ 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 Jan. 16, 2024).

³⁵ 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 Jan. 16, 2024).

³⁶ “Cookies are small files of information that a web server generates and sends to a web browser. Cookies help inform websites about the user, enabling the websites to personalize the user experience.” See <https://www.cloudflare.com/learning/privacy/what-are-cookies/> (last visited Jan. 9, 2024).

1 like the User's Facebook ID to Facebook along with the other data relating to the User's
2 Website inputs. The same is true for the other Pixel Information Recipients, which also
3 create cookies that are stored in the User's computer and accessed by the Pixels to identify
4 the User.

5 75. The Pixels are programmable, meaning that LifeStance controls which of
6 the webpages on the Website contain the Pixels and which events are tracked and
7 transmitted to the Pixel Information Recipients.

8 76. LifeStance utilized Facebook Pixels (and, upon information and good faith
9 belief, other tracking technologies) since at least April 11, 2020.

10 77. Specifically, LifeStance installed a Meta Pixel account with the ID
11 182326009171632.

12 78. LifeStance used the data it collected from Plaintiffs and Class Members,
13 without their consent, to improve its advertising and bolster its revenues.

14 ***C. Facebook's Conversions Application Programming Interface.***

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

19 80. Facebook's workaround, for example, is called Facebook's Conversions
20 Application Programming Interface ("CAPI") on its servers.

21 81. CAPI is an effective workaround because it does not intercept data
22 communicated from the user's browser; rather, CAPI "is designed to create a direct
23 connection between [Web hosts'] marketing data and [Facebook]."

24 82. Thus, the (supposedly) private communications between patients and
25 Defendant, which are necessary to use Website, are actually received by Defendant and
26 stored on its server before CAPI collects and sends the Private Information contained in
27 those communications directly from Defendant to Facebook. Client devices do not have
28

1 access to host servers and thus cannot prevent (or even detect) this transmission.³⁷

2 83. Facebook CAPI and similar tracking technologies allow businesses to send
3 web events, such as clicks, form submissions, keystroke events and other user actions
4 performed by the user on the Website, from their own servers to Facebook and other third
5 parties.³⁸

6 84. CAPI is an alternative method of tracking versus the Pixel because no
7 privacy protections on the user's end can defeat it. This is because it is "server-side"
8 implementation of tracking technology, whereas the Pixels are "client-side"—executed
9 on users' computers in their web browsers.

10 85. Because CAPI is server-side, it cannot access the Facebook c_user cookie
11 to retrieve the Facebook ID.³⁹ Therefore, other roundabout methods of linking the user to
12 their Facebook account are employed.⁴⁰ For example, Facebook has an entire page within
13 its developers' website about how to de-duplicate data received when both the Facebook
14

15 ³⁷ While there is no way to confirm with certainty that a Web host like Defendant has
16 implemented workarounds like CAPI without access to the host server, companies like
17 Facebook instruct the companies it partners with to "[u]se the Conversions API in
18 addition to the [] Pixel, and share the same events using both tools," because such a
19 "redundant event setup" allows Defendant "to share website events [with Facebook] that
20 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).

21 ³⁸ *See* <https://revealbot.com/blog/facebook-conversions-api/> (last visited Jan. 9,
22 2024).

23 ³⁹ "Our systems are designed to not accept customer information that is unhashed
24 Contact Information, unless noted below. Contact Information is information that
25 personally identifies individuals, such as names, email addresses and phone numbers, that
we use for matching purposes only." *See*
[https://developers.facebook.com/docs/marketing-api/conversions-
api/parameters/customer-information-parameters/](https://developers.facebook.com/docs/marketing-api/conversions-api/parameters/customer-information-parameters/) (last visited Jan. 9, 2024).

26 ⁴⁰ "Sending additional customer information parameters may help increase Event
27 Match Quality. Only matched events can be used for ads attribution and ad delivery
28 optimization, and the higher the matching quality, the better."
[https://developers.facebook.com/docs/marketing-api/conversions-api/best-
practices/#req-rec-params](https://developers.facebook.com/docs/marketing-api/conversions-api/best-practices/#req-rec-params) (last visited Jan. 9, 2024).

1 Pixel and CAPI are executed.⁴¹

2 86. Thus, without any knowledge, authorization or action by a User, a website
3 owner (like LifeStance) can use its source code to commandeer a user's computing
4 device, causing the device to contemporaneously and invisibly re-direct the users'
5 communications to third parties.

6 ***C. LifeStance Discloses Plaintiffs' and Class Members' Private Information to***
7 ***Facebook.***

8 87. LifeStance "offers long-term online care and medication management for a
9 wide range of mental health conditions," from depression and PTSD to bipolar disorder
10 and alcohol dependence, through therapy and medication.⁴²

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

13 89. Defendant purposely installed the Pixel and other tracking tools on its
14 Website and programmed them to surreptitiously share its patients' private and protected
15 communications with Facebook and Pixel Information Recipients, including
16 communications that contain Plaintiffs' and Class Members' Private Information.

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

19 91. Facebook operates the world's largest social media company and generated
20 \$117 billion in revenue in 2021, roughly 97% of which was derived from selling
21 advertising space.⁴³

22 92. In conjunction with its advertising business, Facebook encourages and
23 promotes entities and website owners, such as Defendant, to utilize its "Business Tools"

24 ⁴¹ See [https://developers.facebook.com/docs/marketing-api/conversions-](https://developers.facebook.com/docs/marketing-api/conversions-api/deduplicate-pixel-and-server-events)
25 [api/deduplicate-pixel- and-server-events](https://developers.facebook.com/docs/marketing-api/conversions-api/deduplicate-pixel-and-server-events) (last visited Jan. 9, 2024).

26 ⁴² <https://lifestance.com/> (last visited Jan. 16, 2024).

27 ⁴³ META REPORTS FOURTH QUARTER AND FULL YEAR 2021 RESULTS,
28 [https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-](https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx)
[Quarter-and-Full-Year-2021-Results/default.aspx](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 Jan.
16, 2024).

1 to gather, identify, target and market products and services to individuals.

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

5 94. The Business Tools are automatically configured to capture “Standard
6 Events” such as when a user visits a particular webpage, that webpage’s Universal
7 Resource Locator (“URL”) and metadata, button clicks, etc.⁴⁴

8 95. Notably, advertisers, such as Defendant, can track other user actions and can
9 create their own tracking parameters by building a “custom event.”⁴⁵

10 96. One such Business Tool is the Pixel. When a User accesses a webpage with
11 the Pixel, their communications with the host webpage are instantaneously and
12 surreptitiously duplicated and sent to Facebook’s servers—traveling from the user’s
13 browser to Facebook’s server.

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

17 98. As explained below, this unlawful transmission is initiated by Defendant’s
18 source code concurrent with communications made via the Website.

19 ***C. LifeStance’s Method of Transmitting Plaintiffs’ & Class Members’ Private***
20 ***Information via the Meta Pixel.***

21 ⁴⁴ *Specifications for Facebook Pixel Standard Events*,
22 <https://www.facebook.com/business/help/402791146561655?id=1205376682832142>,
23 FACEBOOK.COM (last visited Jan. 16, 2024); *see*, META PIXEL, GUIDES, ADVANCED,
24 <https://developers.facebook.com/docs/facebook-pixel/advanced/>, FACEBOOK.COM (last
25 visited Jan. 16, 2024); *see also* BEST PRACTICES FOR META PIXEL SETUP,
26 <https://www.facebook.com/business/help/218844828315224?id=1205376682832142>,
FACEBOOK.COM (last visited Jan. 16, 2024); META MARKETING API, APP EVENTS API,
27 <https://developers.facebook.com/docs/marketing-api/app-event-api/> FACEBOOK.COM
(last visited Jan. 16, 2024).

28 ⁴⁵ ABOUT STANDARD AND CUSTOM WEBSITE EVENTS,
<https://www.facebook.com/business/help/964258670337005?id=1205376682832142>,
FACEBOOK.COM (last visited Jan. 16, 2024); *see also* META MARKETING API, APP
EVENTS API, <https://developers.facebook.com/docs/marketing-api/app-event-api/>,
FACEBOOK.COM (last visited Jan. 16, 2024).

99. 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).

100. 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.

101. 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.⁴⁶

102. 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 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).

⁴⁶ One browsing session may consist of hundreds or thousands of individual HTTP Requests and HTTP Responses.

1 103. Every website is comprised of Markup and “Source Code.” Source Code is
2 a set of instructions that commands the website visitor’s browser to take certain actions
3 when the web page first loads or when a specified event triggers the code.

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

8 105. When patients visit Defendant’s Website via an HTTP Request to
9 LifeStance’s server, that server sends an HTTP Response including the Markup that
10 displays the Webpage visible to the user and Source Code including Defendant’s Pixel.

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

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

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

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

26 110. Thus, the communications between patients and Defendant, which are
27 necessary to use Defendant’s Website, are actually received by Defendant and stored on
28 its server before CAPI collects and sends the Private Information contained in those

1 communications directly from Defendant to Facebook.

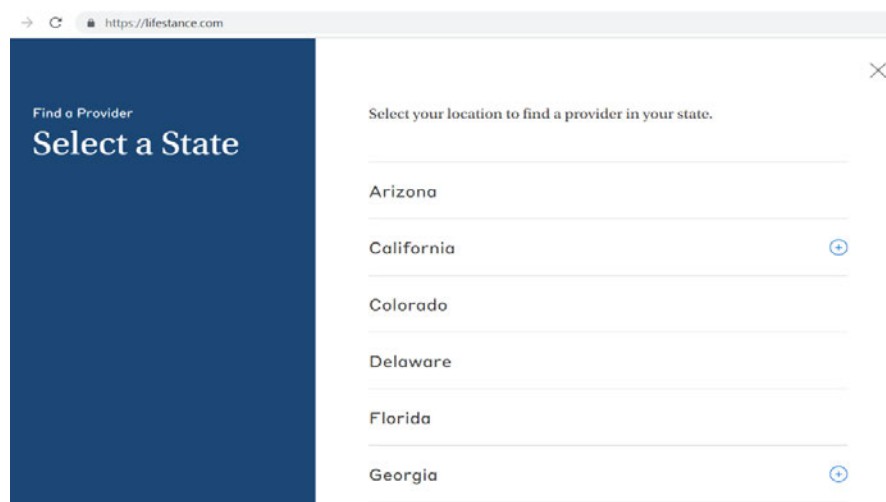
2 111. Client devices do not have access to host servers and thus cannot prevent (or
3 even detect) this transmission.

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

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

12 114. In this case, Defendant employed the Tracking Pixel and CAPI to intercept,
13 duplicate and re-direct Plaintiffs' and Class Members' Private Information to Facebook.

14 115. For example, when a patient visits <https://lifestance.com/> and selects "Find
15 Provider" in New York, NY, the patient's browser automatically sends an HTTP Request
16 to Defendant's web server. The Defendant's web server automatically returns an HTTP
17 Response, which loads the Markup for that particular webpage as depicted below.



18
19
20
21
22
23
24
25
26
27 **Figure 1. Image taken from <https://www.lifestance.com>**

28 116. The patient visiting this particular web page only sees the Markup, not the

Defendant's Source Code or underlying HTTP Requests and Responses.

117. 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.

▼ Request Headers

```
:authority: www.facebook.com
:method: GET
:path: /tr/?id=182326009171632&ev=SubscribedButtonClick&dl=https%3A%2F%2Flifescance.com%2F&rl=https%3A%2F%2Fwww.google.com%2F&if=false&ts=1677886960197&cd[buttonFeatures]={%7B%22classList%22%3A%22btn--primary%22%2C%22destination%22%3A%22%2C%22id%22%3A%22%22%2C%22imageUrl%22%3A%22%2C%22innerText%22%3A%22Find%20a%20Provider%22%2C%22numChildButtons%22%3A%22%2C%22tag%22%3A%22button%22%2C%22type%22%3A%22%2C%22name%22%3A%22%2C%22value%22%3A%22%22%2C%22cd[buttonText1=Find%20a%20Provider%22%2C%22formFeatures]={%5B%5D&cd[pageFeatures]={%7B%22title%22%3A%22Online%20Therapy%20%26%20Psychiatry%20Appointments%20%7C%20Lifescance%20Health%22%7D&sw=1664&sh=1110&udff[st]=b5252c3a46889dfab36f8b107b182bce34c7d892ad371e2c62980177440843eb&v=2.9.98&r=stable&ec=2&o=2078&cs_est=true&fbp=fb.1.1677811625287.507077028&it=1677886902461&coo=false&es=automatic&tm=3&rqm=GET
:scheme: https
:accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
:accept-encoding: gzip, deflate, br
:accept-language: en-US,en;q=0.9,ru;q=0.8
:cookie: datr=QtI1, sb=GrxtY1jj9lKwncg7UAhijMv; dpr=1.5; usida=eyJ2ZXIiOiJEsImkIjoiQXJxdDZlYzE2Y2Ywc2MXQiLCJ0aWwIjoiXjNjE4NjYwFQ%3D%3D; fr=0lxmnh0G2Dqbhu0Fv.AWNBFTXMo-GBug23VyULX1atrg.BkASUV.-f.AAA.0.0.BkAS6t.AWNgD00qC_c
:referer: https://lifescance.com/
```

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).⁴⁷

Query String Parameters	view source	view URL-encoded
id: 182326009171632		
ev: SubscribedButtonClick		
dl: https://lifescance.com/		
rl: https://www.google.com/		
if: false		
ts: 1677886960197		
cd[buttonFeatures]: {"classList": "btn btn--primary", "destination": "", "id": "", "imageUrl": "", "innerText": "Find a Provider", "numChildButtons": 0, "tag": "button", "type": null, "name": "", "value": ""}		
cd[buttonText]: Find a Provider		
cd[formFeatures]: []		
cd[pageFeatures]: {"title": "Online Therapy & Psychiatry Appointments Lifescance Health"}		
sw: 1664		
sh: 1110		
udff[st]: b5252c3a46889dfab36f8b107b182bce34c7d892ad371e2c62980177440843eb		
v: 2.9.98		
r: stable		
ec: 2		
o: 2078		
cs_est: true		
fbp: fb.1.1677811625287.507077028		
it: 1677886902461		

latr
r's

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

118. 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,⁴⁸ effectively open a spying window through which the webpage can funnel the visitor's data, actions, and communications to third parties.

119. 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.

120. 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.

121. Thus, without its patients' consent, Defendant has effectively used its source code to commandeer patients' computing devices thereby re-directing their Private Information to third parties.

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

123. Consequently, when Plaintiffs 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,

⁴⁸ 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.

1 specific button/menu selections, and appointment type and date.

2 ***E. Defendant's Pixel and/or Tracking Practices caused Plaintiffs' & Class***
3 ***Members' PII & PHI to be sent to Facebook.***

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

8 125. Defendant's Website contain a unique identifier which indicates that the
9 Pixel is being used on a particular webpage, identified as 182326009171632 on
10 www.lifestance.com, which identified and categorized which actions the User took on
11 the webpage at issue (including "PageView" which identifies the User as having viewed
12 the particular webpage, "Microdata" which contains page metadata,
13 "SubscribedButtonClick," which tracks each click on the webpage and shares the
14 metadata of buttons clicked by the User, such the "inner text" of the button, with
15 Facebook) and "FindTelehealth," a custom event informing Facebook when this event
16 occurred.

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

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

22 128. While seeking and using Defendant's services as a medical provider,
23 Plaintiffs and Class Members communicated their Private Information to Defendant via
24 its Website.

25 129. Defendant did not disclose to Plaintiffs and Class Members that their Private
26 Information would be shared with Facebook as it was communicated to Defendant.

27 130. Plaintiffs and Class Members never consented, agreed, authorized or
28 otherwise permitted Defendant to disclose their Private Information to Facebook, nor did

1 they intend for Facebook to be a party to their communications with Defendant.

2 131. Defendant's Pixel and CAPI sent non-public Private Information to
3 Facebook, including but not limited to Plaintiffs' and Class Members': (i) status as
4 medical patients; (ii) health conditions; (iii) sought treatment or therapies; (iv)
5 appointment requests and appointment booking information; (v) locations or facilities
6 where treatment is sought; and (vi) which web pages were viewed.

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

12 133. Through the source code deployed by Defendant, the cookies that it uses to
13 help Facebook identify patients include but are not necessarily limited to cookies named:
14 c_user, datr, fr, and fbp.⁴⁹

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

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

24 136. The datr cookie identifies the patient's specific web browser from which the
25

26 ⁴⁹ Defendant's Website tracks and transmits data via first-party and third-party
27 cookies. C user, datr, and fr cookies are third-party cookies. The fbp cookie is a
28 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.

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

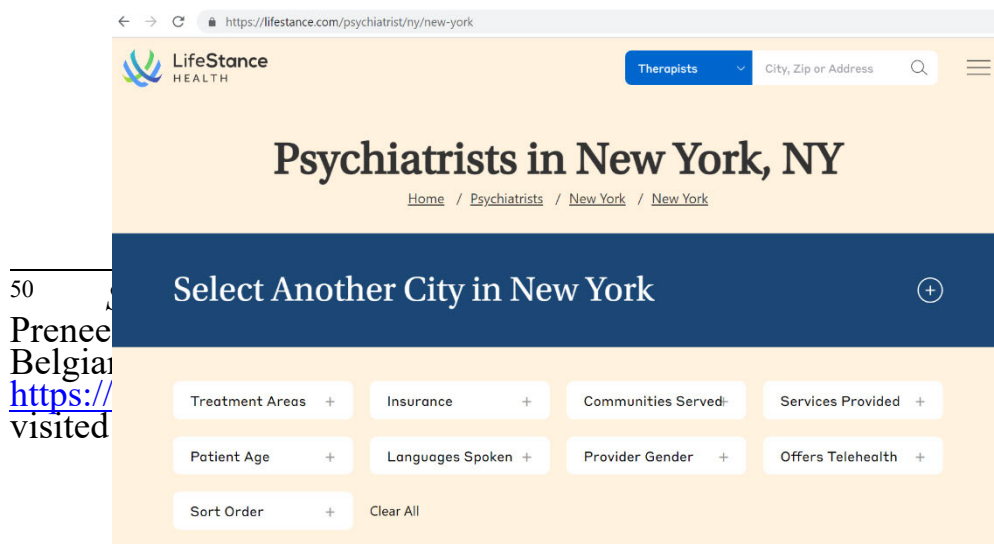
6 137. The fr cookie is a Facebook identifier that is an encrypted combination of
 7 the c_user and datr cookies.⁵⁰

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

15 ***D. Defendant's Pixel Disseminates Patient Information Via***
 16 ***www.lifestance.com.***

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

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



24
 25
 26 50
 27 Prenee
 28 Belgium
 29 [https://](https://www.lifestance.com/psychiatrist/ny/new-york)
 30 visited

31 laudia Diaz, and Bart
 32 report prepared for the
 33) (available at
 34 [sv1.0.pdf](https://www.lifestance.com/psychiatrist/ny/new-york)) (last

1
2
3
4
5
6
7 ***Figure 4. Defendant directs patients to its “Find a Provider” webpage for psychiatrists***
8 ***in New York, NY, with embedded Pixels—which are invisible to the regular user.***

9 141. If a User selects filters or enters keywords into the search bar on the “Find a
10 Provider” webpage, the filters and search terms are transmitted via the Facebook Pixel.
11 Similarly, if a patient uses the Website’s general search bar or chat, the terms and phrases
12 the patient types are transmitted to Facebook, even if they contain a patient’s treatment,
13 procedures, medical conditions, and related queries.

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

18 143. Without alerting the user, Defendant’s Pixel sends each and every
19 communication the user made to the Defendant via the Webpage to Facebook, and the
20 images below confirm that the communications Defendant sends to Facebook contain the
21 user’s Private Information.

22 144. For example, a patient can search for a provider specializing in alcohol and
23 drug use issues, with the option of using additional filters - from provider’s gender to
24 their additional specialties.

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

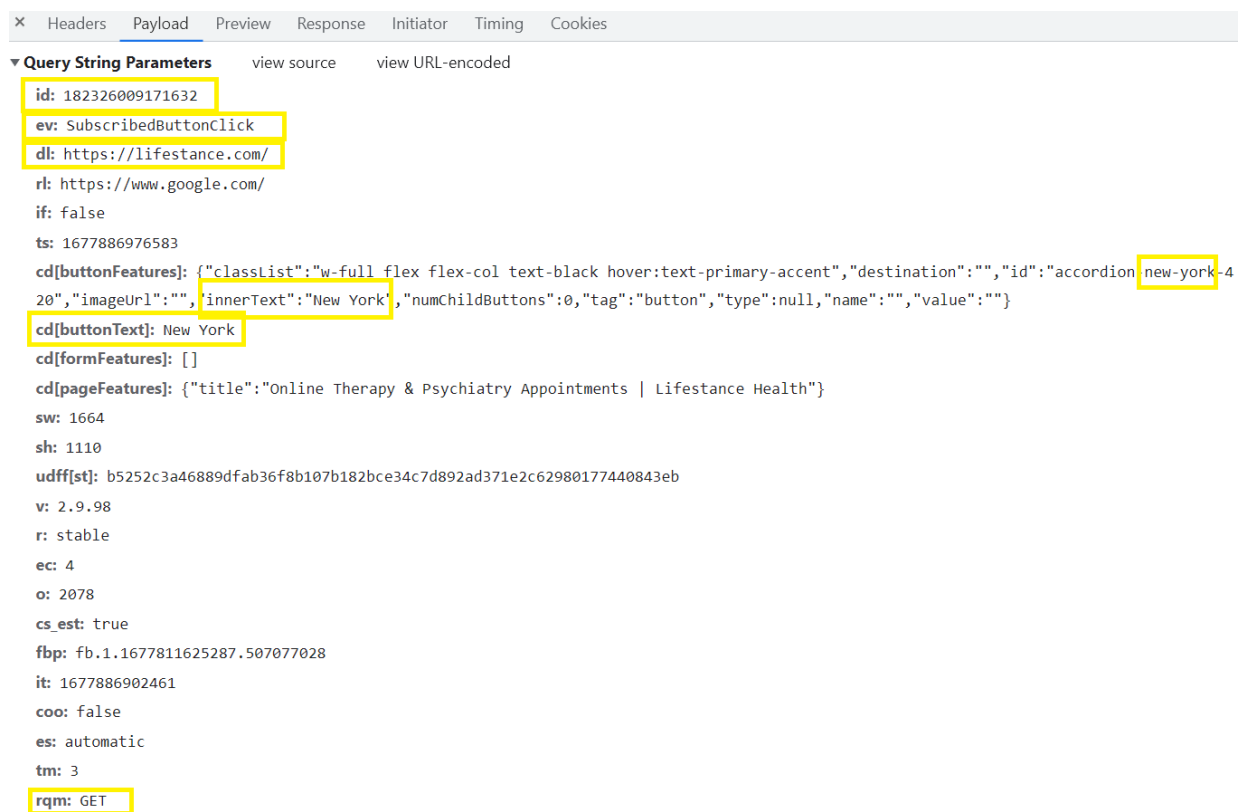


Figure 5. Defendant's transmission to Facebook of patient's search parameters showing location search terms (New York, NY)

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

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).

146. 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.

147. 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.

```

Request Headers
:authority: www.facebook.com
:method: GET
:path: /tr/?id=182326009171632&ev=SubscribedButtonClick&dl=https%3A%2F%2Flifestance.com%2Fpsychiatrist%2Fny%2Fnew-york%2F&rl=&if=fal
se&ts=1677812164603&cd[buttonFeatures]=%7B%22classList%22%3A%22custom-checkbox%22%2C%22destination%22%3A%22%22%2C%22id%22%3A%22%22
%22%22imageUri%22%3A%22%22%2C%22innerText%22%3A%22Alcohol%20and%20Drug%20Use%20Issues%22%2C%22numChildButtons%22%3A%22%22tag%22%3A
%22label%22%2C%22type%22%3Anull%7D&cd[buttonText]=Alcohol%20and%20Drug%20Use%20Issues&cd[formFeatures]=%5B%5D&cd[pageFeatures]=%7B%2
2title%22%2C%22%3A%22Psychiatrists%22%2C%22New%20York%22%2C%22New%20York%22%7D&sw=1664&sh=1110&udf[st]=b5252c3a46889dfab36f8b107b182bce34c7d
892ad371e2c62980177440843eb&v=2.9.97&r=stable&ec=2&o=2078&cs_est=true&fbp=fb.1.1677811625287.507077028&it=1677812054939&coo=false&e
s=automatic&tm=3&rqm=GET
:scheme: https
:accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
:accept-encoding: gzip, deflate, br
:accept-language: en-US,en;q=0.9,ru;q=0.8
:cookie: datr=QtI1; sb=GrxtY1jj9lKwnpCg7UAhIMv; dpr=1.5; usida=eyJ2ZXI0IjEsImklIjojIjQxdDZlY2YwY2MxQjI0aWw1I
joXnjc3NjE4NjVwfQ3D%3D; fr=0lmmh0G2Dqbhu0Fv.AWwBFTXmNO-G8ug23VyULX1atrG.BkASUV.-f.AAA.0.0.BkAS6t.AWwGDDoqC_c
:referer: https://lifestance.com/

```

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.

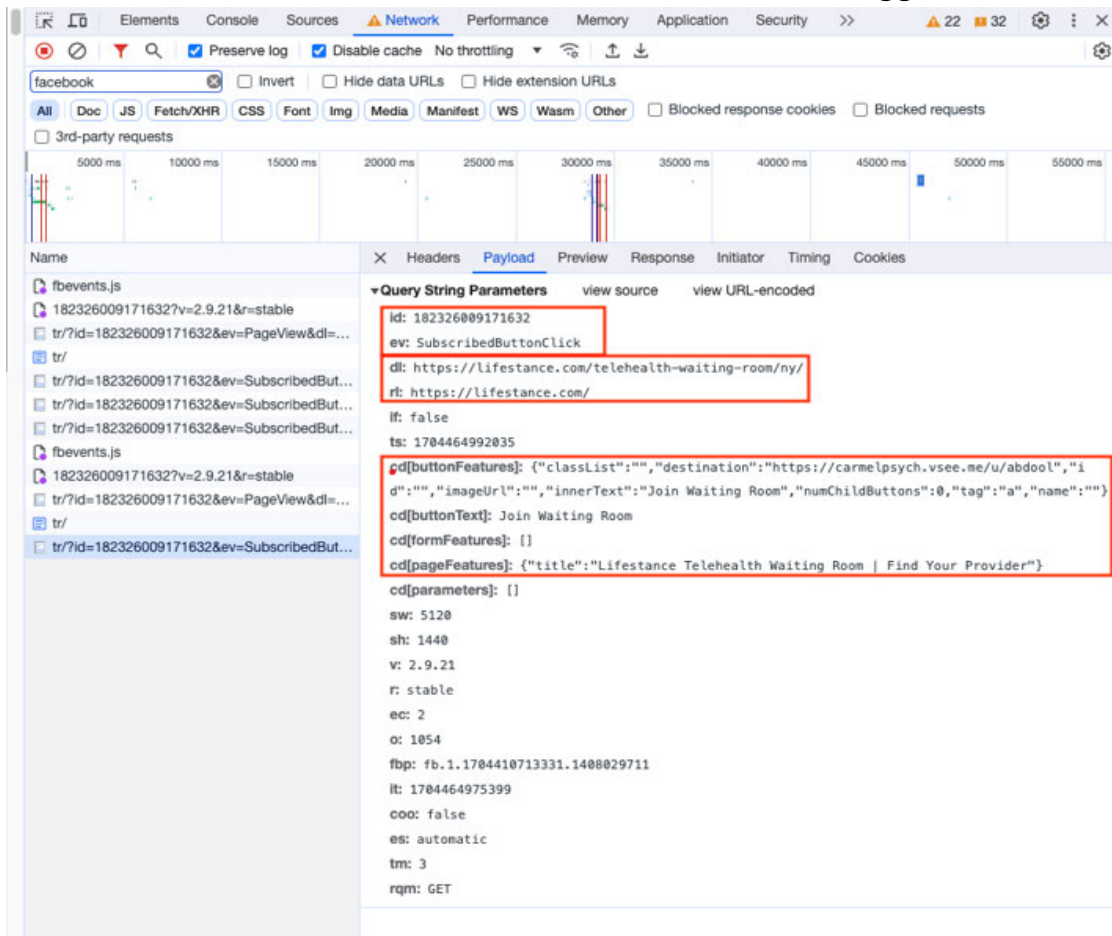
148. In the event a patient clicked to join the waiting room to meet with a provider, that event was also disclosed to Facebook.

Figure 9. An HTTP single communication session sent from the device to Facebook that reveals the user's entry into a waiting room.

149. 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.

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

151. 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.

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

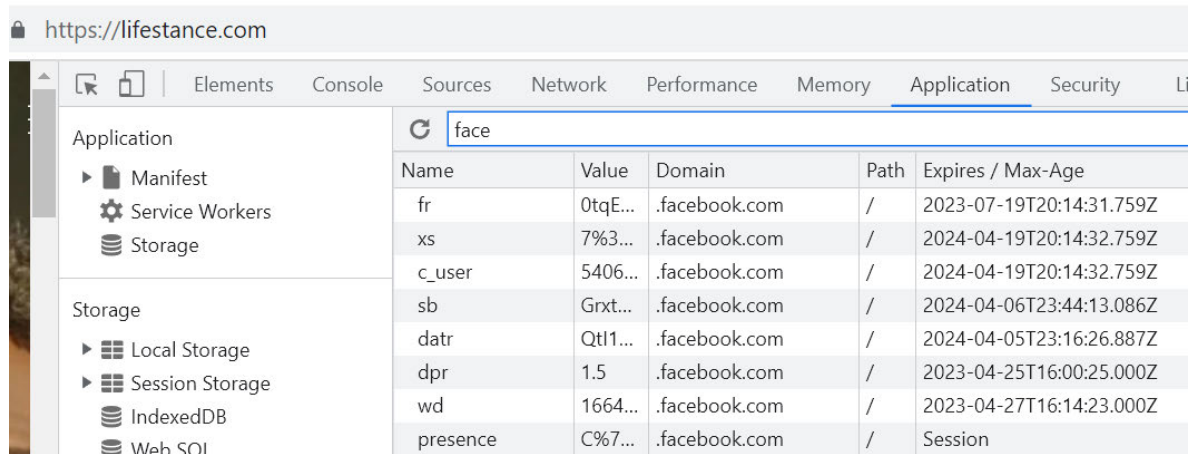


Figure 10.

153. When a visitor's browser has recently logged out of an account, Facebook compels the visitor's browser to send a smaller set of cookies⁵¹:

fr	00Zp...	.facebook.com
wd	1156...	.facebook.com
sb	qqAz...	.facebook.com
datr	Malz...	.facebook.com

Figure 11.

154. The fr cookie contains, at least, an encrypted Facebook ID and browser identifier.⁵² Facebook, at a minimum, uses the fr cookie to identify users.⁵³

155. At each stage, Defendant also utilized the _fbp cookie, which attaches to a browser as a first-party cookie, and which Facebook uses to identify a browser and a

⁵¹ 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.

⁵² 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 Jan. 16, 2024).

⁵³ *Cookies & other storage technologies*, FACEBOOK.COM, <https://www.facebook.com/policy/cookies/> (last visited Jan. 16, 2024).

1 user:⁵⁴

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

3 **Figure 12.**

4 156. The fr cookie expires after 90 days unless the visitor's browser logs back
5 into Facebook.⁵⁵ If that happens, the time resets, and another 90 days begins to accrue.

6 157. The _fbp cookie expires after 90 days unless the visitor's browser accesses
7 the same website.⁵⁶ If that happens, the time resets, and another 90 days begins to accrue.

8 158. The Facebook Tracking Pixel uses both first- and third-party cookies. A
9 first-party cookie is "created by the website the user is visiting"—i.e., Defendant.⁵⁷

10 159. A third-party cookie is "created by a website with a domain name other than
11 the one the user is currently visiting"—i.e., Facebook.⁵⁸

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

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

17 162. As shown in the above figures, Defendant sent these identifiers with the
18 event data.

19 163. Plaintiffs never consented, agreed, authorized, or otherwise permitted
20 Defendant to disclose their personally identifiable information and protected health

21 ⁵⁴ *Id.*

22 ⁵⁵ *Id.*

23 ⁵⁶ *Id.*

24 ⁵⁷ *First-Party Cookie*, PCMAG.COM,
25 <https://www.pcmag.com/encyclopedia/term/first-party-cookie> (last visited Jan. 16,
26 2024). This is confirmable by using developer tools to inspect a website's cookies and
track network activity.

27 ⁵⁸ *Third-Party Cookie*, PCMAG.COM,
28 <https://www.pcmag.com/encyclopedia/term/third-party-cookie> (last visited Jan. 16,
2024). This is also confirmable by tracking network activity.

1 information nor did she authorize any assistance with intercepting her communications.

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

5 165. Despite this, Defendant knowingly and intentionally disclosed Plaintiffs'
6 PHI to Facebook.

7 ***E. LifeStance Does Not Disclose That It Sends Private Information to Third***
8 ***Parties for Marketing Purposes.***

9 166. LifeStance represents to patients and visitors to its Website that it will only
10 disclose PHI provided to it under certain circumstances, ***none of which apply here.***⁵⁹

11 167. Defendant's privacy policy does ***not*** permit Defendant to use and disclose
12 Plaintiffs' and Class Members' Private Information for marketing purposes. In fact,
13 LifeStance acknowledges that it must obtain Users' "written authorization" to use or to
14 disclose PHI; "[s]pecific, examples, of uses or disclosures that require written
15 authorization include: Marketing activities (unless an exception applies)."⁶⁰

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

21 169. The Pixel, which is embedded in and throughout the Website, collects search
22 queries regarding users' personal information including their name and email, their
23 medical conditions, treatment and/or specific providers. Even non-Facebook users can be
24 individually identified via the information gathered on the Website, like an IP address or
25
26

27 ⁵⁹ <https://lifestance.com/privacy-policy/> (last visited Jan. 16, 2024).

28 ⁶⁰ *Id.*

1 personal device identifying information.⁶¹

2 ***F. Facebook’s Business Tools & Customization.***

3 170. The Pixel is customizable and programmable, meaning that the website
4 owner controls which of its web pages contain the Pixel and which events are tracked and
5 transmitted to Facebook.

6 171. The process of adding the Pixel to webpages is a multi-step process that
7 must be undertaken *by the website owner*.⁶²

8 172. Facebook guides the website owner through setting up the Pixel during the
9 setup process. Specifically, Facebook explains that there are two steps to set up a pixel:

- 10 1. Create your pixel and set up the pixel base code on your
11 website. You can use a partner integration if one is available
12 to you or you can manually add code to your website.
- 13 2. Set up events on your website to measure the actions you
14 care about, like making a purchase. You can use a partner
15 integration, the point-and-click event setup tool, or you can
16 manually add code to your website.⁶³

17 173. Aside from the various steps to embed and activate the Pixel, website
18 owners, like LifeStance, must also agree to Facebook’s Business Tools Terms by which
19 Facebook requires website owners using the Pixel to “represent and warrant” that they
20 have adequately and prominently notified users about the collection, sharing and usage
21 of data through Facebook’s Business Tools (including the Pixel)⁶⁴ and that websites “will

21 ⁶¹ This is precisely the type of information for which HIPAA requires the use of de-
22 identification techniques to protect patient privacy. See <https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html>, HHS.GOV (last visited
23 Jan. 16, 2024).

23 ⁶² *Business Help Center: How to set up and install a Meta Pixel*,
24 <https://www.facebook.com/business/help/952192354843755?id=1205376682832142>
25 (last visited Jan. 9, 2024); see Ivan Mana, *How to Set Up & Install the Facebook Pixel (in 2022)*, <https://www.youtube.com/watch?v=ynTNs5FAUm8> (last visited Jan. 9, 2024).

26 ⁶³ *Id.*

27 ⁶⁴ *Meta Business Tools Terms*,
28 https://www.facebook.com/legal/business?paipv=0&eav=AfbOvnb7E0sZ-wzgCW6xNLFKEOEvh_fr6JjkMINTJNqN7i1R-3MPh5caFgmdgAOxbL8&_rdr (last

1 not share Business Tool Data . . . that [websites] know or reasonably should know . . .
 2 includes health, financial information or other categories of sensitive information”⁶⁵

3 174. Once fully loaded and operational, the Pixel prompts the Users’ web
 4 browser to transmit specific information based on parameters set by the website owner.
 5 This customizable nature of the Meta Pixel allows the website owner to determine which
 6 webpages contain the Pixel, which events are tracked and shared with Facebook and
 7 whether the tracked events are standard (chosen from the list of 18 provided by Facebook)
 8 or custom (defined by the website owner). For example, the Pixel can be set to capture
 9 the URLs visited by website visitors via a “PageView” event, or to capture the exact inner
 10 text of buttons clicked by a visitor, via a “SubscribedButtonClick” event.

11 175. The Business Tools are automatically configured to capture “Standard
 12 Events,” such as when a user visits a particular webpage, that webpage’s Universal
 13 Resource Locator (“URL”) and metadata, button clicks, etc.⁶⁶

14 176. Advertisers, such as LifeStance, can track other User actions and can create
 15 their own tracking parameters by building a “custom event.”⁶⁷

16
 17 visited Jan. 9, 2024) (“When you use any of the Meta Business Tools to send us or
 18 otherwise enable the collection of Business Tool Data . . . , these Business Tools Terms
 govern the use of that data”).

19 ⁶⁵ *Id.*; see also Pratyush Deep Kotoky, *Facebook collects personal data on abortion*
 20 *seekers: Report* (June 16, 2022) [https://www.newsbytesapp.com/news/science/facebook-](https://www.newsbytesapp.com/news/science/facebook-collects-personal-data-on-abortion-seekers/story)
 21 [collects-personal-data-on-abortion-seekers/story](https://www.newsbytesapp.com/news/science/facebook-collects-personal-data-on-abortion-seekers/story) (quoting Facebook spokesman Dale
 Hogan as saying that it is “against [Facebook’s] policies for websites and apps to send
 sensitive health data about people through [its] Business Tools”) (last visited Jan. 9,
 2024).

22 ⁶⁶ *Specifications for Facebook Pixel Standard Events*,
 23 <https://www.facebook.com/business/help/402791146561655?id=1205376682832142>
 (last visited Jan. 9, 2024); see also META PIXEL, GUIDES, ADVANCED,
 24 <https://developers.facebook.com/docs/facebook-pixel/advanced/> (last visited Jan. 9,
 2024); BEST PRACTICES FOR META PIXEL SETUP,
 25 <https://www.facebook.com/business/help/218844828315224?id=1205376682832142>
 (last visited Jan. 9, 2024); APP EVENTS API,
 26 <https://developers.facebook.com/docs/marketing-api/app-event-api/> (last visited Jan. 9,
 2024).

27 ⁶⁷ ABOUT STANDARD AND CUSTOM WEBSITE EVENTS,
 28 <https://www.facebook.com/business/help/964258670337005?id=1205376682832142>
 (last visited Jan. 9, 2024).

177. When a User accesses a webpage that is hosting 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.

178. This additional, simultaneous secret transmission contains the original GET request sent to the host website, along with additional data that the Pixel is configured to collect. This transmission is initiated by Facebook code and concurrent with the communications with the host website. Two sets of code are thus automatically run as part of the browser’s attempt to load and read LifeStance’s Website—LifeStance’s own code and Facebook’s embedded code.

179. LifeStance tracked users through “PageView,” “Microdata” and “SubscribedButtonClick” events as well as custom events such as a “FindTelehealth” event. These events disclosed at least the following:

- Users’ search queries;
- When Users clicked to use the telehealth waiting room;
- When Users clicked which state they were in for the telehealth waiting room;
- When Users clicked to access and review conditions treated by LifeStance;
- When Users clicked to search for therapists and
- When Users clicked to call a therapist.

180. Accordingly, during the same transmissions, the Website routinely provides Facebook with its patients’ Facebook IDs, IP addresses and/or device IDs and the other information they input into LifeStance’s Website, including not only their medical searches, treatment requests and the webpages they view, but, upon information and good faith belief, also their location, name, email address and/or phone number.

181. This is precisely the type of identifying information that HIPAA requires healthcare providers to de-anonymize to protect the privacy of patients.⁶⁸ Plaintiffs’ and Class Members identities can be easily determined based on the Facebook ID, IP address and/or reverse lookup from the collection of other identifying information that was

⁶⁸ See <https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html> (last visited Jan. 9, 2024).

1 improperly disclosed.

2 182. Instead of taking proactive steps to verify that businesses using the Pixel
3 obtain the required consent, Meta uses an “honor system” under which Meta assumes
4 these businesses have “provided robust and sufficient prominent notice to users regarding
5 the Business Tool Data collection, sharing, and usage.”⁶⁹

6 183. After intercepting and collecting this information, Facebook processes it,
7 analyzes it and assimilates it into datasets like Core Audiences and Custom Audiences.
8 When the website visitor is also a Facebook user, the information collected via the Meta
9 Pixel is associated with the user’s Facebook ID that identifies their name and Facebook
10 profile—their real-world identity.

11 184. The pixel collects data regardless of whether the visitor has an account.
12 Facebook maintains “shadow profiles” on users without Facebook accounts, and links
13 the information collected via the Meta Pixel to the user’s real-world identity using their
14 shadow profile.⁷⁰

15 185. A User’s Facebook ID is linked to their Facebook profile, which generally
16 contains a wide range of demographic and other information about the user, including
17 pictures, personal interests, work history, relationship status and other details. Because
18 the user’s Facebook Profile ID uniquely identifies an individual’s Facebook account,
19 Facebook—or any ordinary person—can easily use the Facebook Profile ID to quickly
20 and easily locate, access and view the user’s corresponding Facebook profile. To find the
21 Facebook account associated with a c_user cookie, one simply needs to type
22 www.facebook.com/ followed by the c_user ID.

23 186. The Private Information disclosed via the Pixel allows Facebook to know
24 that a specific patient is seeking confidential medical care and the type of medical care

25 ⁶⁹ See Facebook Business Tools Terms,
26 <https://www.facebook.com/legal/terms/businessstools>.

27 ⁷⁰ See Russell Brandom, *Shadow Profiles Are the Biggest Flaw In Facebook’s*
28 *Privacy Defense*, (Apr 11, 2018),
<https://www.theverge.com/2018/4/11/17225482/facebook-shadow-profiles-zuckerberg-congress-data-privacy> (last visited Jan. 9, 2024).

1 being sought. Facebook then uses that information to sell advertising to LifeStance and
 2 other advertisers and/or sells that information to marketers who use it to online target
 3 Plaintiffs and Class Members.

4 187. Thus, the communications between patients and LifeStance, which are
 5 necessary to achieve the purpose of LifeStance's Website, are received by LifeStance and
 6 stored on their server before CAPI collects and sends the Private Information contained
 7 in those communications directly from LifeStance to Facebook. Client devices do not
 8 have access to host servers and thus cannot prevent (or even detect) this transmission.⁷¹

9 188. The Pixel Information Recipients track user data and communications for
 10 their own marketing purposes and for the marketing purposes of the website owner.
 11 Ultimately, the purpose of collecting user data is to make money.

12 189. Thus, without any knowledge, authorization or action by a user, website
 13 owners like LifeStance use source code to commandeer the user's computing device,
 14 causing the device to contemporaneously and invisibly re-direct the users'
 15 communications to third parties.

16 190. In this case, LifeStance employed the Pixel and CAPI, among other tracking
 17 technologies, to intercept, duplicate and re-direct Plaintiffs' and Class Members' Private
 18 Information to Facebook and the other Pixel Information Recipients.

19 ***G. Meta Encourages Healthcare Partners, Including LifeStance, to Upload***
 20 ***Patient Lists for Ad Targeting.***

21 191. Meta operates the world's largest social media company. Meta's revenue is
 22 derived almost entirely from selling targeted advertising. Meta's Health division is
 23 dedicated to marketing to and servicing Meta's healthcare partners. Meta defines its
 24 Partners to include businesses that use Meta's products, including the Meta Pixel or Meta

25 ⁷¹ Although prior to discovery there is no way to confirm that LifeStance has
 26 implemented CAPI or another workaround (as that would require accessing the host
 27 server), Facebook instructs website owners like LifeStance to "[u]se the Conversions API
 28 in addition to the [] Pixel, and share the same events using both tools," because such a
 "redundant event setup" allows LifeStance "to share website events [with Facebook] that
 the pixel may lose." See
<https://www.facebook.com/business/help/308855623839366?id=818859032317965>
 (last visited Jan. 9, 2024).

1 Audience Network tools to advertise, market or support their products and services.

2 192. Meta works with hundreds of Meta healthcare Partners, using Meta
3 Collection Tools to learn about visitors to their websites and leverage that information to
4 sell targeted advertising based on patients' online behavior. Meta's healthcare Partners
5 also use Meta's other ad targeting tools, including tools that involve uploading patient
6 lists to Meta.

7 193. Meta offers an ad targeting option called "Custom Audiences."

8 194. When a patient takes an action on a Meta healthcare partner's website
9 embedded with the Pixel, the Pixel will be triggered to send Meta "Event" data that Meta
10 matches to its users.

11 195. A web developer can then create a "Custom Audience" based on Events to
12 target advertisements to those patients.

13 196. The Pixel can then be used to measure the effectiveness of an advertising
14 campaign.⁷²

15 197. Meta also allows Meta healthcare partners to create a Custom Audience by
16 uploading a patient list to Meta. As Meta describes it:⁷³

17
18
19
20
21
22
23
24 ⁷² Meta Business Help Center, *About Customer List Custom Audiences* (2023),
25 <https://www.facebook.com/business/help/341425252616329?id=2469097953376494>;
26 *see also*, Meta Blueprint, *Connect your data with the Meta Pixel and Conversion API*
27 (2023), https://www.facebookblueprint.com/student/activity/212738?fbclid=IwAR3HPO1d_fnzRCUAhKGYsLqNA-VcLTMr3G_hxxFr3GZC_uFUcymuZopeNVw#/page/5fc6e67d4a46d349e9dff7fa.

28 ⁷³ Meta Business Help Center, *About Customer List Custom Audiences* (2023),
<https://www.facebook.com/business/help/341425252616329?id=2469097953376494>.

A Custom Audience made from a customer list is a type of audience you can create to connect with people who have already shown an interest in your business or product. It's made of information - called "identifiers" - you've collected about your customers (such as email, phone number and address) and provided to Meta. Prior to use, Meta hashes this information.

Then, we use a process called matching to match the hashed information with Meta technologies profiles so that you can advertise to your customers on Facebook, Instagram and Meta Audience Network. The more information you can provide, the better the match rate (which means our ability to make the matches). Meta doesn't learn any new identifying information about your customers.

198. Meta provides detailed instructions for healthcare partners to send their patients' Private Information to Meta through the customer list upload. For example:⁷⁴

Prepare your customer list in advance. To make a Custom Audience from a customer list, you provide us with information about your existing customers and we match this information with Meta profiles. The information on a customer list is known as an "identifier" (such as email, phone number, address) and we use it to help you find the audiences you want your ads to reach.

Your customer list can either be a CSV or TXT file that includes these identifiers. To get the best match rates, use as many identifiers as possible while following our formatting guidelines. You can hover over the identifiers to display the formatting rules and the correct column header. For example, **first name** would appear as **fn** as a column header in your list.

Alternatively, we have a file template you can download to help our system map to your identifiers more easily. (You can upload from Mailchimp as well.)

199. Meta healthcare partners can then use the Custom Audiences derived from their patient list with the Pixel and Pixel Events for Meta marketing campaigns and to measure the success of those campaigns.

H. LifeStance's Use of the Pixel Violated Its Own Privacy Policies.

200. LifeStance publishes a privacy policy that represent to patients and visitors to its Website that it will only disclose PII and PHI provided to it under certain circumstances, ***none of which apply here***.⁷⁵

201. LifeStance's privacy policy further represents that it "may share your

⁷⁴ Create a customer list custom audience, <https://www.facebook.com/business/help/170456843145568?id=2469097953376494> (last visited Jan. 9, 2024).

⁷⁵ See <https://lifestance.com/privacy-policy/>.

1 protected health information with a third party “business associates” that perform various
 2 activities (e.g., billing, transcription services, accounting services, legal services) for
 3 LifeStance. Whenever an arrangement between LifeStance and a business associate
 4 involves the use or disclosure of your protected health information, we will have a **written**
 5 **contract** that contains terms that will protect the privacy of your protected health
 6 information.”⁷⁶

7 202. Defendant’s Privacy Policy does **not** permit Defendant to use nor disclose
 8 Plaintiffs’ and Class Members’ PHI for marketing purposes without written
 9 authorization.⁷⁷

10 203. LifeStance acknowledges that “protected health information involving
 11 mental health”—the healthcare service that LifeStance provides—may be subject to
 12 special protections.⁷⁸

13 204. LifeStance breached its own privacy policy by unlawfully intercepting and
 14 disclosing Users’ Private Information to third parties, the Pixel Information Recipients,
 15 without obtaining patients’ consent or authorization.

16 ***I. LifeStance’s Disclosure of PHI Without Informed Consent Violates HIPAA.***

17 205. Defendant’s disclosure of Plaintiffs’ and Class Members’ Private
 18 Information to entities like Facebook also violated HIPAA.

19 206. LifeStance’s disclosure of Plaintiffs’ and Class Members’ Private
 20 Information to entities like Facebook violated HIPAA’s Privacy Rule, which defines
 21 “individually identifiable health information” as “a subset of health information,
 22 including demographic information collected from an individual” that is (1) “created or
 23 received by a health care provider;” (2) “[r]elates to the past, present, or future physical
 24 or mental health or condition of an individual; the provision of health care to an
 25

26 ⁷⁶ *Id.*

27 ⁷⁷ *Id.*

28 ⁷⁸ *Id.*

individual; or the past, present, or future payment for the 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.

207. 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. § 164.502.⁷⁹

208. The Privacy Rule broadly defines protected health information as individually identifiable health information that is “transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium.” 45 C.F.R. § 160.103.

209. Here, as described *supra*, LifeStance provided patient information to third parties in violation of the Privacy Rule—and its own Privacy Policy. An individual or corporation violates the HIPAA Privacy Rule if it knowingly: “(1) uses or causes to be used a unique health identifier; [or] (2) obtains individually identifiable health information relating to an individual.”

210. The statute states that a “person ... shall be considered to have obtained or disclosed individually identifiable health information ... if the information is maintained by a covered entity ... and the individual obtained or disclosed such information without authorization.” 42 U.S.C. § 1320(d)(6).

211. Violation of 42 U.S.C. § 1320(d)(6) is subject to criminal penalties where “the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm.” 42 U.S.C. § 1320(d)(6)(b). In such cases, an entity that knowingly obtains individually

⁷⁹ 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.”

1 identifiable health information relating to an individual “shall be fined not more than
2 \$250,000, imprisoned not more than 10 years, or both.” 42 U.S.C. § 1320(d)(6)(b)(1).

3 212. HIPAA also requires LifeStance to “review and modify the security
4 measures implemented . . . as needed to continue provision of reasonable and appropriate
5 protection of electronic protected health information.” 45 C.F.R. § 164.306(c), and to
6 “[i]mplement technical policies and procedures for electronic information systems that
7 maintain electronic protected health information to allow access only to those persons or
8 software programs that have been granted access rights,” 45 C.F.R. § 164.312(a)(1)—
9 which LifeStance failed to do.

10 213. Under HIPAA, LifeStance may not disclose PII about a patient, potential
11 patient or household member of a patient for marketing purposes without the patient’s
12 express written authorization. *See* HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.501;
13 164.508(a)(3), 164.514(b)(2)(i).

14 214. LifeStance further failed to comply with other HIPAA safeguard regulations
15 as follows:

- 16 a) Failing to ensure the confidentiality and integrity of
17 electronic PHI that LifeStance created, received, maintained
18 and transmitted in violation of 45 C.F.R. section
19 164.306(a)(1);
- 20 b) Failing to implement policies and procedures to prevent,
21 detect, contain and correct security violations in violation of
22 45 C.F.R. section 164.308(a)(1);
- 23 c) Failing to identify and respond to suspected or known
24 security incidents and mitigate harmful effects of security
25 incidents known to LifeStance in violation of 45 C.F.R.
26 section 164.308(a)(6)(ii);
- 27 d) Failing to protect against reasonably anticipated threats or
28 hazards to the security or integrity of electronic PHI in
violation of 45 C.F.R. section 164.306(a)(2);
- e) Failing to protect against reasonably anticipated uses or

disclosures of electronic PHI not permitted under the privacy rules pertaining to individually identifiable health information in violation of 45 C.F.R. section 164.306(a)(3), and

- f) Failing to design, implement and enforce policies and procedures that would establish physical and administrative safeguards to reasonably safeguard PHI in violation of 45 C.F.R. section 164.530(c).

215. 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.”⁸⁰

216. 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.”⁸¹

217. Defendant’s placing of a third-party tracking code on its Website is a violation of Plaintiffs’ and Class Members’ privacy rights under HIPAA’s Privacy Rule. While Plaintiffs do not bring a claim under HIPAA itself, this violation demonstrates LifeStance’s wrongdoing relevant to other claims and establishes its duty to maintain patient privacy.

218. Technology companies are under particular scrutiny because they already have access to a massive trove of information about people, which they use to serve their

⁸⁰ *Marketing*, <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/marketing/index.html>, HHS.GOV (last visited Jan. 16, 2024).

⁸¹ *‘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 Jan. 16, 2024).

own purposes. For instance, the health data Google collects could eventually help it micro-target advertisements to people with certain health conditions.

219. 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.⁸²

220. 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.⁸³

221. LifeStance gave away Plaintiffs’ and Class Members’ private communications and transactions on its Website 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.

222. In disclosing the content of Plaintiffs and the Class Members’ communications, LifeStance had a purpose that was tortious, criminal and designed to violate state constitutional and statutory provisions.⁸⁴

J. LifeStance Violated Industry Standards.

223. A medical provider’s duty of confidentiality is embedded in the physician-patient and hospital-patient relationship—it is a cardinal rule.

224. The American Medical Association’s (“AMA”) Code of Medical Ethics contains numerous rules protecting the privacy of patient data and communications.

⁸² *Id.*

⁸³ 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 Jan. 16, 2024).

⁸⁴ While Plaintiffs do not bring a claim under HIPAA itself, this violation demonstrates LifeStance’s wrongdoing relevant to other claims and establishes its duty to maintain patient privacy.

1 225. AMA Code of Ethics Opinion 3.1.1 provides:

2 Protecting information gathered in association with the care of
3 the patient is a core value in health care... Patient privacy
4 encompasses a number of aspects, including, ... personal data
(informational privacy)[.]⁸⁵

5 226. AMA Code of Medical Ethics Opinion 3.2.4 provides:

6 Information gathered and recorded in association with the care
7 of the patient is confidential. Patients are entitled to expect that
8 the sensitive personal information they divulge will be used
9 solely to enable their physician to most effectively provide
10 needed services. Disclosing information for commercial
11 purposes without consent undermines trust, violates principles
12 of informed consent and confidentiality, and may harm the
13 integrity of the patient-physician relationship. Physicians who
14 propose to permit third-party access to specific patient
15 information for commercial purposes should: (a) Only provide
16 data that has been de-identified. [and] (b) Fully inform each
patient whose record would be involved (or the patient's
authorized surrogate when the individual lacks decision-
making capacity about the purposes for which access would be
granted.⁸⁶

17 227. LifeStance's use of the Pixel also violates FTC data security guidelines. The
18 FTC has promulgated numerous guides for businesses, which highlight the importance
19 of implementing reasonable data security practices.

20 228. The FTC's October 2016 publication *Protecting Personal Information: A*
21 *Guide for Business*⁸⁷ established cyber-security guidelines for businesses. These
22 guidelines state that businesses should protect the personal patient information that they
23 keep, properly dispose of personal information that is no longer needed, encrypt
24 information stored on computer networks, understand their network vulnerabilities and

25
26 ⁸⁵ <https://www.ama-assn.org/sites/ama-assn.org/files/corp/media-browser/code-of-medical-ethics-chapter-3.pdf> (last visited Jan. 9, 2024).

27 ⁸⁶ *Id.*

28 ⁸⁷ *See* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Jan. 9, 2024).

1 implement policies to correct any security problems.

2 229. In fact, the FTC has recently brought enforcement actions against several
3 healthcare companies, including Premom, BetterHelp, GoodRx and Flow Health for
4 conveying information—or enabling an inference—about their consumers’ health to
5 unauthorized third parties without the consumers’ consent.

6 230. Like the telehealth companies fined by the FTC in recent years, LifeStance
7 failed to implement these basic, industry-wide data security practices.

8 ***K. Plaintiffs’ & Class Members’ Reasonable Expectation of Privacy.***

9 231. Plaintiffs and Class Members were aware of Defendant’s duty of
10 confidentiality when they sought medical services from Defendant.

11 232. Indeed, at all times when Plaintiffs and Class Members provided their PII
12 and PHI to Defendant, they each had a reasonable expectation that the information would
13 remain private and that Defendant would not share the Private Information with third
14 parties for a commercial purpose, unrelated to patient care.

15 233. Privacy polls and studies show that the overwhelming majority of
16 Americans consider obtaining an individual’s affirmative consent before a company
17 collects and shares its customers’ data to be one of the most important privacy rights.

18 234. For example, a recent Consumer Reports study shows that 92% of
19 Americans believe that internet companies and websites should be required to obtain
20 consent before selling or sharing consumer data, and the same percentage believe those
21 companies and websites should be required to provide consumers with a complete list of
22 the data that is collected about them.⁸⁸

23 235. Personal data privacy and obtaining consent to share Private Information are
24 material to Plaintiffs and Class Members.

25 236. Plaintiffs’ and Class Members’ reasonable expectations of privacy in their
26

27 ⁸⁸ *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New*
28 *Survey Finds*, (May 11, 2017), <https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety-a3980496907/> (last visited Jan. 9, 2024).

1 PII/PHI are grounded in, among other things, Defendant's status as a healthcare provider,
2 Defendant's common law obligation to maintain the confidentiality of patients' PII/PHI,
3 state and federal laws protecting the confidentiality of medical information, state and
4 federal laws protecting the confidentiality of communications and computer data, state
5 laws prohibiting the unauthorized use and disclosure of personal means of identification,
6 and Defendant's express and implied promises of confidentiality.

7 ***L. The Information LifeStance Discloses to Third Parties Is PHI.***

8 237. IP addresses are PII.

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

13 239. An IP address is a number that identifies the address of a device connected
14 to the Internet.

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

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

19 242. Facebook tracks every IP address ever associated with a Facebook user.

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

23 244. Under HIPAA, an IP address is considered personally identifiable
24 information.

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

28 246. 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).

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

M. LifeStance was Enriched & Benefitted from the Use of the Pixel & Other Tracking Technologies.

248. One of the primary reasons that LifeStance decided to embed the Pixel and other tracking technologies on its Website was to improve marketing by creating campaigns that maximize conversions and thereby decrease costs to LifeStance and boost its revenues.

249. After receiving individually identifiable patient health information communicated on LifeStance’s Website, Facebook forwards this data, and its analysis of this data, to LifeStance.

250. LifeStance then uses this data and analysis for its own commercial purposes that include understanding how Users utilize its Website.

251. LifeStance also receives an additional commercial benefit from using Facebook’s tracking tools, such as the Pixel and CAPI, namely being able to serve more targeted advertisements to existing and prospective patients on their Meta accounts such as Facebook and Instagram.

252. Facebook advertises its Pixel as a piece of code “that can help you better understand the *effectiveness of your advertising* and the actions people take on your site, like visiting a page or adding an item to their cart. You’ll also be able to see when customers took an action after seeing your ad on Facebook and Instagram, which can help you with retargeting. And when you use the CAPI alongside the Pixel, it creates a more reliable connection that helps the delivery system *decrease your costs*.”⁸⁹

⁸⁹ *What is the Meta Pixel*, <https://www.facebook.com/business/tools/meta-pixel> (emphasis added) (last visited Jan. 9, 2024).

1 253. Retargeting is a form of online marketing that targets users with
2 advertisements based on previous internet communications and interactions. In
3 particular, retargeting operates through code and tracking pixels placed on a website and
4 cookies to track website visitors and then places advertisements on other websites the
5 visitor goes to later.⁹⁰

6 254. The process of increasing conversions and retargeting occurs in the
7 healthcare context by sending a successful action on a health care website back to
8 Facebook via the tracking technologies and the Pixel embedded on, in this case,
9 LifeStance's Website. For example, when a User searches for therapists or medical
10 conditions or treatment on LifeStance's Website, that information is sent to Facebook.
11 Facebook can then use its data on the User to find more users to click on a LifeStance ad
12 and ensure that those users targeted are more likely to convert.⁹¹

13 255. Through this process, the Pixel loads and captures as much data as possible
14 when a User loads a telehealth website that has installed the Pixel. The information the
15 Pixel captures, "includes URL names of pages visited, and actions taken—all of which
16 could be potential examples of health information."⁹²

17 256. Plaintiffs' and Class Members' Private Information has considerable value
18 as highly monetizable data especially insofar as it allows companies to gain insight into
19 their customers so that they can perform targeted advertising and boost their revenues.

20 257. In exchange for disclosing the Private Information of their account holders
21 and patients, LifeStance is compensated by the Pixel Information Recipients in the form
22 of enhanced advertising services and more cost-efficient marketing on their platform.

23 258. But companies have started to warn about the potential HIPAA violations
24

25 ⁹⁰ *The complex world of healthcare retargeting*, <https://www.medicodigital.com/the-complicated-world-of-healthcare-retargeting/> (last visited Jan. 9, 2024).

26 ⁹¹ *See, e.g., How to Make Facebook Ads HIPAA Compliant and Still Get Conversion*
27 *Tracking* (Mar. 14, 2023), <https://www.freshpaint.io/blog/how-to-make-facebook-ads-hipaa-compliant-and-still-get-conversion-tracking> (last visited Jan. 9, 2024).

28 ⁹² *Id.*

1 associated with using pixels and tracking technologies because many such trackers are
2 not HIPAA-compliant or are only HIPAA-compliant if certain steps are taken.⁹³

3 259. For example, Freshpaint, a healthcare marketing vendor, cautioned that
4 “Meta isn’t HIPAA-compliant. They don’t sign BAAs, and the Meta Pixel acts like a
5 giant personal user data vacuum sending PHI to Meta servers,” and “[i]f you followed
6 the Facebook (or other general) documentation to set up your ads and conversion tracking
7 using the Meta Pixel, remove the Pixel now.”⁹⁴

8 260. Medico Digital also warns that “retargeting requires sensitivity, logic and
9 intricate handling. When done well, it can be a highly effective digital marketing tool.
10 But when done badly, it could have serious consequences.”⁹⁵

11 261. Whether a user has a Facebook profile is not indicative of damages because
12 Facebook creates shadow profiles, and at least one court has recognized that the pixels’
13 ability to track comprehensive browsing history is also relevant. *See, e.g., Brown v.*
14 *Google LLC*, 525 F. Supp. 3d 1049, 1078–79 (N.D. Cal. 2021) (finding a reasonable
15 expectation of privacy where Google combined the unique identifier of the user it collects
16 from websites and Google Cookies that it collects across the internet on the same user).

17 262. LifeStance retargeted Users and potential patients, including Plaintiffs and
18 Class Members.

19 263. Thus, utilizing the Pixels directly benefits LifeStance by, among other
20 things, reducing the cost of advertising and retargeting.

21 **N. *Plaintiffs’ Private Information is Extremely Valuable.***

22 264. Plaintiffs’ and Class Members’ Private Information had value, and
23 LifeStance’s disclosure and interception harmed Plaintiffs and the Class by not
24

25 ⁹³ *See The guide to HIPAA compliance in analytics*, [https://campaign.piwik.pro/wp-](https://campaign.piwik.pro/wp-content/uploads/2023/10/The-guide-to-HIPAA-compliance-in-analytics.pdf)
26 [content/uploads/2023/10/The-guide-to-HIPAA-compliance-in-analytics.pdf](https://campaign.piwik.pro/wp-content/uploads/2023/10/The-guide-to-HIPAA-compliance-in-analytics.pdf) (explaining
that Google Analytics 4 is not HIPAA-compliant) (last visited Jan. 9, 2024).

27 ⁹⁴ *How To Make Facebook Ads HIPAA Compliant and Still Get Conversion*
Tracking, *supra* note 91.

28 ⁹⁵ *The complex world of healthcare retargeting*, *supra* note 90.

1 compensating them for the value of their Private Information and, in turn, decreasing the
2 value of their Private Information.

3 265. Technology companies are under particular scrutiny because they already
4 have access to a massive trove of information about people, which they use to serve their
5 own purposes, including potentially micro-targeting advertisements to people with
6 certain health conditions.

7 266. The value of personal data is well understood and generally accepted as a
8 form of currency. It is now incontrovertible that a robust market for this data undergirds
9 the tech economy.

10 267. The robust market for Internet user data has been analogized to the “oil” of
11 the tech industry.⁹⁶ A 2015 article from TechCrunch accurately noted that “[d]ata has
12 become a strategic asset that allows companies to acquire or maintain a competitive
13 edge.”⁹⁷ That article noted that the value of a single Internet user—or really, a single
14 user’s data—varied from about \$15 to more than \$40.

15 268. Conservative estimates suggest that in 2018, Internet companies earned
16 \$202 per American user from mining and selling data (after costs).⁹⁸ That figure is only
17 due to keep increasing; estimates for 2022 were as high as \$434 per user, for a total of
18 more than \$200 billion industry wide.

19 269. Professor Paul M. Schwartz, writing in the Harvard Law Review, notes:
20 “Personal information is an important currency in the new millennium. The monetary
21 value of personal data is large and still growing, and corporate America is moving quickly
22 to profit from the trend. Companies view this information as a corporate asset and have
23

24 ⁹⁶ See <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> (last visited Jan. 9, 2024).

25 ⁹⁷ See <https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/> (last visited
26 Jan. 9, 2024).

27 ⁹⁸ See *What Your Data is Really Worth to Facebook* (Jul. 12, 2019),
28 <https://washingtonmonthly.com/2019/07/12/what-your-data-is-really-worth-to-facebook/> (last visited Jan. 9, 2024).

1 invested heavily in software that facilitates the collection of consumer information.”⁹⁹

2 270. This economic value has been leveraged largely by corporations who
3 pioneered the methods of its extraction, analysis and use. However, the data also has
4 economic value to Internet users. Market exchanges have sprung up where individual
5 users like Plaintiffs herein can sell or monetize their own data. For example, Nielsen Data
6 and Mobile Computer will pay Internet users for their data.¹⁰⁰

7 271. There are countless examples of this kind of market, which is growing more
8 robust as information asymmetries are diminished through revelations to users as to how
9 their data is being collected and used.

10 272. Courts recognize the value of personal information and the harm when it is
11 disclosed without consent. *See, e.g., In re Facebook Privacy Litig.*, 572 F. App’x 494,
12 494 (9th Cir. 2014) (holding that plaintiffs’ allegations that they were harmed by the
13 dissemination of their personal information and by losing the sales value of that
14 information were sufficient to show damages for their breach of contract and fraud
15 claims); *In re Marriott Int’l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447,
16 462 (D. Md. 2020) (recognizing “the value that personal identifying information has in
17 our increasingly digital economy”).

18 273. Healthcare data is particularly valuable on the black market because it often
19 contains all of an individual’s PII and medical conditions as opposed to a single piece of
20 information that may be found in a financial breach.

21 274. Healthcare data is incredibly valuable because, unlike a stolen credit card
22 that can be easily canceled, most people are unaware that their medical information has
23 been sold. Once it has been detected, it can take years to undo the damage caused.

24 275. The value of health data is well-known and various reports have been
25 conducted to identify its value.

26 _____
27 ⁹⁹ Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 Harv. L. Rev. 2055,
2056-57 (2004).

28 ¹⁰⁰ *See 10 Apps for Selling Your Data for Cash*, <https://wallethacks.com/apps-for-selling-your-data/> (last visited Jan. 9, 2024).

276. Specifically, in 2023, the Value Examiner published a report entitled Valuing Healthcare Data. The report focused on the rise in providers, software firms and other companies that are increasingly seeking to acquire clinical patient data from healthcare organizations. The report cautioned providers that they must de-identify data and that purchasers and sellers of “such data should ensure it is priced at fair market value to mitigate any regulatory risk.”¹⁰¹

277. Trustwave Global Security published a report entitled The Value of Data. With respect to healthcare data records, the report found that they may be valued at up to \$250 per record on the black market, compared to \$5.40 for the next highest value record (a payment card).¹⁰²

278. The value of health data has also been reported extensively in the media. For example, Time Magazine published an article in 2017 titled “How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry,” in which it described the extensive market for health data and observed that the market for information was both lucrative and a significant risk to privacy.¹⁰³

279. Similarly, CNBC published an article in 2019 in which it observed that “[d]e-identified patient data has become its own small economy: There’s a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers.”¹⁰⁴

280. The dramatic difference in the price of healthcare data compared to other forms of private information commonly sold is evidence of the value of PHI.

281. These rates are assumed to be discounted because they do not operate in

¹⁰¹ See <https://www.healthcapital.com/researchmaterialdocuments/publishedarticles/Valuing%20Healthcare%20Data.pdf> (last visited Jan. 9, 2024).

¹⁰² See <https://www.imprivata.com/blog/healthcare-data-new-prize-hackers> (last visited Jan. 9, 2024) (citing https://www.infopoint-security.de/media/TrustwaveValue_of_Data_Report_Final_PDF.pdf).

¹⁰³ See <https://time.com/4588104/medical-data-industry/> (last visited Jan. 9, 2024).

¹⁰⁴ See <https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html> (last visited Jan. 9, 2024).

1 competitive markets, but rather, in an illegal marketplace. If a criminal can sell other
 2 Internet users' stolen data, surely Internet users can sell their own data.

3 282. In short, there is a quantifiable economic value to Internet users' data that is
 4 greater than zero. The exact number will be a matter for experts to determine.

5 283. LifeStance gave away Plaintiffs' and Class Members' communications and
 6 transactions on its Website without permission.

7 284. The unauthorized access to Plaintiffs' and Class Members' personal and
 8 Private Information has diminished the value of that information, resulting in harm to
 9 Website Users, including Plaintiffs and Class Members.

10 285. Plaintiffs have a continuing interest in ensuring that their future
 11 communications with LifeStance are protected and safeguarded from future
 12 unauthorized disclosure.

13 **REPRESENTATIVE PLAINTIFFS' EXPERIENCES**

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

15 286. Plaintiff Strong initially became aware of LifeStance via an advertisement
 16 on Facebook.

17 287. Plaintiff Strong started receiving healthcare services from LifeStance in or
 18 about March of 2022 and continued such activity thereafter through early 2023. Plaintiff
 19 Strong received those services via Defendant's Website, which she accessed on her phone
 20 and computer.

21 288. Plaintiff Strong used Defendant's Website to [REDACTED]
 22 [REDACTED], communicate with healthcare providers,
 23 research particular medical concerns and treatments, fill out forms, schedule and attend
 24 appointments and perform other tasks related to her specific medical inquiries and
 25 treatment.

26 289. In using LifeStance's Website, Plaintiff Strong also provided her medical
 27 history and her height, weight and ethnicity.

28 290. In particular, Plaintiff Strong used LifeStance's Website every time she had

1 [REDACTED]. In doing so, Plaintiff Strong was required to enter
2 the state she was located in, her name and her address.

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

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

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

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

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

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

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

1 298. After disclosing her private medical information to Defendant, Plaintiff
2 Strong began receiving targeted advertisements on her social media accounts such as
3 Facebook, including those related to her specific [REDACTED]
4 [REDACTED] (including but not limited to, [REDACTED]).

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

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

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

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

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

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

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

20 305. Plaintiff Yick used Defendant's Website to communicate with healthcare
21 providers who [REDACTED], research particular medical concerns and
22 treatments, fill out forms, schedule and attend appointments and perform other tasks
23 related to her specific medical inquiries and treatment.

24 306. In particular, Plaintiff Yick used Defendant's Website to search for a
25 [REDACTED].

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

1 Defendant.

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

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

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

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

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

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

24 314. After disclosing her private medical information to Defendant, Plaintiff
25 Yick began receiving targeted advertisements on her social media accounts such as
26 Facebook, including those related to her specific [REDACTED]
27 [REDACTED] (including but not limited to, [REDACTED]).

28 315. Defendant did not inform Plaintiff Yick that it had shared her Private

1 Information with Facebook.

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

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

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

10 TOLLING

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

16 CLASS ACTION ALLEGATIONS

17 320. Plaintiffs bring this action on behalf of themselves and on behalf of various
18 classes of persons similarly situated, as defined below, pursuant to Rule 23(b)(2),
19 23(b)(3) and 23(c)(4) of the Federal Rules of Civil Procedure. The Class is a national
20 class with the subclasses defined below. Within the national Class are the California
21 Class and New York Class, each with the subclasses defined below.

22 321. The Class or Classes are defined as:

23 All natural persons who are members of the following Settlement
24 Subclass 1 or Settlement Subclass 2:

- 25 i. **Subclass 1**: All members of LifeStance's total patient population
26 who booked at least one session through LifeStance's online
booking tool, accessed through LifeStance's public website
lifestance.com, between March 1, 2020 and April 30, 2023.
- 27 ii. **Subclass 2**: All other members of LifeStance's total patient
28 population between March 1, 2020 and April 30, 2023, not
including those in Settlement Subclass 1.

322. The “California Class” that Plaintiff Yick seeks to represent is defined as:

- i. **California Subclass 1:** All members of LifeStance’s patient population residing in the State of California who booked at least one session through LifeStance’s online booking tool, accessed through LifeStance’s public website [lifestance.com](https://www.lifestance.com), between March 1, 2020 and April 30, 2023.
- ii. **California Subclass 2:** All other members of LifeStance’s patient population residing in the State of California between March 1, 2020 and April 30, 2023, not including those in Settlement Subclass 1.

323. The “New York Class” that Plaintiff Strong seeks to represent is defined as:

- i. **New York Subclass 1:** All members of LifeStance’s total patient population residing in the State of New York who booked at least one session through LifeStance’s online booking tool, accessed through LifeStance’s public website [lifestance.com](https://www.lifestance.com), between March 1, 2020 and April 30, 2023.
- ii. **New York Subclass 2:** All other members of LifeStance’s total patient population residing in the State of New York between March 1, 2020 and April 30, 2023, not including those in Settlement Subclass 1.

324. The Nationwide Class, the California Class and the New York Class (and any subclasses) are referred to collectively as the “Classes.” Excluded from the Class and Classes are: (i) Defendant’s officers and directors and any entity in which Defendant or its parents have a controlling interest; (ii) all Class Members who timely and validly request exclusion; and (iii) Defendant’s Counsel and in-house counsel who advised Defendant on the Action. Also excluded from the Class are members of the judiciary to whom this case is assigned, their families, and members of their staff.

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

326. **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.

327. **Commonality & Predominance, Fed. R. Civ. P. 23(a)(2) and (b)(3).**

1 Questions of law and fact common to the Classes exist and predominate over any
2 questions affecting only individual Class Members. These include:

- 3 a. Whether and to what extent Defendant has a duty to protect the
4 PII and PHI of Plaintiffs and Class Members;
- 5 b. Whether Defendant owes a duty to not disclose the PII and PHI
6 of Plaintiffs and Class Members to unauthorized third parties;
- 7 c. Whether Defendant violated its privacy policy by disclosing the
8 PII and PHI of Plaintiffs and Class Members to Facebook,
9 Google, and/or other third parties.
- 10 d. Whether Defendant adequately, promptly and accurately
11 informed Plaintiffs and Class Members that their PII and PHI
12 would be disclosed to third parties;
- 13 e. Whether Defendant violated the law by failing to promptly
14 notify Plaintiffs and Class Members that their PII and PHI had
15 been compromised;
- 16 f. Whether Defendant adequately addressed and fixed the practices
17 which permitted the disclosure of patient PHI and PII;
- 18 g. Whether Defendant engaged in unfair, unlawful or deceptive
19 practices by failing to safeguard the PII and PHI of Plaintiffs and
20 Class Members;
- 21 h. Whether Defendant violated consumer protection statutes
22 invoked herein;
- 23 i. Whether Plaintiffs and Class Members are entitled to actual,
24 consequential, and/or nominal damages as a result of
25 Defendant's wrongful conduct;
- 26 j. Whether Defendant knowingly made false representations as to
27 its data security and/or privacy policy practices;
- 28 k. Whether Defendant knowingly omitted material representations

1 with respect to its data security and/or privacy policy practices;
2 and

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

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

12 329. **Adequacy, Fed. R. Civ. P. 23(a)(4).** Plaintiffs will fairly and adequately
13 represent and protect the interests of Class Members in that Plaintiffs have no disabling
14 conflicts of interest that would be antagonistic to those of the other Class Members.
15 Plaintiffs seek no relief that is antagonistic or adverse to the Class Members, and the
16 infringement of rights and the damages Plaintiffs have suffered are typical of other Class
17 Members. Plaintiffs have also retained counsel experienced in complex class action
18 litigation, and Plaintiffs intend to prosecute this action vigorously.

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

1 would still be economically impractical and impose a burden on the courts.

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

10 332. The nature of this action and the nature of laws available to Plaintiffs and
11 Class Members make the use of the class action device a particularly efficient and
12 appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs
13 alleged because Defendant would otherwise gain an unconscionable advantage since it
14 would be able to exploit and overwhelm the limited resources of each individual Class
15 Member with superior financial and legal resources; the costs of individual suits could
16 unreasonably consume the amounts that would be recovered; proof of a common course
17 of conduct to which Plaintiffs was exposed is representative of that experienced by the
18 Class and will establish the right of each Class Member to recover on the cause of action
19 alleged; and individual actions would create a risk of inconsistent results and would be
20 unnecessary and duplicative of this litigation.

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

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

28 335. **Class-wide Injunctive Relief, Fed. R. Civ. P. 23(b)(2).** Unless a Class-

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

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

- 12 ♦ Whether Defendant owes a legal duty to not disclose
 13 Plaintiffs' and Class Members' Private Information;
- 14 ♦ Whether Defendant owes a legal duty to not disclose
 15 Plaintiffs' and Class Members' Private Information under
 16 Defendant's privacy policy;
- 17 ♦ Whether Defendant breached a legal duty to Plaintiffs and
 18 Class Members to exercise due care in collecting, storing,
 19 using, and safeguarding their Private Information;
- 20 ♦ Whether Defendant failed to comply with its own policies
 21 and applicable laws, regulations, and industry standards
 22 relating to data security;
- 23 ♦ Whether Defendant adequately and accurately informed
 24 Plaintiffs and Class Members that their Private Information
 25 would be disclosed to third parties;
- 26 ♦ Whether Defendant failed to implement and maintain
 27 reasonable security procedures and practices appropriate to
 28 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**

337. The State of Arizona has a significant interest in regulating the conduct of

1 businesses operating within its borders.

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

7 339. The principal place of business and headquarters of LifeStance, located in
8 Scottsdale, Arizona, is the “nerve center” of its business activities—the place where its
9 high-level officers direct, control and coordinate its activities, including major policy,
10 financial and legal decisions.

11 340. Upon information and good faith belief, Defendant’s actions and corporate
12 decisions surrounding the allegations made in the Complaint were made from and in
13 Arizona.

14 341. Defendant’s breaches of duty to Plaintiffs and Class Members emanated
15 from Arizona.

16 342. Application of Arizona law to the Classes with respect to Plaintiffs’ and the
17 Classes’ common law claims is neither arbitrary nor fundamentally unfair because,
18 further to choice of law principles applicable to this action, the common law of Arizona
19 applies to the nationwide common law claims of all Class members. Additionally, given
20 Arizona’s significant interest in regulating the conduct of businesses operating within its
21 borders, and that Arizona has the most significant relationship to Defendant, as it is
22 headquartered in Arizona, there is no conflict in applying Arizona law to non-resident
23 consumers such as Plaintiffs and the Class members.

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

26 **CLAIMS FOR RELIEF**

27 **COUNT I**

28 **VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT**

Cal. Penal Code §§ 630, *et. Seq.*
(By Plaintiff Yick on Behalf of the California Class)

344. 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.

345. The California Invasion of Privacy Act (“CIPA”) is codified at California Penal Code §§ 630 to 638.

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

347. 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.

348. 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)[.]

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

350. At all relevant times, Defendant aided, employed, agreed with, and conspired with Facebook and Pixel Information Recipients to track and intercept Plaintiffs’ and Class Members’ internet communications while using Defendant’s

1 Website.

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

5 352. These communications were intercepted in California where Meta is
6 located.

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

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

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

- 16 a. The computer codes and programs Facebook used to track
17 Plaintiffs' and Class Members' communications while
they were navigating the Website;
- 18 b. Plaintiffs' and Class Members' browsers;
- 19 c. Plaintiffs' and Class Members' computing and mobile
20 devices;
- 21 d. Facebook's web and ad servers;
- 22 e. The web and ad servers from which Facebook tracked and
23 intercepted Plaintiffs' and Class Members'
communications while they were using a web browser to
access or navigate the Website;
- 24 f. The computer codes and programs used by Facebook to
25 effectuate its tracking and interception of Plaintiffs' and
Class Members' communications while they were using a
26 browser to visit the Website; and
- 27 g. The plan Facebook carried out to effectuate its tracking
28 and interception of Plaintiffs' and Class Members'
communications while they were using a web browser or
mobile application to visit the Website.

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

7 357. The patient communication information that Defendant transmits while
8 using the Pixel constitutes protected health information.

9 358. As demonstrated herein, Defendant violates CIPA by aiding and permitting
10 third parties to receive its patients' online communications in real time through its
11 Website without their consent.

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

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

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

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

28 **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)

363. 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.

364. 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.

365. “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.

366. Defendant is a “provider of health care” as defined by California Civil Code § 56.06(b).

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

368. As set forth above, device identifiers, web URLs, 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.

369. 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 Website, including but not limited to the following: patient medical

1 conditions, medical concerns, treatment(s) sought by the patients, medical specialty of
2 the doctor(s) searched for and selected by patients and appointment information.

3 370. The information described above constitutes medical information pursuant
4 to the CMIA because it is patient information derived from a provider of health care
5 regarding patients' medical treatment and physical condition, and this medical
6 information is linked with individually identifying information. *See* CAL. CIV. CODE §
7 56.05(i).

8 371. As demonstrated herein, Defendant fails to obtain its patients' authorization
9 for the disclosure of medical information and fails to disclose in its Privacy Policy that it
10 shares protected health information with Facebook or other third parties for marketing
11 purposes.

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

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

26 374. Based on the foregoing, Plaintiffs and Class Members seek nominal
27 damages, compensatory damages, punitive damages, attorney's fees and costs of
28 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 & Disclosure

(By Plaintiffs Strong & Yick on behalf of the Nationwide Class)

375. 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.

376. The Electronic Communications Privacy Act (“ECPA”) prohibits the intentional interception of the content of any electronic communication. 18 U.S.C. § 2511.

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

378. 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.

379. 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).

380. Electronic Communications. The transmission of PII and PHI between Plaintiffs and Class Members and Defendant’s Website 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).

381. 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).

382. Interception. The ECPA defines an interception as the “acquisition of the

1 contents of any wire, electronic, or oral communication through the use of any electronic,
 2 mechanical, or other device” and “contents . . . include any information concerning the
 3 substance, purport, or meaning of that communication.” 18 U.S.C. § 2510(4), (8).

4 383. Electronical, Mechanical, or Other Device. The ECPA defines “electronic,
 5 mechanical, or other device” as “any device ... which can be used to intercept a[n] ...
 6 electronic communication[.]” 18 U.S.C. § 2510(5).

7 384. The following constitute “devices” within the meaning of 18 U.S.C. §
 8 2510(5):

- 9 a. The cookies LifeStance and Meta use to track Plaintiffs’ and the
 Class Members’ communications;
- 10 b. Plaintiffs’ and Class Members’ browsers;
- 11 c. Plaintiffs’ and Class Members’ computing devices;
- 12 d. Defendant’s web-servers and
- 13 e. The Pixels deployed by Defendant to effectuate sending
 14 and acquiring Users’ and patients’ sensitive
 15 communications.

16 385. Plaintiffs and Class Members’ interactions with LifeStance’s Website are
 17 electronic communications under the ECPA.

18 386. By utilizing and embedding the Pixel on its Website, Defendant
 19 intentionally intercepted, endeavored to intercept, and/or procured another person to
 20 intercept, the electronic communications of Plaintiffs and Class Members, in violation of
 21 18 U.S.C. § 2511(1)(a).

22 387. Specifically, Defendant intercepted Plaintiffs’ and Class Members’
 23 electronic communications via the Meta Pixel, CAPI and other tracking technologies,
 24 which tracked, stored and unlawfully disclosed Plaintiffs’ and Class Members’ Private
 25 Information to third parties such as Facebook.

26 388. Defendant intercepted communications that include, but are not limited to,
 27 communications to/from Plaintiffs and Class Members regarding PII and PHI, including
 28 first and last name, address, IP address, Facebook ID, treatment information, medications

1 and scheduling details. Additionally, through the above-described tracking tools,
2 Defendant transmitted the communications about doctors, treatments and conditions,
3 including but not limited to the name(s), location(s) and specialty(s) of physicians’
4 Plaintiff searched for on Defendant’s Website. This information was, in turn, used by
5 third parties, such as Facebook, to) place Plaintiffs in specific health-related categories
6 and 2) target Plaintiffs with particular advertising associated with Plaintiffs’ specific
7 health conditions. Defendant knowingly transmits this data and does so for the purpose
8 of financial gain.

9 389. By intentionally disclosing or endeavoring to disclose Plaintiffs’ and Class
10 Members’ electronic communications to affiliates and other third parties, while knowing
11 or having reason to know that the information was obtained through the interception of
12 an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated
13 18 U.S.C. § 2511(1)(c).

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

19 391. Unauthorized Purpose. Defendant intentionally intercepted the contents of
20 Plaintiffs’ and Class Members’ electronic communications for the purpose of committing
21 a criminal or tortious act in violation of the Constitution or laws of the United States or
22 of any State—namely, invasion of privacy, among others.

23 392. Any party exception in 18 U.S.C. § 2511(2)(d) does not apply. The party
24 exception in § 2511(2)(d) does not permit a party that intercepts or causes interception to
25 escape liability if the communication is intercepted for the purpose of committing any
26 tortious or criminal act in violation of the Constitution or laws of the United States or of
27 any State. Here, as alleged above, Defendant violated a provision of the Health Insurance
28 Portability and Accountability Act, specifically 42 U.S.C. § 1320d-6(a)(3). This

1 provision imposes a criminal penalty for knowingly disclosing individually identifiable
 2 health information (IIHI) to a third party. HIPAA defines IIHI as:

3 any information, including demographic information
 4 collected from an individual, that—(A) is created or
 5 received by a health care provider ... (B) *relates to the past,*
 6 *present, or future physical or mental health or condition*
 7 *of an individual, the provision of health care to an*
 8 *individual, or the past, present, or future payment for the*
 9 *provision of health care to an individual, and (i) identifies*
 10 *the individual; or (ii) with respect to which there is a*
 11 *reasonable basis to believe that the information can be*
 12 *used to identify the individual.*¹⁰⁵

13 393. Plaintiffs' information that Defendant disclosed to third parties qualifies as
 14 IIHI, and Defendant violated Plaintiffs' expectations of privacy, and constitutes tortious
 15 and/or criminal conduct through a violation of 42 U.S.C. § 1320d(6). Defendant used the
 16 wire or electronic communications to increase its profit margins. Defendant specifically
 17 used the Pixel to track and utilize Plaintiffs' and Class Members' PII and PHI for financial
 18 gain.

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

21 395. Plaintiffs and Class Members did not authorize Defendant to acquire the
 22 content of their communications for purposes of invading Plaintiffs' privacy via the Pixel
 23 tracking code. Plaintiffs and absent class members (all of whom are patients) had a
 24 reasonable expectation that Defendant would not re-direct their communications content
 25 to Facebook, Google or others attached to their personal identifiers in the absence of their
 26 knowledge or consent.

27 396. Any purported consent that Defendant received from Plaintiffs and Class
 28 Members was not valid.

397. In sending and in acquiring the content of Plaintiffs' and Class Members'

¹⁰⁵ *Id.* § 1320d-(6) (emphasis added).

1 communications relating to the browsing of Defendant's Website, researching medical
 2 conditions and treatment and scheduling appointments with doctors and therapists,
 3 Defendant's purpose was tortious, criminal and designed to violate federal and state legal
 4 provisions including a knowing intrusion into a private place or matter that would be
 5 highly offensive to a reasonable person.

6 398. LifeStance's acquisition of patient communications that were used and
 7 disclosed to Facebook and other third parties was also done for purposes of committing
 8 criminal and tortious acts in violation of the laws of the United States, Arizona and New
 9 York.

10 399. Consumers have the right to rely upon the promises that companies make to
 11 them. LifeStance accomplished its tracking and retargeting through deceit and disregard,
 12 such that an actionable claim may be made, in that it was accomplished through source
 13 code that cause Facebook pixels and cookies (including but not limited to the fbp, ga and
 14 gid cookies) and other tracking technologies to be deposited on Plaintiffs' and Class
 15 members' computing devices as "first-party" cookies that are not blocked.

16 400. LifeStance's scheme or artifice to defraud in this action consists of:

- 17 a. the false and misleading statements and omissions in its
 18 privacy policies set forth above, including the statements
 19 and omissions recited in the claims below;
- 20 b. the placement of the 'fbp' cookie on patient computing
 21 devices disguised as a first-party cookie on LifeStance's
 22 Website rather than a third-party cookie from Meta.

23 401. LifeStance acted with the intent to defraud in that it willfully invaded and
 24 took Plaintiffs' and Class Members' property:

- 25 a. property rights to the confidentiality of Private Information
 26 and their right to determine whether such information
 27 remains confidential and exclusive right to determine who
 28 may collect and/or use such information for marketing
 purposes; and

- 1 b. property rights to determine who has access to their
2 computing devices.

3 402. LifeStance acted with the intent to defraud in that it willfully invaded and
4 took Plaintiffs' and Class Members' property:

- 5 a. with knowledge that (1) LifeStance did not have the right to
6 share such data without written authorization; (2) courts had
7 determined that a healthcare providers' use of the Meta
8 Pixel gave rise to claims for invasion of privacy and
9 violations of state criminal statutes; (3) a reasonable
10 Facebook user would not understand that Meta was
11 collecting their Private Information based on their activities
12 on LifeStance's Website; (4) "a reasonable Facebook user
13 would be shocked to realize" the extent of Meta's collection
14 of Private Information; (5) a Covered Incident had occurred
15 which required a report to be made to the FTC pursuant to
16 Meta's consent decrees with the FTC and (6) the subsequent
17 use of health information for advertising was a further
18 invasion of such property rights in making their own
19 exclusive use of their Private Information for any purpose
20 not related to the provision of their healthcare; and

- 21 b. with the intent to (1) acquire Plaintiffs and Class Members'
22 Private Information without their authorization and without
23 their healthcare providers or covered entities obtaining the
24 right to share such information; (2) use Plaintiffs' and Class
25 Members' Private Information without their authorization
26 and (3) gain access to Plaintiffs' and Class Members'
27 personal computing devices through the 'fbp' cookie
28 disguised as a first-party cookie.

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

25 404. As a direct and proximate result of LifeStance's violation of the ECPA,
26 Plaintiffs and Class Members were damaged by LifeStance's conduct.

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

406. 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

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)

407. 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 California Class.

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

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

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

411. 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.

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

413. 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.

414. 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),

1 *et seq.*; and 18 U.S.C. § 1030, *et seq.*

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

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

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

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

13 419. Defendant was in sole possession of and had a duty to disclose the material
14 information that Plaintiff Yick's and California Class Members' Private Information was
15 being shared with a third party.

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

27 421. Had Defendant disclosed that it shared Private Information with third
28 parties, Plaintiff Yick would not have used Defendant's services or would have paid

1 considerably less for those services.

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

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

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

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

22 426. As a direct result of its unlawful practices, Defendant has been unjustly
23 enriched and should be required to make restitution to Plaintiff Yick and California Class
24 Members pursuant to §§ 17203 and 17204 of the California Business & Professions Code,
25 disgorgement of all profits accruing to Defendant because of its unlawful business
26 practices, declaratory relief, attorney's fees and costs (pursuant to Cal. Code Civ. Proc.
27 §1021.5) and injunctive or other equitable relief.

28 **COUNT V**

**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)**

427. 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.

428. 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.

429. 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.

430. 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.

431. 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.

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

433. 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.

434. Had Defendant disclosed that it shared Private Information with third parties, Plaintiff Yick would not have used Defendant’s services or would have paid

1 considerably less for those services.

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

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

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

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

21 439. As a direct result of its unfair practices, Defendant has been unjustly
22 enriched and should be required to make restitution to Plaintiff Yick and California Class
23 Members pursuant to §§ 17203 and 17204 of the California Business & Professions Code,
24 disgorgement of all profits accruing to Defendant because of its unlawful business
25 practices, declaratory relief, attorney's fees and costs (pursuant to Cal. Code Civ. Proc.
26 §1021.5) and injunctive or other equitable relief.

27 **COUNT VI**

28 **VIOLATION OF ARIZONA CONSUMER FRAUD ACT, A.R.S. §44-1521, *et seq.***

(On behalf of Plaintiffs & the Nationwide Class)

440. 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.

441. 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.

442. 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.

443. 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.

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

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

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

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

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

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

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

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

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

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

28 454. Defendant's conduct complained of is ongoing. Injunctive and declaratory

1 relief is necessary and appropriate to prevent further violations.

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

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

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

12 **COUNT VII**

13 **VIOLATIONS OF NEW YORK GENERAL BUSINESS LAW**

14 **N.Y. Gen. Bus. Law § 349, *et seq.***

15 **(On Behalf of Plaintiff Strong & the New York Subclass)**

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

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

22 460. GBL §349(a) provides:

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

26 461. By reason of the conduct alleged herein, Defendant engaged in unlawful
27 practices within the meaning of the N.Y. Gen. Bus. Law § 349.

28 462. 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.

463. By the acts and conduct alleged herein, Defendant committed deceptive acts

1 and practices in violation of the N.Y. Gen. Bus. Law § 349, by:

- 2 a. promising to maintain the privacy and security of Plaintiffs' and
- 3 Class Members' protected health information as required by law;
- 4 b. installing the Facebook Pixel to operate as intended and transmit
- 5 Plaintiffs' and Class Members' Private Information without their
- 6 authorization to Facebook;
- 7 c. failing to disclose or omitting material facts to Plaintiffs and Class
- 8 Members regarding the disclosure of their Private Information to
- 9 Facebook;
- 10 d. failing to take proper action to ensure the Pixel was configured to
- 11 prevent unlawful disclosure of Plaintiffs' and Class Members'
- 12 Private Information and
- 13 e. unlawfully disclosing Plaintiffs' and Class Members' Private
- 14 Information to Facebook.

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

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

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

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

28 468. 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.

469. Defendant's disclosures of Plaintiff Strong's and New York Class Members'

1 Private Information were made without their knowledge, consent, or authorization, and
2 were unprivileged.

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

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

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

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

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

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

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

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

26 **COUNT VIII**

27 **COMMON LAW INVASION OF PRIVACY – INTRUSION UPON SECLUSION** 28 **(By Plaintiffs Strong & Yick on behalf of the Nationwide Class)**

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

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

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

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

15 482. Plaintiffs and Nationwide Class Members had a reasonable expectation of
16 privacy because Defendant's privacy policy states that they can expect such privacy and
17 they were entitled to the protection of their Private Information from disclosure to
18 unauthorized third parties, including the Pixel Information Recipients.

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

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

24 485. LifeStance failed to protect Plaintiffs' and Class Members' Private
25 Information and acted knowingly when it installed the Pixel and tracking technologies
26 onto the Website because the purpose of the Pixel is to track and disseminate Users'
27 communications on the Website for marketing and advertising.

28 486. As a result of Defendant's actions, Plaintiffs and Nationwide Class Members

1 have suffered harm and injury, including but not limited to an invasion of their privacy
2 rights.

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

6 488. Based on the foregoing, Plaintiffs and Nationwide Class Members seek
7 appropriate relief for these injuries, including but not limited to damages that will
8 reasonably compensate Plaintiffs and Nationwide Class Members for the harm to their
9 privacy interests as a result of the intrusion(s) upon Plaintiffs' and Nationwide Class
10 Members' privacy.

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

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

- 16 A. For an Order certifying the Classes (as defined herein)
17 and appointing Plaintiffs as Class Representatives and
Plaintiffs' counsel as Class Counsel;
- 18 B. For equitable relief enjoining Defendant from engaging
19 in the wrongful conduct complained of herein pertaining
20 to the misuse and/or disclosure of Plaintiffs' and Class
21 Members' Private Information, and from refusing to
issue prompt, complete and accurate disclosures to
Plaintiffs and Class Members;
- 22 C. For equitable relief compelling Defendant to utilize
23 appropriate methods and policies with respect to
24 consumer data collection, storage and safety, and to
disclose with specificity the type of PII and PHI
disclosed to third parties;
- 25 D. For equitable relief requiring restitution and
26 disgorgement of the revenues wrongfully retained as a
result of Defendant's wrongful conduct;
- 27 E. For an award of actual damages, compensatory damages,
28 statutory damages and statutory penalties, in an amount
to be determined, as allowable by law;

- 1 F. For an award of punitive damages, as allowable by law;
2 G. For an award of attorneys' fees and costs, and any other
3 expense, including expert witness fees;
4 H. Pre- and post-judgment interest on any amounts awarded
5 and
6 I. Such other and further relief as this Honorable Court
7 may deem just and proper.

8 **DEMAND FOR JURY TRIAL**

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

11 Respectfully submitted,

12 **ZIMMERMAN REED LLP**

13 Dated: December 3, 2025

14 By: s/ Ryan Ellersick

15 Hart L. Robinovitch
16 Ryan J. Ellersick
17 14648 N. Scottsdale Road, Suite 130
18 Scottsdale, AZ 85254
19 Telephone: (480) 348-6400
20 Facsimile: (480) 348-6415
21 hart.robinovitch@zimmreed.com
22 ryan.ellersick@zimmreed.com

23 **ALMEIDA LAW GROUP LLC**

24 David S. Almeida (*pro hac vice*)
25 Elena A. Belov (*pro hac vice*)
26 849 W. Webster Avenue
27 Chicago, Illinois 60614
28 Tel: (312) 576-3024
david@almeidalawgroup.com
elena@almeidalawgroup.com

Attorneys for Plaintiffs & the Classes