

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

LILY NGUYEN, EMZORA MITCHELL and FRANK ORTEGA, <i>on behalf of themselves and all others similarly situated</i> , Plaintiffs, v. ABBOTT LABORATORIES, INC. Defendant.	Case No. 1:24-cv-8289 JURY TRIAL DEMANDED
--	--

CLASS ACTION COMPLAINT

Plaintiffs Lily Nguyen, Emzora Mitchell and Frank Ortega (“Plaintiffs”) bring this class action lawsuit on behalf of themselves, and all others similarly situated, by and through undersigned counsel, and hereby allege the following against Defendant Abbott Laboratories, Inc. d/b/a Freestyle Libre (“Defendant” or “Abbott”). Facts pertaining to Plaintiffs and their experiences and circumstances are alleged based upon personal knowledge, and all other facts alleged herein are based upon investigation of counsel and—where indicated—upon information and good faith belief.

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. The mishandling of such information can

have serious consequences including, but certainly not limited to, discrimination in the workplace and/or denial of insurance coverage.¹

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

3. The need for data privacy, 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 technology companies, health data is some of the most extensive, valuable and controversial.²

4. Plaintiffs bring this class action lawsuit to address Abbott's illegal and widespread practice of disclosing its customers' confidential personally identifiable information ("PII") and

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) <https://www.wired.com/story/substance-abuse-telehealth-privacy-tracking-tech/> (last visited Sep. 5, 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), <https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites> (last visited Sep. 5, 2024).

² Protected and highly sensitive medical information collected by telehealth companies includes many categories from intimate details of an individual's conditions, symptoms, diagnoses and treatments to personally identifying information to unique codes which can identify and connect individuals to the collecting entity. See Molly Osberg & Dhruv Mehrotra, *The Spooky, Loosely Regulated World of Online Therapy*, JEZEBEL (Feb. 19, 2020), <https://jezebel.com/the-spooky-loosely-regulated-world-of-online-therapy-1841791137> (last visited Sep. 5, 2024).

protected health information (“PHI” and collectively with PII, “Private Information”) to unauthorized third parties, including Meta Platforms, Inc. d/b/a Meta (“Facebook” or “Meta”) and Google LLC (“Google”), without consent, through the use of tracking software that is embedded in Defendant’s website for its Freestyle Libre products.³

5. Defendant Abbott is an American corporation that manufactures and sells medical devices and health care equipment worldwide.

6. Abbott specializes in cardiovascular, diagnostics, diabetes and neuromodulation products.⁴

7. In order to market and sell its products, Defendant owns, controls and maintains various websites, including the website for its FreeStyle Libre continuous glucose monitors (“CGM”), www.freestyle.abbott/us-en/ and its webpages (the “Website”).

8. Abbott encourages its customers to use the Website to, among other things, review its FreeStyle Libre CGM systems, compare their cost and insurance coverage, and to try one of the FreeStyle Libre CGM systems.⁵

9. Defendant’s unlawful privacy violations occurred and continue to occur because of the tracking technologies that it installed on its Website including, but not limited to, the Meta

³ While this Complaint focuses on tracking tools from Facebook and Google, research shows that Defendant also embedded tracking codes from a number of other marketing companies including Amazon, AppNexus (Ad Nexus Media), Bing (Microsoft), BidSwitch, BlueKai (Oracle), Casale Media, DemDex (Adobe), Dotomi, eXelate (Nielsen), GumGum, Krux, Media Innovation Group, Mediarithmics SAS, Neustar, Inc., OpenX, Pinterest, Pubmatic, Rubicon Project, Scorecard Research, Semasio, Smart AdServer, StickyAds.tv, Taboola, Tremor Hub (Taptica), TripleLift, Twitter, Yahoo, and 360 Polaris (Improve Digital).

⁴ See *About Abbott*, DRUGWATCH, <https://www.drugwatch.com/manufacturers/abbott-laboratories> (last visited Sep. 5, 2024).

⁵ See *FreeStyle Libre*, ABBOTT, <https://www.freestyle.abbott/us-en/home.html> (last visited Sep. 5, 2024).

Pixel (the “Meta Pixel” or the “Pixel”), Google Analytics, Google DoubleClick and Google Tag Manager, (collectively with the Pixel, “Tracking Tools”).⁶

10. The Tracking Tools used by the Defendant allow unauthorized third parties to intercept the contents of customer communications, view customers’ Private Information, mine its customer’s Private Information for purposes unrelated to the provision of healthcare and further monetize it to deliver targeted advertisements, among other things.

11. In doing so, and by designing its Website in the manner described throughout this Complaint, Abbott knew or should have known that its customers would use the Website to communicate Private Information in conjunction with obtaining and receiving medical services and products from it.

12. Operating as designed and as implemented by Defendant, the Tracking Tools caused the Private Information that Plaintiffs and Class Members submitted to Defendant to be unlawfully disclosed to Facebook, alongside personal identifiers including their unique and persistent Facebook ID, IP address, and unique cookie values in violation of Health Insurance Portability and Accountability Act (“HIPAA”), state laws, industry standards and customer expectations.

13. By installing Tracking Tools, including the Pixel, on its Website, Defendant effectively planted a bug on Plaintiffs’ and Class Members’ web browsers that caused their communications with Defendant to be intercepted, accessed, viewed and captured by third parties in real time.

14. Facebook connects user data from Defendants’ Website to the individual’s

⁶ This Complaint contains images and evidence demonstrating the Meta Pixels and Google Tracking Tools are used on Defendant’s Website, but Plaintiffs (without the benefit of discovery) do not have access to every tracking tool that was previously installed on the Website.

Facebook ID (FID). The FID links the user to her/his Facebook profile, which contains detailed information about the profile owner's identity sufficient to identify them personally.

15. Similarly, Google “stores users’ logged-in identifier on non-Google websites...in its logs ... Whenever a user logs-in on non-Google websites, whether in private browsing mode or non-private browsing mode, the same identifier is associated with the data Google collects from the user’s browsing activities on that website. Google further logs all such data (private and non-private) within the same logs and uses these data for serving personalized ads.”⁷

16. Facebook tracks and collects data even on people who do not have a Facebook account or have deactivated their Facebook accounts. Those individuals can find themselves in an even worse situation because even though their Private Information is sent to Facebook—without their consent—they cannot clear past activity or disconnect the collection of future activity since they do not possess an account (or an active account).⁸

17. Then, completely unencumbered by any pretense of restriction or regulation, Facebook and Google, in turn, use that Private Information for various business purposes, including using such information to “improve” advertisers’ ability to target specific demographics and selling such information to third-party marketers who target those users online (through their Facebook, Instagram, Gmail and other social media and personal accounts):

Along with encouraging businesses to spend ad dollars, Facebook also receives the transmitted data, and can use it to hone its algorithms. Facebook can also use data from the pixel to link website visitors to their Facebook accounts, meaning businesses can reach the exact people who visited their

⁷ See *Brown v. Google LLC*, Case No. 4:20-cv-3664-YGR, 2023 WL 5029899 (N.D. Cal. Aug. 7, 2023) (order denying summary judgment and citing internal evidence from Google employees).

⁸ In the past, these were referenced as “ghost accounts” or “shadow profiles.” See Laura Hautula, *Shadow profiles: Facebook has information you didn’t hand over*, CNET (April 11, 2018), <https://www.cnet.com/news/privacy/shadow-profiles-facebook-has-information-you-didnt-hand-over/> (last visited Sep. 5, 2024).

sites. The pixel collects data regardless of whether the visitor has an account.⁹

18. Simply put, the health information disclosed through the Tracking Tools is personally identifiable.

19. In addition to the Tracking Tools, Plaintiffs also allege upon information and belief that Defendant also installed and implemented Facebook's Conversions Application Programming Interface ("CAPI") on its Website servers.¹⁰

20. Unlike the Facebook Pixel which co-opts a website user's browser and forces it to transmit information to Facebook in addition to the website owner, CAPI does not cause the user's browser to transmit information directly to Facebook. Instead, CAPI tracks the user's website interaction, including Private Information, records and stores that information on the website owner's servers, and then transmits the data to Facebook from the website owner's servers.^{11, 12} Indeed, Facebook markets CAPI as a "better measure [of] ad performance and attribution across your customer's full journey, from discovery to conversion. This helps you better understand how

⁹ See Colin Lecher & Ross Teixeira, *Facebook Watches Teens Online As They Prep For College*, THE MARKUP (Nov. 22, 2023), <https://themarkup.org/pixel-hunt/2023/11/22/facebook-watches-teens-online-as-they-prep-for-college> (stating that "[b]usinesses embed the pixel on their own websites voluntarily, to gather enough information on their customers so they can advertise to them later on Meta's social platforms") (last visited Sep. 5, 2024).

¹⁰ "CAPI works with your Facebook pixel to help improve the performance and measurement of your Facebook ad campaigns." *How To Implement Facebook Conversions API (in Shopify)*, FETCH & FUNNEL, <https://www.fetchfunnel.com/how-to-implement-facebook-conversions-api-in-shopify/> (last visited Sep. 5, 2024).

¹¹ *What is the Facebook Conversions API and how to use it*, REVEALBOT, <https://revealbot.com/blog/facebook-conversions-api/> (last visited Sep. 5, 2024).

¹² "Server events are linked to a dataset ID and are processed like events sent via the Meta Pixel... This means that server events may be used in measurement, reporting, or optimization in a similar way as other connection channels." *Conversions API*, META, <https://developers.facebook.com/docs/marketing-api/conversions-api> (last visited Sep. 5, 2024).

digital advertising impacts both online and offline results.”¹³

21. Because CAPI is located on the website owner’s servers and is not a bug planted onto the website user’s browser, it allows website owners like Defendant to circumvent any ad blockers or other denials of consent by the website user that would prevent the Pixel from sending website users’ Private Information to Facebook directly.

22. Defendant utilized the Pixel and CAPI data for marketing purposes to bolster its profits. The Facebook Pixel and CAPI are routinely used to target specific customers by utilizing data and information from users’ communications with the Website to build profiles for the purposes of retargeting and future marketing. Facebook also uses Plaintiffs’ and Class Members’ Private Information to create targeted advertisements based on the medical conditions and other information disclosed to Defendant.

23. Plaintiffs and Class Members used Defendant’s Website to submit information related to their past, present or future health conditions, including, for example, searches and requests for diabetes testing and monitoring equipment. Such Private Information would allow a third party, such as Facebook or Google, to know that a specific user was seeking testing products from Defendant for a specific medical condition.

24. Defendant is a healthcare entity and thus its disclosure of health and medical communications is tightly regulated.

25. The United States Department of Health and Human Services (“HHS”) has established “Standards for Privacy of Individually Identifiable Health Information” (also known as the “Privacy Rule”) governing how health care providers must safeguard and protect Private

¹³*About Conversions API, META*, <https://www.facebook.com/business/help/2041148702652965?id=818859032317965> (last visited Sep. 5, 2024).

Information. Under the HIPAA Privacy Rule, no health care provider may disclose a person's personally identifiable protected health information to a third party without express written authorization.

26. In addition, as explained further below, HHS has specifically warned healthcare regulated entities that tracking technologies like those used by Defendant transmit personally identifying information to third parties, including on the public portion of the website, and that such information should not be transmitted without a HIPAA-acceptable written authorization from the relevant patient.

27. The Federal Trade Commission ("FTC") has also warned healthcare entities that "even if you are not covered by HIPAA, you still have an obligation to protect against impermissible disclosures of personal health information under the FTC Act and the FTC Health Breach Notification Rule."¹⁴

28. Despite these warnings, Defendant embedded hidden Tracking Tools and, upon information and good faith belief, CAPI, on the Website and its servers, essentially planting a bug on customers' web browsers that forced them disclose private and confidential communications to third parties. Defendant did not disclose the presence of these Tracking Tools to its Website users and customers.

29. Healthcare customers simply do not anticipate or expect that their trusted healthcare provider will send personal health information or confidential medical information collected via its webpages to a hidden third party—let alone Facebook and Google, which both have a sordid history of privacy violations in pursuit of ever-increasing advertising revenue—without the

¹⁴ OCR & FTC Joint Letter re: Use of Online Tracking Technologies (July 20, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf (last visited Sep. 5, 2024).

customers' consent. Neither Plaintiffs nor any other Class Member signed a written authorization permitting Defendant to send their Private Information to Facebook or Google.

30. Rather than attempt to collect more and more confidential and protected health information, telehealth and diagnostic medical device companies should minimize data collection and storage to what is necessary to provide health care services. In practice, few do; rather, likely cognizant that consumers would not voluntarily provide this sensitive and protected information, these companies resort to doing so covertly by installing invisible tracking technologies on their websites to collect and monetize that data.¹⁵

31. Moreover, many companies do not publicly disclose what types of data will be shared — for instance, whether they collect users' contact information or aspects of their health data. By disclosing customer data to third parties for commercial use and providing little transparency into what data is shared and with whom, test providers make it more likely that sensitive data could be leaked, used to discriminate, and/or sold (and re-sold) by data brokers without oversight or consent.¹⁶

¹⁵ See, e.g., *Top Mental Health & Prayer Apps Fail Spectacularly at Privacy, Security*, MOZILLA (May 2, 2022), <https://foundation.mozilla.org/en/blog/top-mental-health-and-prayer-apps-fail-spectacularly-at-privacy-security/> (last visited Sep. 5, 2024).. Moreover, the policies of many telehealth providers fail to include specific limitations around data retention and deletion, instead relying on vague, catchall language.

¹⁶ Kaylana Mueller-Hsia & Laura Hecht-Fellala, *Evaluating the Privacy of At-Home Covid 19 Tests, The Tests Are Essential for Fighting the Pandemic, but Poor Privacy Policy Practices Could Discourage Some People from Using Them*, BRENNAN CENTER FOR JUSTICE (Jan. 19, 2021), <https://www.brennancenter.org/our-work/analysis-opinion/evaluating-privacy-covid-19-home-tests> (last visited Sep. 5, 2024).

32. In fact, Abbott assures its customers in its privacy policy that “We believe your personal information belongs to you. . . . Abbott does not sell Personal Information or disclose Personal Information to third parties to use for their own benefit without your consent.”¹⁷

33. As detailed herein, those statements are certainly suspect given Defendant’s outrageous, illegal and widespread practice of surreptitiously collecting and disclosing Plaintiffs’ and putative Class Members’ confidential Private Information to third party data brokers.

34. Defendant breached its statutory and common law obligations to Plaintiffs and Class Members by, *inter alia*: (i) failing to adequately review their marketing programs to ensure the Freestyle Libre 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, Google and/or others before doing so; (iv) failing to take steps to block the transmission of Plaintiffs’ and Class Members’ Private Information through Tracking Tools like the Facebook Pixel, Google Analytics or CAPI; (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 the Freestyle Libre Website to maintain the security, confidentiality and integrity of customer Private Information.

35. Consequently, Plaintiffs bring this action for legal and equitable remedies to address and rectify the illegal conduct and actions described herein, to enjoin Defendant from making similar disclosure of its customers’ Private Information in the future, and to fully articulate, *inter alia*, the specific Private Information it disclosed to third parties and to identify the recipients

¹⁷ See <https://web.archive.org/web/20230529223526/https://www.abbott.com/privacy-policy.html> (Abbott’s privacy policy in effect on May 29, 2023).

of that information.

36. Defendant breached its statutory and common law obligations to Plaintiffs and Class Members by, *inter alia*: (i) failing to remove or disengage technology that was known and designed to share web-users' information; (ii) failing to obtain the written consent of Plaintiffs and Class Members to disclose their Private Information to Facebook, Google or others; (iii) failing to take steps to block the transmission of Plaintiffs' and Class Members' Private Information through Tracking Tools like the Facebook Pixel or Google Analytics; (iv) failing to warn Plaintiffs and Class Members; and (v) otherwise failing to design, and monitor its Website to maintain the confidentiality and integrity of patient Private Information.

37. As a result of Defendant's conduct, Plaintiffs and Class Members have suffered numerous injuries, including: (i) invasion of privacy; (ii) loss of benefit of the bargain; (iii) diminution of value of their Private Information; (iv) statutory damages; and (v) the continued and ongoing risk to their Private Information.

38. Plaintiffs seek to remedy these harms and brings causes of action for (i) Violation of the Electronics Communication Privacy Act ("ECPA"), 18 U.S.C. § 2511(1), *et seq.*; (ii) Negligence; and (iii) Violation of the California Invasion of Privacy Act, Cal. Penal Code § 934.01 *et seq.*

PARTIES

39. Plaintiff Lily Nguyen is, and at all relevant times was, an individual residing in Kennesaw, Cobb County, in the State of Georgia.

40. Plaintiff Emzora Mitchell is, and at all relevant times was, an individual residing in Chicago, Cook County, in the State of Illinois.

41. Plaintiff Frank Ortega is, and at all relevant times was, an individual residing in

Reseda, the County of Los Angeles, in the State of California.

42. Defendant Abbott is a domestic corporation incorporated in the State of Delaware, with a principal place of business at 100 Abbott Park Road, Abbott Park, Illinois 60064.

JURISDICTION & VENUE

43. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1331 because it arises under the laws of the United States and under 28 U.S.C. § 1332(d) because this case is brought as a class action where the amount in controversy exceeds the sum or value of \$5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

44. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein from part of the same case or controversy.

45. This Court has personal jurisdiction over Defendant because Defendant regularly conducts business in Illinois, its principal place of business is in Illinois and a substantial portion of the acts and omissions giving rise to Plaintiffs' claims occurred in and emanated in Illinois.

46. Venue is proper under 28 U.S.C § 1391(a)-(d) because: (i) a substantial part of the events giving rise to this action occurred in this judicial district, including decisions made by Defendant's governance and management personnel or inaction by those individuals that led to the unauthorized sharing of Plaintiffs' and Class Members' Private Information; (ii) Defendant's principal place of business is located in this judicial district; (iii) Defendant collects and redistributes Class Members' Private Information in this judicial district and (iv) Defendant caused harm to Class Members residing in this judicial district.

COMMON FACTUAL ALLEGATIONS

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

47. The surreptitious collection and divulgence of Private Information is an extremely serious data security and privacy issue. Both the FTC and the Office for Civil Rights (“OCR”) of the Department of Health and Human Services have, in recent months, reiterated the importance of and necessity for data security and privacy concerning health information.

48. For instance, the FTC recently published a bulletin entitled *Protecting the privacy of health information: A baker’s dozen takeaways from FTC cases*, in which it noted that “[h]ealth information is not just about medications, procedures, and diagnoses. ***Rather, it is anything that conveys information—or enables an inference—about a consumer’s health.*** Indeed, [recent FTC enforcement actions involving] *Premom, BetterHelp, GoodRx and Flo Health make clear that the fact that a consumer is using a particular health-related app or website—one related to mental health or fertility, for example—or how they interact with that app (say, turning ‘pregnancy mode’ on or off) may itself be health information.*”¹⁸

49. The FTC is unequivocal in its stance, informing healthcare companies—in no uncertain terms—that they should ***not*** use tracking technologies to collect sensitive health information and disclose it to various platforms without informed consent:

Don’t use behind-the-scenes tracking technologies that contradict your privacy promises or otherwise harm consumers.

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 See Elisa Jillison, *Protecting the privacy of health information: A baker’s dozen takeaways from FTC cases*, FTC BUSINESS BLOG (July 25, 2023) (emphasis added), <https://www.ftc.gov/business-guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-ftc-cases> (last visited Sep. 5, 2024).

[Recent FTC enforcement actions such as] *BetterHelp*, *GoodRx*, *Premom*, and *Flo* make clear that practices like that *may run afoul of the FTC Act if they violate privacy promises or if the company fails to get consumers' affirmative express consent for the disclosure of sensitive health information*.¹⁹

50. The federal government is taking these violations of health data privacy and security seriously as recent high-profile FTC settlements against several telehealth companies evidence. For example, last year, the FTC imposed a \$1.5 million penalty on GoodRx for violating the FTC Act by sharing its customers' sensitive PHI with advertising companies and platforms, including Facebook, Google and Criteo, and reached a \$7.8 million settlement with the online counseling service BetterHelp, resolving allegations that the company shared customer health data with Facebook and Snapchat for advertising purposes. Similarly, Easy Healthcare was ordered to pay a \$100,000 civil penalty for violating the Health Breach Notification Rule when its ovulation tracking app Premon shared health data for advertising purposes.²⁰

¹⁹ *Id.* (emphasis added) (further noting that *GoodRx* & *Premom* underscore that this conduct may also violate the Health Breach Notification Rule, which requires notification to consumers, the FTC and, in some cases, the media, of disclosures of health information without consumers' authorization).

²⁰ See *How FTC Enforcement Actions Will Impact Telehealth Data Privacy*, Health IT Security, <https://healthitsecurity.com/features/how-ftc-enforcement-actions-will-impact-telehealth-data-privacy> (last visited Sep. 5, 2024); see also Allison Grande, *FTC Targets GoodRx In 1st Action Under Health Breach Rule*, Law360 (Feb. 1, 2023), 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 wield its full range of enforcement powers when it dinged GoodRx for allegedly sharing sensitive health data with advertisers, teeing up a big year for the agency and boosting efforts to regulate data privacy on a larger scale.") (last visited Sep. 5, 2024); <https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-gives-final-approval-order-banning-betterhelp-sharing-sensitive-health-data-advertising>; *FTC Gives Final Approval to Order Banning BetterHelp from Sharing Sensitive Health Data for Advertising, Requiring It to Pay \$7.8 Million*, <https://www.ftc.gov/news-events/news/press-releases/2023/05/ovulation-tracking-app-premon-will-be-barred-sharing-health-data-advertising-under-proposed-ftc> (last visited Sep. 5, 2024).

51. In July 2023, federal regulators sent a letter to approximately 130 healthcare providers warning them about using online tracking technologies that could result in unauthorized disclosures of Private Information to third parties. The letter highlighted the “risks and concerns about the use of technologies, such as the Meta/Facebook Pixel and Google Analytics, that can track a user’s online activities,” and warned about “[i]mpermissible disclosures of an individual’s personal health information to third parties” that could “result in a wide range of harms to an individual or others.” According to the letter, “[s]uch disclosures can reveal sensitive information including health conditions, diagnoses, medications, medical treatments, frequency of visits to health care professionals, where an individual seeks medical treatment, and more.”²¹

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

Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals’ HIPAA-compliant authorizations, would constitute impermissible disclosures.²²

²¹ Office for Civil Rights, *Use of Online Tracking Technologies* (July 20, 2023), <https://www.hhs.gov/sites/default/files/use-online-tracking-technologies.pdf> (last visited Sep. 5, 2024).

²² See *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, DEPT. OF HEALTH AND HUMAN SERVICES, <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html> (noting that “IIHI collected on a regulated entity’s website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, such as in some circumstances IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services.”) (last visited Sep. 5, 2024).

This guidance was recently vacated *in part* by the Federal District Court for the Northern District of Texas due to the court finding it in part to be the product of improper rulemaking and it is cited

53. The OCR Bulletin discusses the harms that disclosure may cause persons:

An impermissible disclosure of an individual's PHI not only violates the Privacy Rule but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft, financial loss, ***discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI.*** Such disclosures can reveal incredibly sensitive information about an individual, ***including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment.*** While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, ***because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI only as expressly permitted or required by the HIPAA Privacy Rule.***²³

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

for reference only until the OCR updates its guidance, should it do so in the future. *See American Hosp. Ass'n. v. Becerra*, No. 4:23-cv-01110-P, ECF No. 67 (S.D. Tex., Jun. 20, 2024). Notably, the court's order found only that the OCR's guidance regarding covered entities disclosing to third parties users' IP addresses while users navigated *unauthenticated public webpages* ("UPWs") was improper rulemaking. The Order in no way affects or undermines the OCR's guidance regarding covered entities disclosing personal identifiers, such as Google or Facebook identifiers, to third parties while patients were making appointments for particular conditions, paying medical bills or logging into (or using) a patient portal. *See id.* at 3-4, 31, n. 8 (vacating the OCR guidance with respect to the "Proscribed Combination" defined as "circumstances where an online technology connects (1) an individual's IP address with (2) a visit to a UPW addressing specific health conditions or healthcare providers" but stating that "[s]uch vacatur is not intended to, and should not be construed as, limiting the legal operability of other guidance in the germane HHS document."). Furthermore, the FTC bulletin on the same topics remains untouched, as do the FTC's enforcement actions against healthcare providers for committing the same actions alleged herein).

²³ *Id.* (emphasis added).

55. For instance, in the aptly titled report “*Out of Control*”: *Dozens of Telehealth Startups Sent Sensitive Health Information to Big Tech Companies*, a joint investigation by STAT and THE MARKUP of 50 direct-to-consumer telehealth companies reported that telehealth companies or virtual care websites were providing sensitive medical information they collect to the world’s largest advertising platforms.²⁴

56. Many telehealth sites had at least one tracker—from Meta, Google, TikTok, Bing, Snap, Twitter, LinkedIn and/or Pinterest—that collected patients’ answers to medical intake questions.²⁵

B. Abbott Installed and Configured Facebook Tracking Tools on its Website.

57. Facebook operates the world’s largest social media company and generated \$117 billion in revenue in 2021, roughly 97% of which came from selling advertising space.²⁶

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

²⁴ Todd Feathers, Katie Palmer (STAT) & Simon Fondrie-Teitler, “*Out Of Control*”: *Dozens of Telehealth Startups Sent Sensitive Health Information to Big Tech Companies: An investigation by The Markup and STAT found 49 out of 50 telehealth websites sharing health data via Big Tech’s tracking tools*, THE MARKUP (Dec. 13, 2022), <https://themarkup.org/pixel-hunt/2022/12/13/out-of-control-dozens-of-telehealth-startups-sent-sensitive-health-information-to-big-tech-companies> (last visited Sep. 5, 2024).

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

²⁶ Facebook, *Meta Reports Fourth Quarter and Full Year 2021 Results*, META INVESTOR RELATIONS, (Feb. 2, 2022), <https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx> (last visited Sep. 5, 2024).

59. Facebook's Business Tools, including the Pixel and Conversions API, are bits of code that advertisers can integrate into their webpages, mobile applications and servers, thereby enabling the interception and collection of website visitors' activity.

60. Specifically, the Pixel "tracks the people and type of actions they take."²⁷ When a user accesses a webpage hosting the Pixel, their communications with the host webpage are instantaneously and surreptitiously duplicated and sent to Facebook's servers. Notably, this transmission does not occur unless the webpage contains the Pixel.

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

62. The process of adding the Pixel to webpages is a multi-step process that must be undertaken by the website owner.²⁸

63. Facebook guides the website owner through setting up the Pixel during the setup process. Specifically, Facebook explains that there are two steps to set up a Pixel: (1) Create your pixel and set up the pixel base code on your website. You can use a partner integration if one is available to you, or you can manually add code to your website. (2) Set up events on your website to measure the actions you care about, like making a purchase. You can use a partner integration, the point-and-click event setup tool, or you can manually add code to your website."²⁹

²⁷ *Retargeting*, META, <https://www.facebook.com/business/goals/retargeting> (last visited Sep. 5, 2024).

²⁸ *Business Help Center: How to set up and install a Meta Pixel*, META, <https://www.facebook.com/business/help/952192354843755?id=1205376682832142> (last visited Sep. 5, 2024).

²⁹ *Id.*

64. Aside from the various steps to embed and activate the Pixel, website owners, like Defendant, must also agree to Facebook’s Business Tools Terms which requires website owners using the Pixel to “represent and warrant” that they have adequately and prominently notified users about the collection, sharing and usage of data through Facebook’s Business Tools (including the Pixel) and that websites “will not share Business Tool Data . . . that [websites] know or reasonably should know . . . includes health, financial information or other categories of sensitive information”³⁰

65. Stated differently, Plaintiffs’ and Class Members’ Private Information would not have been disclosed to Facebook but for Defendant’s decisions to install the Pixel on its Website.

66. As explained in more detail below, this secret transmission to Facebook is initiated by Defendant’s source code concurrently with Plaintiffs’ and Class Members’ communications to their intended recipient, Defendant.

C. Abbott Assisted Third Parties in Intercepting Customers’ Communications with its Website and Disclosed Its Customer’s Private Information to Third Parties.

67. Defendant’s Website is accessible on mobile devices and desktop computers and allows customers to communicate with Defendant regarding their medical conditions, specifically, diabetes, as well as testing and diabetes management.

68. Defendant encouraged customers to use its Website to communicate their Private Information, access information about their condition and Defendant’s diabetes management products, sign up for a free trial of a specific Freestyle Libre CGM and more.

³⁰ *Id.*; see also Pratyush Deep Kotoky, *Facebook collects personal data on abortion seekers: Report*, NEWSBYTES (June 16, 2022) <https://www.newsbytesapp.com/news/science/facebook-collects-personal-data-on-abortion-seekers/story> (last visited Sep. 5, 2024). (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 Sep. 5, 2024).

69. Despite this, Defendant purposely installed Tracking Tools on its Website and programmed specific webpage(s) to surreptitiously share its customers' private and protected communications, including Plaintiffs' and Class Members' PHI and/or PII, which was sent to Facebook, Google and other third parties.

70. The Tracking Tools followed, recorded and disseminated customers' information as they navigated, and communicated with Defendant via the Website, and transmitted the substance of those communications to unintended and undisclosed third parties.

71. The information disseminated by the Tracking Tools and/or intercepted by third parties constitutes Private Information and includes medical information customers requested or viewed, the title of buttons clicked (such as the "Download Guide" option which identifies and communicates the specific diabetes management product sought by a customer as well as their specific medical condition), selections made from drop-down menus or while using filtering tools, the fact that a customer is signing up for a free trial of a specific diabetes monitoring system, requesting a voucher for a specific Freestyle Libre sensor, requesting support for their Freestyle Libre diabetes monitoring system, and other sensitive and confidential information, the divulgence of which is and was highly offensive to Plaintiffs.

72. This information constitutes PHI because the webpages have access to "information that relates to any individual's past, present, or future health, health care, or payment for health care."³¹ In this case, Defendant's Website receives PHI concerning Plaintiffs' or a specific Class Member's past, present, of future health.

³¹ See *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, DEPT. OF HEALTH AND HUMAN SERVICES, <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html> (noting that "IIHI collected on a regulated entity's website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, such as in some circumstances

73. The information collected and disclosed by Defendant's Tracking Tools is not anonymous and is viewed and categorized by the intercepting party on receipt.

74. The information Facebook received via the Tracking Tools was linked and connected to customers' Facebook profiles (via their Facebook ID or "c_user id"), which includes other PII.

75. Similarly, Google, via its tracking codes, stores users' logged-in identifier on non-Google websites in its logs. Whenever a user logs-in on non-Google websites, whether in private browsing mode or non-private browsing mode, the same identifier is associated with the data Google collects from the user's browsing activities on that website. Google further logs all such data (private and non-private) within the same logs and uses this data to serve personalized ads.³² Upon information and belief, Google uses DoubleClick cookies including DSID and IDE that operate similarly to the unique Facebook ID, to track users across websites and target them with ads based on their browsing activities.

76. Simply put, the health information that was disclosed via the Tracking Tools is personally identifiable and was sent alongside other persistent unique identifiers such as the customers' IP address, Facebook ID, unique Google cookies, and device identifiers.³³

D. Underlying Web Technology.

IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services.") (last visited Sep. 5, 2024).

³² See *Brown v. Google LLC*, Case No. 4:20-cv-3664-YGR, 2023 WL 5029899 (N.D. Cal. Aug. 7, 2023) (order denying summary judgment and citing internal evidence from Google employees).

³³ See *Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1056 (N.D. Cal. 2021) (discussing how Google collects personal information and IP addresses); see also *Meta Pixel*, META, <https://developers.facebook.com/docs/meta-pixel/> (last visited Sep. 5, 2024).

77. Web browsers are software applications that allow consumers to navigate the internet and exchange electronic communications. Every “client device” (computer, tablet or smart phone) has a web browser (e.g., Microsoft Edge, Google Chrome, Mozilla’s Firefox, etc.).

78. Every website is hosted by a computer “server” which allows the website’s owner (Defendant) to display the Website and exchange communications with the website’s visitors (Plaintiffs and Class Members) via the visitors’ web browser.

79. When customers used Defendant’s Website, they engaged in an ongoing back-and-forth exchange of electronic communications with Defendant wherein their web browser communicated with Defendant’s computer server.

80. These communications are invisible to ordinary consumers, but one browsing session may consist of thousands of individual HTTP Requests and HTTP Responses.

81. A patient’s HTTP Request essentially asks Defendant’s Website to retrieve certain information (such as a “Find Your Location” 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).

82. Every webpage is comprised of both Markup and “source code.” Source code is simply a set of instructions that commands the website visitor’s browser to take certain actions when the web page first loads or when a specified event triggers the code.

83. Defendant’s Tracking Tools were embedded in its Website’s source code, which is contained in its HTTP Response. The Tracking Tools, which were programmed to automatically track customers’ communications and transmit them to third parties, executed instructions that effectively opened a hidden spying window into each customers’ web browser, through which third parties intercepted customers’ communications and activity.

84. For example, when a user visits <https://www.freestyle.abbott/us-en/products/> and selects “FreeStyle Libre 2,” the customer’s browser automatically sends an HTTP Request to Defendant’s web server. Defendant’s web server automatically returns an HTTP Response, which loads the Markup for that particular webpage. As depicted below, the user only sees the Markup, not Defendant’s source code or underlying HTTP Requests and Responses.

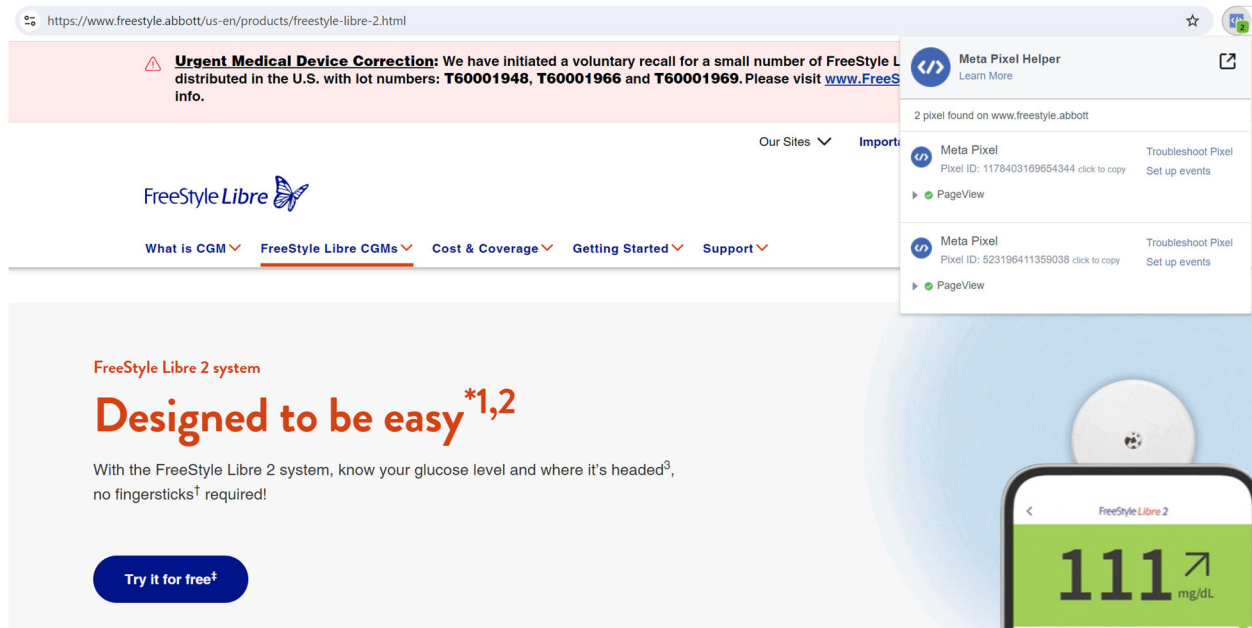


Figure 1. The image above is a screenshot taken from the user’s web browser upon visiting <https://www.freestyle.abbott/us-en/products/freestyle-libre-2.html>.

85. The image above displays the Markup of Defendant’s webpage. Behind the scenes, however, Tracking Tools like the Meta Pixel and Google Analytics are embedded in the source code, automatically transmitting everything the user does on the webpage and effectively opening a hidden spy window into the customers’ browser.

E. Defendant Disclosed Plaintiffs’ and Class Members’ Private Information to Facebook and Google Using Tracking Tools.

86. In this case, Defendant employed Tracking Tools to intercept, disclose, and re-direct Plaintiffs’ and Class Members’ Private Information to Facebook, Google and other third

parties.

87. Defendant's source code manipulates the patient's browser by secretly instructing it to duplicate the patient's communications (HTTP Requests) with Defendant and to send those communications to Facebook and Google. These transmissions occur contemporaneously, invisibly and without the patient's knowledge.

88. Thus, without its customers' consent, Defendant used its source code to commandeer and "bug" or "tap" its customers' computing devices, allowing Facebook, Google and other third parties to listen in on their communications with Defendant and thereby intercept those communications, including Private Information.

89. The Tracking Tools, including the Pixel, allow Defendant to optimize the delivery of ads, measure cross-device conversions, create custom audiences and decrease advertising and marketing costs. However, Defendant's Website does not rely on the Tracking Tools to function.

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

91. Plaintiffs and Class Members were not aware that their Private Information would be shared with third parties as it was communicated to Defendant because, amongst other reasons, Defendant did not disclose this fact.

92. Plaintiffs and Class Members never consented, agreed, authorized or otherwise permitted Defendant to disclose their Private Information to third parties, nor did they intend for anyone other than Defendant to be a party to their communications (many of them highly sensitive and confidential) with Defendant.

93. Defendant's Tracking Tools, including the Pixel, sent non-public Private Information to third parties like Facebook and Google, including but not limited to Plaintiffs' and Class Members': (i) status as medical customers; (ii) specific health conditions, i.e. diabetes; (iii) and the specific diabetes management device used or sought.

94. Importantly, the Private Information Defendant's Tracking Tools sent to third parties included PII that allowed those third parties to connect the Private Information to a specific person. Information sent to Facebook was sent alongside Plaintiffs' and Class Members' Facebook ID, thereby allowing individual customers' communications with Defendant, including the Private Information contained in those communications, to be linked to their unique Facebook accounts and therefore their identity.³⁴

95. A user's Facebook ID is linked to their Facebook profile, which contains a wide range of demographic and other information about the user including, but not limited to, name, location, pictures, personal interests, work history and relationship status. Because the user's Facebook ID uniquely identifies an individual's Facebook account, Facebook—or any ordinary person—can easily use the Facebook ID to locate, access and view the user's corresponding Facebook profile.

96. Defendant's use of Google trackers is also problematic, and other healthcare providers have sent data breach notification letters to customers who used digital platforms outfitted with these tools. Like Facebook, Google receives the contents of customers' communications alongside data that individually identifies anyone with an existing Google account such as an email address "Gmail" or YouTube account.

³⁴ Defendant's Website tracks and transmits data via first-party and third-party cookies. The c_user cookie or Facebook ID is a type of third-party cookie assigned to each person who has a Facebook account, and is comprised of a unique and persistent set of numbers.

97. Defendant deprived Plaintiffs and Class Members of their privacy rights when it: (i) implemented Tracking Tools that surreptitiously tracked, recorded and disclosed Plaintiffs' and other customers' confidential communications and Private Information; (ii) disclosed customers' protected information to unauthorized third parties; and (iii) undertook this pattern of conduct without notifying Plaintiffs or Class Members and without obtaining their express written consent.

98. By installing and implementing both the Pixel and Google Tracking Tools, Defendant caused Plaintiffs' and Class Member's communications to be intercepted by and/or disclosed to Facebook and Google and rendered personally identifiable.

99. As explained below, these unlawful transmissions are initiated by Defendant's source code concurrent with communications made via certain webpages.

F. Defendant's Tracking Tools Divulge Customer Information Via Its Website.

100. If a customer uses Defendant's Website to find healthcare, the Website directs them to communicate Private Information including, but not limited to, the reason for seeking care (*i.e.*, their medical condition), the type of FreeStyle Libre diabetes management device sought, information about the device in question, requests and printing of Defendant's vouchers for FreeStyle continuous glucose monitoring devices, and/or the fact that the customer is requesting a trial of a specific FreeStyle CGM system or sensor.

101. Unbeknownst to the customer, these communications are sent to Facebook and other third-party entities via Defendant's Tracking Tools, along with the customer's PII.

102. In the example below, the user navigated to the "Freestyle Libre 3" page on Defendant's Website where the user was prompted to request a free sensor or start a free trial of this particular CGM device:

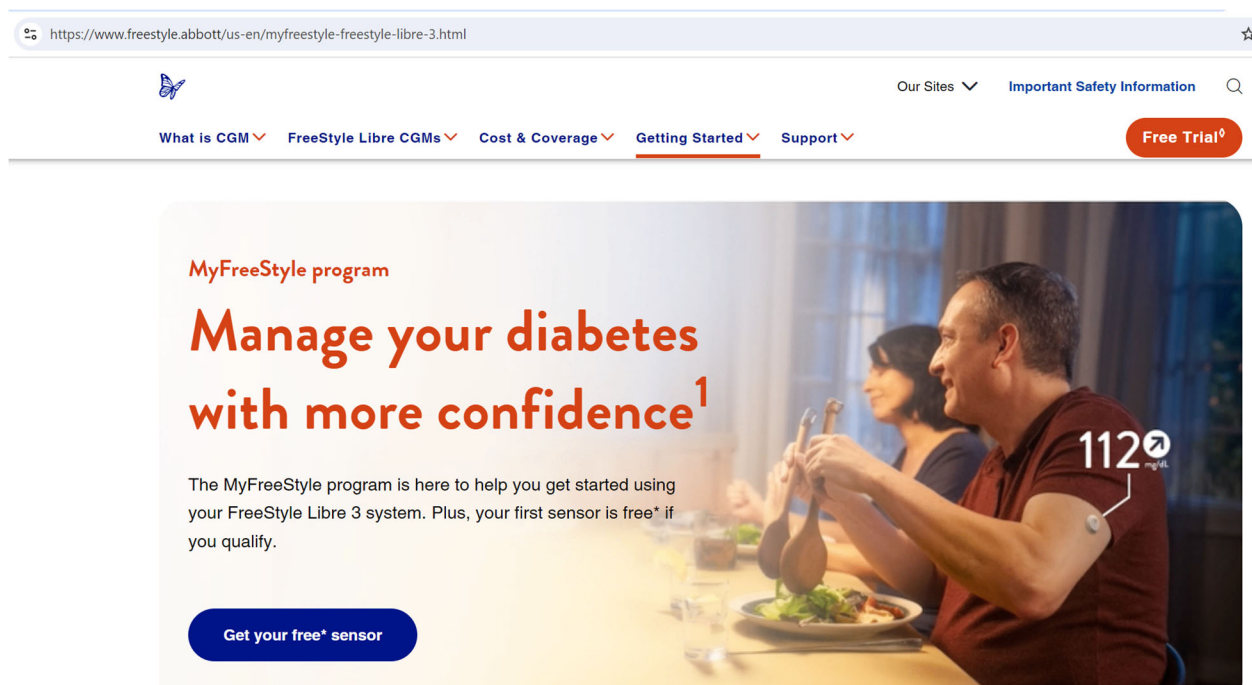


Figure 1. Screenshot taken from <https://www.freestyle.abbott/us-en/myfreestyle-freestyle-libre-3.html> as the user searches for information on the FreeStyle Libre 3 CGM device.

103. Unbeknownst to customers, this webpage—which is undoubtedly used to communicate Private Information for the purpose of seeking medical treatment—contains Defendant’s Tracking Tools. The image below shows the “behind the scenes” portion of the website that is invisible to ordinary users:

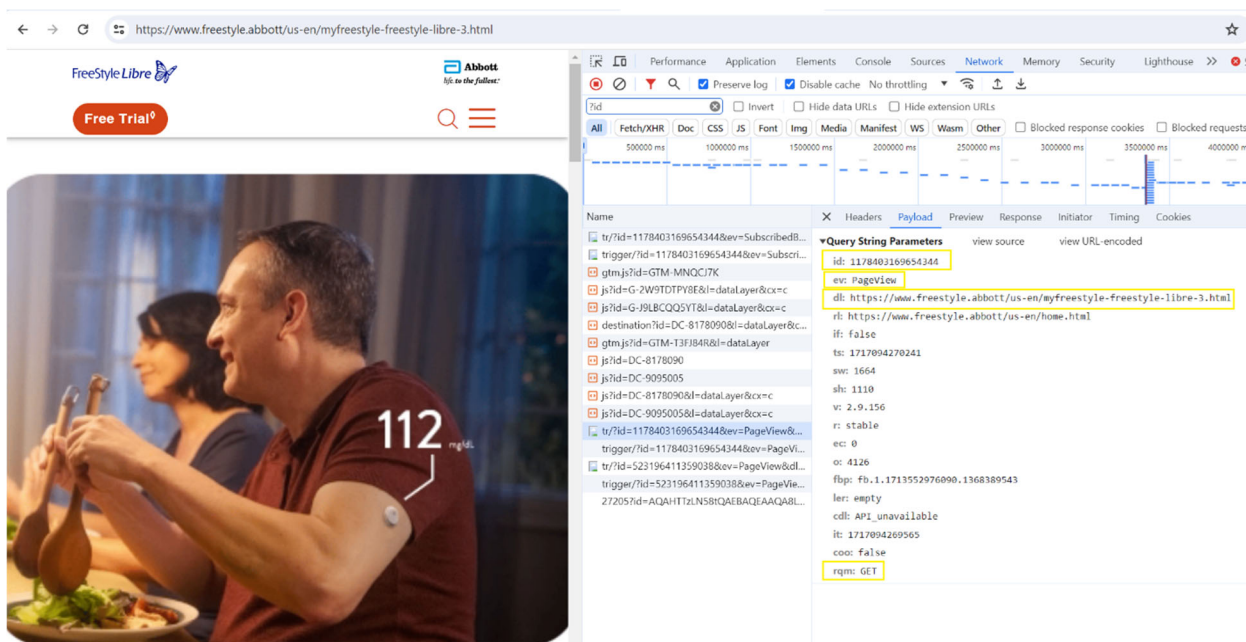


Figure 2. Screenshot from Defendant's Website depicting back-end network traffic which reveals that the user is searching for information on the FreeStyle Libre 3 CGM device.

104. Thus, without alerting the user, Defendant's Pixel sends the communications the user made via the webpage to Facebook, and the images herein confirm that the communications Defendant sends to Facebook contain the user's Private Information.

```

:authority:      www.facebook.com
:method:        GET
:path:          /tr/?id=1178403169654344&ev=PageView&cdl=https%3A%2F%2Fwww.freestyle.abbott%2Fus-en%2Fmyfreestyle-freestyle-libre-3.html&url=https%3A%2F%2Fwww.freestyle.abbott%2Fus-en%2Fhome.html&if=false&ts=1717094270241&sw=1664&sh=1110&v=2.9.156&r=stable&ec=0&o=4126&fbp=fb.1.1713552976090.1368389543&ler=empty&cdl=APl_unavailable&it=1717094269565&coo=false&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
Cache-Control:  no-cache
Cookie:         sb=GrxtY1jj9lKWnpCg7UAhiJMv; c_user=540...; datr=Y5QdZurO628alqBjNG42Gs_R; ps_n=1; dpr=1.5; xs=7%3Ag2wyjfuNYXsJFg%3A2%3A1707506163%3A-1%3A3037%3A%3AAcVzFpVmj4MAzaLe6HM699VZuoatUEN8ZbxCUjh-nE; fr=1CJdUJhSRLrYJkmv9.AWXI5RnfB_hR0bXWOejg49kwOes.BmWL3o..AAA.0.0.BmWL3o.AWXXupPKaCM
Pragma:         no-cache
Priority:        i
Referer:        https://www.freestyle.abbott/
Sec-Ch-Ua:      "Google Chrome";v="125", "Chromium";v="125", "Not.A/Brand";v="24"
Sec-Ch-Ua-Mobile: ?0

```

Figure 3: Screenshot from the Network traffic report depicting the data sent to Facebook including specific user identifiers such as `c_user`, `datr` and `fr` cookie values.

105. The first line of highlighted text, “id=1178403169654344” refers to one of Defendant’s Meta Pixel IDs and confirms that it implemented the Pixel into its source code for this webpage and transmitted info to Facebook from this webpage.³⁵

106. On the same line of text, “ev= PageView,” identifies and categorizes which actions the user took on the webpage (“ev=” is an abbreviation for event, and “PageView” is the type of event). Thus, this identifies the user as having navigated to the Website page.

107. Under request headers, the referrer is showing that Defendant sent the information to Facebook.

108. Finally, the highlighted text (“GET”) demonstrates that Defendant’s Pixel sent the user’s communications, and the Private Information contained therein, alongside the user’s

³⁵ At the time of filing of this Complaint, Defendant embedded at least three different Meta Pixels on the Website, with unique ID numbers 188810848554346, 3133587236896775, and 390603172515567.

Facebook ID (c_user ID), thereby allowing the user's communications and actions on the Website to be linked to their specific Facebook profile.

109. The image demonstrates that the user's Facebook ID (highlighted as "c_user=" in the image above) was sent alongside the other data.

110. In addition to disclosing long-form descriptive URLs to Facebook, Defendant disclosed the exact text of buttons clicked by a customer to Facebook as well.

111. For example, if a customer clicks on the "Get your free* sensor" button, that exact action is sent to Facebook via the "SubscribedButtonClick" event set up by Abbott for its Meta Pixel:

The screenshot shows a web browser window with the URL <https://www.freestyle.abbott/us-en/myfreestyle-freestyle-libre-3/fsl3-sensor-voucher-confirmation.html>. The page content includes a "Free Trial" banner, a "PRINT VOUCHER" button, and a "FREE SAMPLE CARD" for the FreeStyle Libre 3 sensor. The network traffic panel on the right shows a POST request to a Facebook URL with a query string containing user and event data. The query string parameters are highlighted in yellow:

```
id=1178403169654344&ev=SubscribedButtonClick&dl=https://www.freestyle.abbott/us-en/myfreestyle-freestyle-libre-3/fsl3-sensor-voucher-confirmation.html&rl=https://www.freestyle.abbott/us-en/myfreestyle-freestyle-libre-3.html&tf=false&ts=1717095455101&cd[buttonFeatures]={"classList":"btn","destination":"","id":"print-voucher","imageurl":"","innerText":"PRINT VOUCHER","numchildButtons":0,"tag":"a","type":"button","name":""}&cd[buttonText]=PRINT VOUCHER&cd[formFeatures]={}&cd[pageFeatures]={"title":"Thank You for Joining the MyFreeStyle Program","freestyleLibreUS":true}
```

Figure 4. Disclosure of the user's selection of Abbott's voucher for the FreeStyle Libre 3 Sensor, including the printing.

112. Defendant also discloses when a user signs up for a free trial of one of Abbott's diabetes monitoring products, along with personal identifiers.

113. Defendant discloses these searches by its customers to Facebook by sending SubscribedButtonClick events, in this case capturing the user's actions in signing up for the trial, as illustrated below:



Figure 5. Example of disclosure that takes place when a customer signs up for a free trial.

114. In each of the examples above, the user's Website activity and the contents of their communications are sent to Facebook alongside their PII, *see, e.g., Figure 6*:

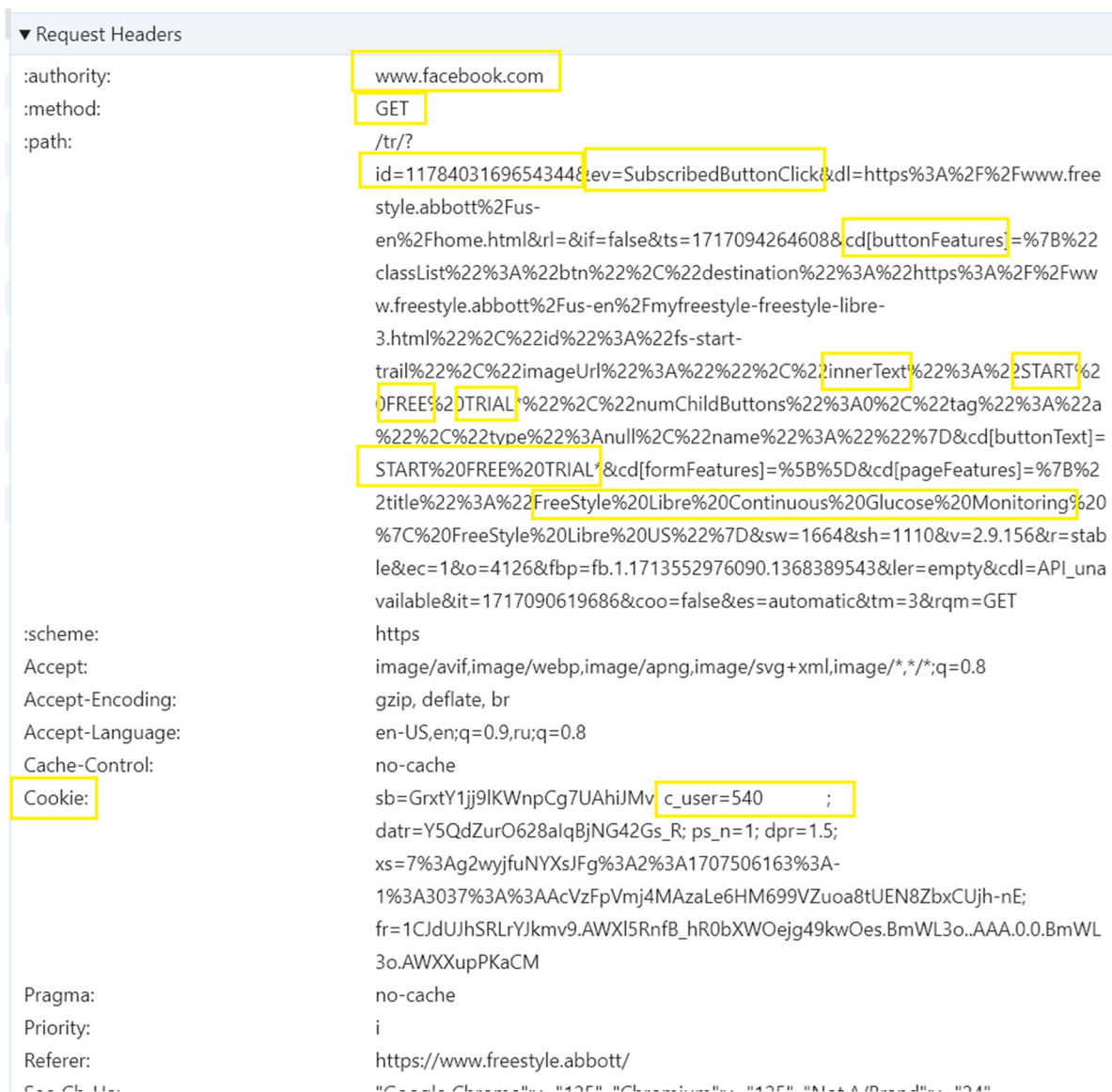
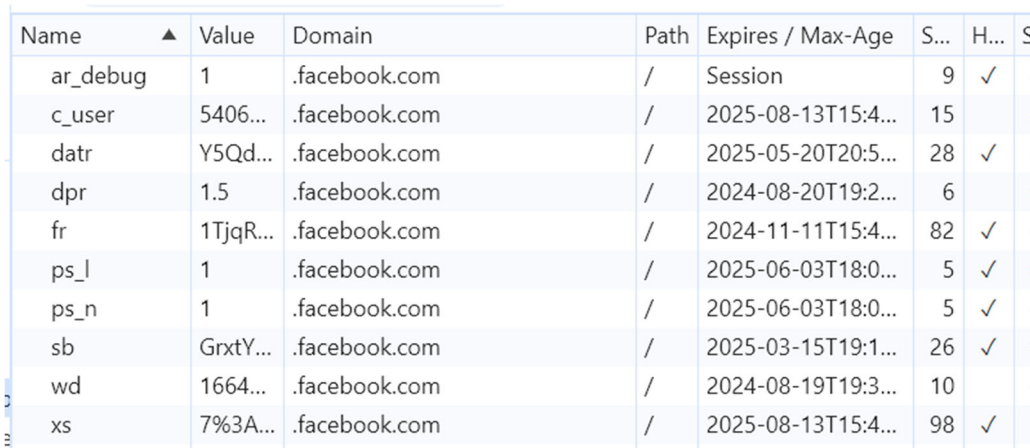


Figure 6: Screenshot from the Network traffic report depicting the data sent to Facebook including specific user identifiers such as *c_user*, *datr* and *fr* cookie values.

115. Several different methods allow marketers and third parties to identify individual Website users, but the examples above demonstrate what happens when the Website user is logged into Facebook on their web browser or device. When this happens, the Website user's identity is revealed via third-party cookies that work in conjunction with the Pixels.

116. For example, the Pixel transmits the user's c_user cookie, which contains that user's unencrypted Facebook ID, and allows Facebook to link the user's online communications and interactions to their individual Facebook profile.

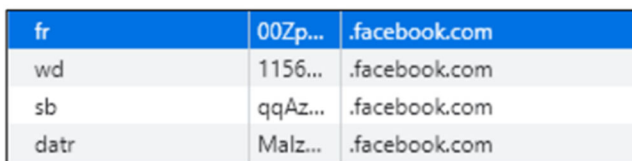
117. Facebook receives at least ten cookies when Defendant's Website transmits information via the Pixels:



Name	Value	Domain	Path	Expires / Max-Age	S...	H...	S
ar_debug	1	.facebook.com	/	Session	9	✓	
c_user	5406...	.facebook.com	/	2025-08-13T15:4...	15		
datr	Y5Qd...	.facebook.com	/	2025-05-20T20:5...	28	✓	
dpr	1.5	.facebook.com	/	2024-08-20T19:2...	6		
fr	1TjqR...	.facebook.com	/	2024-11-11T15:4...	82	✓	
ps_l	1	.facebook.com	/	2025-06-03T18:0...	5	✓	
ps_n	1	.facebook.com	/	2025-06-03T18:0...	5	✓	
sb	GrxTY...	.facebook.com	/	2025-03-15T19:1...	26	✓	
wd	1664...	.facebook.com	/	2024-08-19T19:3...	10		
xs	7%3A...	.facebook.com	/	2025-08-13T15:4...	98	✓	

Figure 7. Screenshot of network analysis showing cookies sent to Facebook when a user visits <https://www.freestyle.abbott/us-en/home.html>.

118. When a visitor's browser has recently logged out of an account, Facebook compels the visitor's browser to send a smaller set of cookies:³⁶



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

Figure 8. Screenshot of cookies for a recently signed out Facebook user.

³⁶ The screenshot below serves as example and demonstrates the types of data transmitted during an HTTP single communication session. Not pictured here or in the preceding image is the _fbp cookie, which is transmitted as a first-party cookie.

119. The fr cookie contains an encrypted Facebook ID and browser identifier.³⁷ Facebook, at a minimum, uses the fr cookie to identify users. This cookie can stay on a user's website browser for up to 90 days after the user has logged out of Facebook.³⁸

120. At each stage, Defendant also utilizes the _fbp cookie, which attaches to a browser as a first-party cookie, and which Facebook uses to identify a browser and a user.³⁹

Name	Value	Domain
_fbp	fb.1.1722914957441.281721702826368900	.freestyle.abbott

Figure 9. Screenshot showing Defendant's use of the _fbp cookie.

121. Google's _ga and _gid cookies function similarly to Facebook's _fbp cookie.

122. The Pixel uses both first- and third-party cookies. Both were used on the Website.⁴⁰

123. At present, the full breadth of Defendant's tracking and data-sharing practices is unclear, but evidence suggests Defendant is using additional tracking pixels and tools to transmit its customers' Private Information to additional third parties. For example, Plaintiffs' counsels' investigation revealed that Defendant is also sending their customers' protected health information to Google via Google tracking tools including Google Analytics and Google Tag Manager.

³⁷ 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 Sep. 5, 2024).

³⁸ *Cookies & other storage technologies*, META, <https://www.facebook.com/policy/cookies/> (last visited Sep. 5, 2024).

³⁹ *ClickID and the fbp and fbc Parameters*, META, <https://developers.facebook.com/docs/marketing-api/conversions-api/parameters/fbp-and-fbc/> (last visited Sep. 5, 2024).

⁴⁰ A first-party cookie is "created by the website the user is visiting"—in this case, Defendant's Website. A third-party cookie is "created by a website with a domain name other than the one the user is currently visiting"—i.e., Facebook. The _fbp cookie is always transmitted as a first-party cookie. At a minimum, Facebook uses the fr, _fbp, and c_user cookies to link website visitors' data to their Facebook IDs and corresponding accounts.

124. Google Tracking Tools installed on the FreeStyle Website appear to collect the same types and categories of sensitive Private Information from Defendant's customers as the Facebook Pixel and, in some instances, even more data including such details of their interaction with the Website as the form fields the customer fills out when signing up for Abbott's MyFreeStyle program:

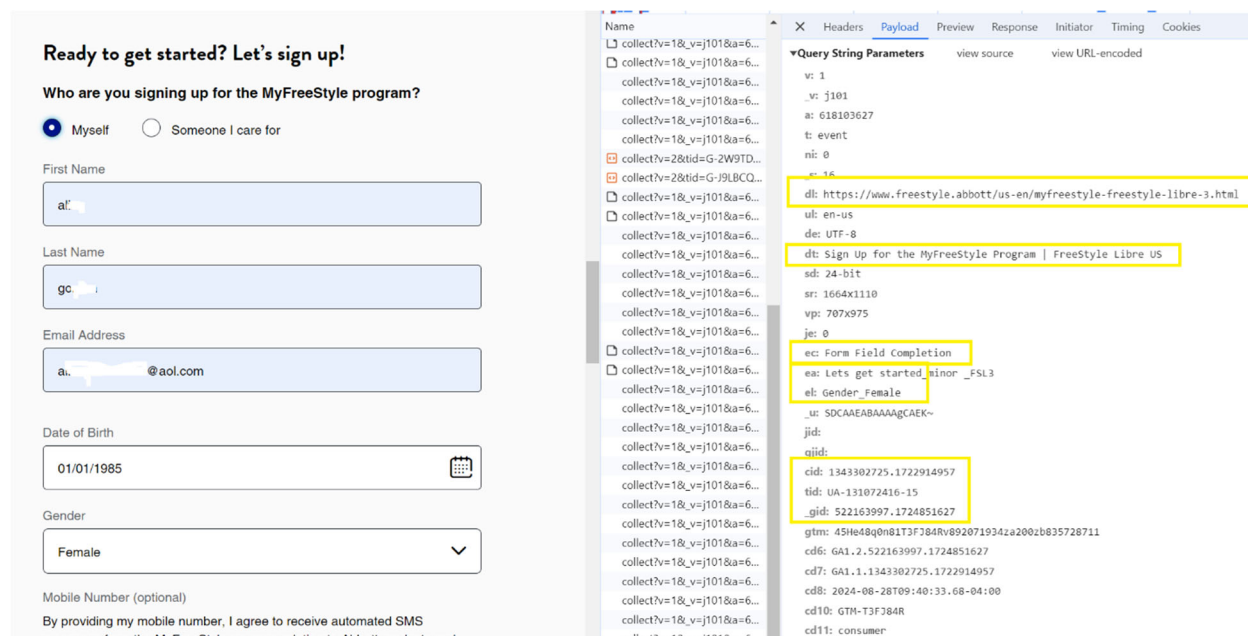


Figure 10. Screenshot of network analysis showing data sent to Google when a customer fills out Defendant's signup form for Abbott's MyFreeStyle program.

125. As described *supra*, this information is shared with Google along with the _ga, _gid, and the DoubleClick DSID cookies which are used to personally identify the customer.

126. At or around the time of filing of this Complaint, Defendant continued to disclose customers' Private Information to Google, including their medical condition, the exact terms of searches via the Website search bar, and FreeStyle Libre diabetes management products selected by the customer.

127. Defendant does not disclose that the Pixels, Google Analytics, or any other Tracking Tools embedded in the Website's source code track, record, and transmit Plaintiffs' and

Class Members' Private Information to Facebook and Google. Moreover, Defendant never received consent or written authorization to disclose Plaintiffs' and Class Members' private communications to Facebook or Google.

G. Defendant's Conduct Is Unlawful and Violated Industry Norms.

i. Defendant Violated its own Privacy Policies.

128. Defendant's Website Privacy Policy which Defendant modified several times during the relevant time period, states the following: "We believe your personal information belongs to you. We will be transparent about the data we collect from you, and how that data will be used."⁴¹

129. The policy defines "Personal Information" as "information that identifies you as an individual or could be used to reasonably identify you."⁴²

130. The Privacy policy also defined "Sensitive Personal Information" as follows:

Personal Information that reveals a consumer's social security, driver's license, state identification card, or passport number; account log-in, financial account number, debit card number, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account; precise geolocation; racial or ethnic origin, religious beliefs, or union membership; contents of email or text messages; and genetic data. Sensitive Personal Information also includes processing of biometric information for the purpose of uniquely identifying a consumer and Personal Information collected and analyzed concerning a consumer's health, sex life, or sexual orientation. Sensitive Personal Information also includes "sensitive data" as that term is defined in the applicable US State Privacy Law.⁴³

⁴¹ See, e.g., Abbott's privacy policy (effective as of December 28, 2022), captured by the Wayback Machine on May 29, 2023, <https://web.archive.org/web/20230529223526/https://www.abbott.com/privacy-policy.html>.

⁴² *Id.*

⁴³ *Id.* (emphasis added).

131. Abbott further represented that it may use “Sensitive Personal Information” or “sensitive data” such as health information only for a specific purpose such as processing transactions, and promised its customers the following:

Abbott may also disclose your Personal Information to our service providers, who act on our behalf, our partners and collaborators, and at your direction. ***Abbott does not sell Personal Information or disclose Personal Information to third parties to use for their own benefit without your consent.***⁴⁴

132. This language reflects Defendant’s awareness of the high value customers such as Plaintiffs and Class Members place on their Personal Information and especially their sensitive health information.

133. Moreover, whereas Abbott disclosed that it “allow[s] certain companies to place tracking technologies like cookies on our websites,” it stated only that “[t]hose companies receive information about your interaction with our websites that is associated with your browser or device and may use that data to serve you relevant ads on our websites or others. Except for this kind of disclosure, we do not sell any of your Personal Information.”⁴⁵

134. Abbott did not disclose that it allows companies like Facebook or Google to capture and disclose customers’ ***Sensitive*** Personal Information including health data, along with unique personal identifiers, for marketing, re-targeting and other commercial uses by third-party data brokers like Facebook and Google.

135. At no point did Abbott seek such authorization from Plaintiffs before transmitting protected health information to a third party for marketing purposes.

⁴⁴ *Id.* (emphasis added).

⁴⁵ *Id.*

136. Defendant violated its own privacy policies by unlawfully disclosing Plaintiffs' and Class Members' Private Information to Meta (Facebook), Google, and likely other third parties without written authorization.

ii. Defendant Violated HIPAA Standards.

137. Under HIPAA, a healthcare provider may not disclose personally identifiable, non-public medical information about a patient, a potential patient or household member of a patient for marketing purposes without the patients' express written authorization.⁴⁶

138. The HIPAA Privacy Rule "establishes national standards to protect individuals' medical records and other individually identifiable health information (collectively defined as 'protected health information') and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically."⁴⁷

139. The Privacy Rule broadly defines "protected health information" ("PHI") as individually identifiable health information ("IIHI") 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.

140. IIHI is defined as "a subset of health information, including demographic information collected from an individual" that is: (1) "created or received by a health care provider, health plan, employer, or health care clearinghouse"; (2) "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual";

⁴⁶ HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).

⁴⁷ *HIPAA For Professionals*, DEPT. OF HEALTH AND HUMAN SERVICES, <https://www.hhs.gov/hipaa/for-professionals/index.html> (last visited Sep. 5, 2024).

and (3) either (a) “identifies the individual” or (b) “[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.

141. Under the HIPAA de-identification rule, “health information is not individually identifiable only if”: (1) an expert “determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information” and “documents the methods and results of the analysis that justify such determination”; or (2) “the following identifiers of the individual or of relatives, employers, or household members of the individual are removed;

A. Names;

H. Medical record numbers;

J. Account numbers;

M. Device identifiers and serial numbers;

N. Web Universal Resource Locators (URLs);

O. Internet Protocol (IP) address numbers; ... and

R. Any other unique identifying number, characteristic, or code...; and

The covered entity must not “have 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.”⁴⁸

142. The HIPAA Privacy Rule requires any “covered entity”—which includes health care providers—to maintain appropriate safeguards to protect the privacy of protected health information and sets limits and conditions on the uses and disclosures that may be made of protected health information without authorization. 45 C.F.R. §§ 160.103, 164.502.

⁴⁸ 45 C.F.R. § 160.514.

143. An individual or corporation violates the HIPAA Privacy Rule if it knowingly and in violation of 42 U.S.C. §§ 1320d-1320d-9 (“Part C”): “(1) uses or causes to be used a unique health identifier; [or] (2) obtains individually identifiable health information relating to an individual.” The statute states that a “person ... shall be considered to have obtained or disclosed individually identifiable health information in violation of [Part C] if the information is maintained by a covered entity ... and the individual obtained or disclosed such information without authorization.” 42 U.S.C. § 1320d-6.

144. Even the fact that an individual is receiving a medical service, i.e., is a customer of a particular healthcare entity, can be PHI.

145. HHS 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.”⁴⁹

146. Consistent with this restriction, HHS has issued marketing guidance that provides, “With limited exceptions, the [Privacy] Rule requires an individual’s written authorization before a use or disclosure of his or her protected health information can be made for marketing . . . Simply put, a covered entity may not sell protected health information to a business associate or any other

⁴⁹ See *Guidance Regarding Methods for De-Identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, DEPT. OF HEALTH AND HUMAN SERVICES, <https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html> (last visited Sep. 5, 2024).

third party for that party's own purposes. Moreover, covered entities may not sell lists of patients or enrollees to third parties without obtaining authorization from each person on the list.”⁵⁰

147. Here, as described *supra*, Defendant provided customer information to third parties in violation of the Privacy Rule—and its own privacy policies.

148. The penalties imposed by 42 U.S.C. § 1320d-6 apply directly to Defendant when it is knowingly disclosing IIHI relating to an individual, as those terms are defined under HIPAA.

149. Violation of 42 U.S.C. § 1320d-6 is subject to criminal penalties. 42 U.S.C. § 1320d-6(b). There is a penalty enhancement where “the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm.” In such cases, the entity that knowingly obtains individually identifiable health information relating to an individual shall “be fined not more than \$250,000, imprisoned not more than 10 years, or both.”

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

151. Under HIPAA, Defendant may not disclose PII about a patient, potential patient or household member of a patient for marketing purposes without the patient's express written

⁵⁰*Marketing*, DEPT. OF HEALTH AND HUMAN SERVICES, <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/marketing/index.html> (last visited Sep. 5, 2024).

authorization. See HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.501; 164.508(a)(3), 164.514(b)(2)(i).

152. Defendant further failed to comply with other HIPAA safeguard regulations as follows:

- a) Failing to ensure the confidentiality and integrity of electronic PHI that Defendant created, received, maintained and transmitted in violation of 45 C.F.R. section 164.306(a)(1);
- b) Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. section 164.308(a)(1);
- c) Failing to identify and respond to suspected or known security incidents and mitigate harmful effects of security incidents known to Defendant in violation of 45 C.F.R. section 164.308(a)(6)(ii);
- d) Failing to protect against reasonably anticipated threats or 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).

153. In disclosing the content of Plaintiffs' and Class Members' communications, Defendant had a purpose that was tortious, criminal, and designed to violate state constitutional and statutory provisions, that is, to illegally disclose Plaintiffs' and Class Members' Private Information to Facebook (and other Pixel Information Recipients) in violation of HIPAA, including 42 U.S.C. § 1320d-6(a)(3), as well as the torts alleged below.

154. Defendant intercepted the content of Plaintiffs' and Class Members' communications, including their Private Information, for a criminal and tortious purpose.

Defendant would not have been able to obtain the Private Information or the marketing services it did if it had complied with the law.

H. Plaintiffs' and Class Members' Reasonable Expectation of Privacy.

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

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

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

158. For example, a Consumer Reports study shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumer data, and the same percentage believe those companies and websites should be required to provide consumers with a complete list of the data that is collected about them.⁵¹

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

160. Plaintiffs and Class Members would not have used Defendant's Website, would not have provided their Private Information to Defendant, and would not have paid for Defendant's

⁵¹ *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, CONSUMER REPORTS (May 11, 2017), <https://www.consumerreports.org/consumer-reports/consumers-lessconfident-about-healthcare-data-privacy-and-car-safety-a3980496907/> (last visited Sep. 5, 2024).

healthcare services or would have paid less for them, had they known that Defendant would disclose their Private Information to third parties.

161. Plaintiffs' and Class Members' reasonable expectations of privacy in their PII/PHI are grounded in, among other things, Defendant's status as a health products provider, Defendant's common law obligation to maintain the confidentiality of customers' PII/PHI, state and federal laws protecting the confidentiality of medical information, state and federal laws protecting the confidentiality of communications and computer data, state laws prohibiting the unauthorized use and disclosure of personal means of identification and Defendant's express and implied promises of confidentiality.

I. Abbott was Enriched and Benefitted from the Use of the Tracking Tools and Unauthorized Disclosures.

162. One of the primary reasons that Defendant decided to embed the Pixel and other Tracking Tools on its Website was to commit criminal and tortious acts in violation of federal and state laws as alleged herein, namely, the use of patient data in the absence of express written consent.

163. Defendant's use of the Private Information after the initial interception and disclosure for marketing and revenue generation was in violation of HIPAA and an invasion of privacy.

164. In exchange for disclosing the Private Information of its customers, Defendant is compensated by Facebook and Google in the form of enhanced advertising services and more cost-efficient marketing.

165. Retargeting is a form of online marketing that targets users with ads based on their previous internet communications and interactions.

166. The process of increasing conversions and retargeting occurs in the healthcare context by sending a successful action on a health care website back to Facebook via the Tracking Tools and the Pixel embedded on, in this case, Defendant's Website.

167. For example, when a user searches for an urgent care location on the Website, that information is sent to Facebook. Facebook can then use its data on the user to find more users to click on an Abbott ad and ensure that those users targeted are more likely to convert.⁵²

168. Through this process, the Pixel loads and captures as much data as possible when a user loads a telehealth website that has installed the Pixel. The information the Pixel captures, "includes URL names of pages visited, and actions taken—all of which could be potential examples of health information."⁵³

169. As part of its marketing campaign, Defendant re-targeted customers and potential customers to get more visitors to its Website. Defendant did so through use of the intercepted patient data it obtained, procured and/or disclosed in the absence of express written consent.

170. Companies have started to warn about the potential HIPAA violations associated with using Pixels and tracking technologies because many such trackers are not HIPAA-compliant or are only HIPAA-compliant if certain steps are taken.⁵⁴

171. For example, Freshpaint, a healthcare marketing vendor, cautioned that "Meta isn't HIPAA-compliant. They don't sign BAAs, and the Meta Pixel acts like a giant personal user data

⁵² See *How to Make Facebook Ads HIPAA Compliant and Still Get Conversion Tracking*, FRESHPAINT (Mar. 14, 2023), <https://www.freshpaint.io/blog/how-to-make-facebook-ads-hipaa-compliant-and-still-get-conversion-tracking> (last visited Sep. 5, 2024).

⁵³ *Id.*

⁵⁴ See *The guide to HIPAA compliance in analytics*, <https://campaign.piwik.pro/wpcontent/uploads/2023/10/The-guide-to-HIPAA-compliance-in-analytics.pdf> (explaining that Google Analytics 4 is not HIPAA-compliant) (last visited Sep. 5, 2024).

vacuum sending PHI to Meta servers,” and “[i]f you followed the Facebook (or other general) documentation to set up your ads and conversion tracking using the Meta Pixel, remove the Pixel now.”⁵⁵

172. Medico Digital also warns that “retargeting requires sensitivity, logic and intricate handling. When done well, it can be a highly effective digital marketing tool. But when done badly, it could have serious consequences.”⁵⁶

173. By utilizing the Tracking Tools, the cost of advertising and retargeting was reduced through further use of the unlawfully intercepted and disclosed Private Information, thereby benefitting Defendant while invading the privacy of Plaintiffs and Class Members and violating their rights under federal and Arizona law.

J. Plaintiffs’ and Class Members’ Private Information Had Financial Value.

174. Plaintiffs’ and Class Members’ Private Information has economic value and Defendant’s disclosures harmed Plaintiffs and Class Members.

175. Facebook regularly uses the data that it acquires to create Core and Custom Audiences as well as Lookalike Audiences and then sells that information to advertising clients.

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

177. Professor Paul M. Schwartz, writing in the Harvard Law Review, notes: “Personal information is an important currency in the new millennium. The monetary value of personal data

⁵⁵ *How To Make Facebook Ads HIPAA Compliant and Still Get Conversion Tracking*, *supra*, note 47.

⁵⁶ *The complex world of healthcare retargeting*, MEDICO (July 10, 2023), <https://www.medicodigital.com/the-complicated-world-of-healthcare-retargeting/> (last visited Sep. 5, 2024).

is large and still growing, and corporate America is moving quickly to profit from the trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information.”⁵⁷

178. Various reports have been conducted to identify the value of health data. For example, 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.”⁵⁸

179. Trustwave Global Security also 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).⁵⁹

180. The value of health data has also been reported extensively in the media. For example, 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.”⁶⁰

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

⁵⁸ See Todd Zigrang & Jessica Bailey-Wheaton, *Valuing Healthcare Data*, <https://www.healthcapital.com/researchmaterialdocuments/publishedarticles/Valuing%20Healthcare%20Data.pdf> (last visited Sep. 5, 2024).

⁵⁹ See *Hackers, breaches, and the value of healthcare data*, IMPRIVATA (June 30, 2021), <https://www.imprivata.com/blog/healthcare-data-new-prize-hackers> (citing https://www.infopoint-security.de/media/TrustwaveValue_of_Data_Report_Final_PDF.pdf) (last visited Sep. 5, 2024).

⁶⁰ See Christina Farr, *Tech Hospital execs say they are getting flooded with requests for your health*

181. Similarly, 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.⁶¹

182. Indeed, numerous marketing services and consultants offering advice to companies on how to build their email and mobile phone lists—including those seeking to take advantage of targeted marketing—direct putative advertisers to offer consumers something of value in exchange for their personal information. “No one is giving away their email address for free. Be prepared to offer a book, guide, webinar, course or something else valuable.”⁶²

183. There is also a market for data in which consumers can participate. Personal information has been recognized by courts as extremely valuable. *See, e.g., In re Marriott Int’l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020) (“Neither should the Court ignore what common sense compels it to acknowledge—the value that personal identifying information has in our increasingly digital economy. Many companies, like Marriott, collect personal information. Consumers too recognize the value of their personal information and offer it in exchange for goods and services.”).

184. This economic value has been leveraged largely by corporations who pioneered the methods of its extraction, analysis and use. However, the data also has economic value to Internet

data, CNBC (Dec. 18, 2019), <https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html> (last visited Sep. 5, 2024).

⁶¹ See Adam Tanner, *How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry*, TIME (Jan. 9, 2017), <https://time.com/4588104/medical-data-industry/> (last visited Sep. 5, 2024).

⁶² *How to Collect Emails Addresses on Twitter*, VERO, <https://www.getvero.com/resources/twitter-lead-generation-cards/> (last visited Sep. 5, 2024).

users. Market exchanges have sprung up where individual users like Plaintiff herein can sell or monetize their own data.

185. Several companies, such as Google, Nielsen, UpVoice, HoneyGain and SavvyConnect, have products through which they pay consumers for a license to track their data.⁶³

186. Facebook also has paid users for their digital information, including browsing history. Until 2019, Facebook ran a “Facebook Research” app through which it paid \$20 a month for a license to collect browsing history information and other communications from consumers between the ages 13 and 35.

187. Additionally, healthcare data is extremely valuable to bad actors. Health care records may be valued at up to \$250 per record on the black market.⁶⁴

188. These rates are assumed to be discounted because they do not operate in competitive markets, but rather, in an illegal marketplace. If a criminal can sell other Internet users’ stolen data, surely Internet users can sell their own data.

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

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

191. Defendant gave away Plaintiffs’ and Class Members’ communications and transactions on its Website without permission.

⁶³ See Kevin Mercadante, *10 Apps for Selling Your Data for Cash*, BESTWALLETHACKS (Nov. 18, 2023), <https://wallethacks.com/apps-for-selling-your-data/> (last visited Sep. 5, 2024).

⁶⁴ Tori Taylor, *Hackers, Breaches, and the Value of Healthcare Data*, SecureLink, IMPRIVATA(June 30, 2021), <https://www.imprivata.com/blog/healthcare-data-new-prize-hackers> (last visited Sep. 5, 2024).

192. The unauthorized access to Plaintiffs' and Class Members' personal and Private Information has diminished the value of that information, resulting in harm to Website users, including Plaintiffs and Class Members.

PLAINTIFFS' REPRESENTATIVE EXPERIENCES

Plaintiff Nguyen

193. As a condition of receiving Defendant's services, Plaintiff Nguyen disclosed her Private Information to Defendant on several occasions, including in May 2023, to request a FreeStyle Libre 3 CGM product via the free trial offered by Abbott.

194. Plaintiff Nguyen has been a customer of Defendant since at least August 2021 as she was using FreeStyle Libre 14-day CGM system at the time.

195. Plaintiff Nguyen accessed Defendant's Website on her phone and computer to research and request diabetes monitoring products from Defendant and at Defendant's direction.

196. Plaintiff Nguyen used Defendant's Website to review and request FreeStyle Libre products for herself as well as search for and communicate information related to her diabetes, insurance, and other Private Information.

197. Her searches for and communication of information included her visiting specific webpages that revealed her PHI through the URLs, as well as searches through the Website's search bar that disclosed the specific phrases she used to search for information related to her medical condition, her searches related to insurance coverage for diabetes monitoring systems sought from Defendant, and the details of her requests for Abbott's diabetes monitoring products.

198. The full scope of Defendant's interceptions and disclosures of Plaintiff Nguyen's communications to Meta can only be determined through formal discovery. However, in addition to disclosing the specific searches Plaintiff entered into the Website's search bar, Defendant

intercepted communications about Plaintiff's past or present medical condition (such as her diabetes), communications concerning her insurance coverage, and specific diabetes monitoring devices sought by Plaintiff.

199. Plaintiff Nguyen has used and continues to use the same devices to maintain and access an active Facebook account and an active Google account since at least 2008.

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

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

202. Defendant transmitted Plaintiff Nguyen's Facebook ID, computer IP address and other device and unique online identifiers to Facebook. Defendant also transmitted information such as health and medical information including Plaintiff's particular health condition, the type of medical service sought, and the fact that Plaintiff attempted to or did sign up for a trial of the FreeStyle Libre diabetes monitoring product.

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

204. Notwithstanding, through the Tracking Tools embedded on Defendant's Website, Defendant transmitted Plaintiff Nguyen's Private Information to, at a minimum, Facebook and Google (and likely many other third parties like Bing, Pinterest, Twitter, Yahoo and others).

205. Plaintiff Nguyen would not have utilized Defendant's medical services and/or used its Website or would have paid much less for Defendant's services had she known that her Private Information would be captured and disclosed to third parties like Facebook and Google without her consent.

206. As a result, Plaintiff Nguyen began receiving targeted advertisements on Facebook and Instagram related to diabetes monitoring and management, including ads for FreeStyle Libre 3, ads for diabetes management programs from Noom, CGM monitors for health and fitness, diabetes-related nutrition ads, and diabetes therapy ads.

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

208. Defendant did not inform Plaintiff Nguyen that it had shared her Private Information with Facebook.

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

Plaintiff Mitchell

210. As a condition of receiving Defendant's services, Plaintiff Mitchell disclosed her Private Information to Defendant on several occasions, including in August 2021, to review and request FreeStyle Libre CGM products via the free trial offered by Abbott.

211. Plaintiff Mitchell has been a customer of Defendant since at least August 2021 as she began using the FreeStyle Libre 2 CGM system at the time.

212. Plaintiff Mitchell accessed Defendant's Website on her phone and computer to research and request diabetes monitoring products from Defendant and at Defendant's direction.

213. Plaintiff Mitchell used Defendant's Website to review and request FreeStyle Libre products for herself as well as search for and communicate information related to her diabetes and other Private Information.

214. Her searches for and communication of information included her visiting specific webpages that revealed her PHI through the URLs as well as searches through the Website's search bar that disclosed the specific phrases she used to search for information related to her medical condition, her searches related to insurance coverage for diabetes monitoring systems sought from Defendant, and the details of her requests for Abbott's diabetes monitoring products.

215. The full scope of Defendant's interceptions and disclosures of Plaintiff Mitchell's communications to Meta can only be determined through formal discovery. However, in addition to disclosing the specific searches Plaintiff entered into the Website's search bar, Defendant intercepted communications about Plaintiff's past or present medical condition (such as her diabetes), communications concerning her insurance coverage, and specific diabetes monitoring devices sought by Plaintiff.

216. Plaintiff Mitchell has used and continues to use the same devices to maintain and access an active Facebook account and an active Google account throughout the relevant period in this case.

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

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

219. Defendant transmitted Plaintiff Mitchell's Facebook ID, computer IP address and other device and unique online identifiers to Facebook. Defendant also transmitted information such as health and medical information including Plaintiff Mitchell's particular health condition, the type of medical service sought, and the fact that Plaintiff attempted to or did sign up for a trial of the FreeStyle Libre diabetes monitoring product.

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

221. Notwithstanding, through the Tracking Tools embedded on Defendant's Website, Defendant transmitted Plaintiff Mitchell's Private Information to, at a minimum, Facebook and Google (and likely many other third parties like Bing, Pinterest, Twitter, Yahoo and others).

222. Plaintiff Mitchell would not have utilized Defendant's medical services and/or used its Website or would have paid much less for Defendant's services had she known that her Private Information would be captured and disclosed to third parties like Facebook and Google without her consent.

223. As a result, Plaintiff Mitchell began receiving targeted advertisements on Facebook and Instagram related to diabetes monitoring and management, including ads for FreeStyle Libre products.

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

225. Defendant did not inform Plaintiff Mitchell that it had shared her Private Information with Facebook.

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

Plaintiff Ortega

227. As a condition of receiving Defendant's services, Plaintiff Ortega disclosed his Private Information to Defendant on several occasions, including in July 2023, to review and request FreeStyle Libre CGM products via the free trial offered by Abbott, review cost and coverage information as well as other parts of the Website FAQ section, and to sign up for Defendant's newsletter.

228. Plaintiff Ortega has been a customer of Defendant since at least July 2023 as he began using the FreeStyle Libre 3 CGM system at the time.

229. Plaintiff Ortega accessed Defendant's Website on his phone and computer to research and request diabetes monitoring products from Defendant and at Defendant's direction.

230. Plaintiff Ortega used Defendant's Website to review and request FreeStyle Libre products for himself as well as search for and communicate information related to his diabetes and other Private Information.

231. His searches for and communication of information included him visiting specific webpages that revealed his PHI through the URLs as well as searches on the Website's Questions and Answers section that disclosed his information requests related to his medical condition, and the details of his requests for Abbott's diabetes monitoring products.

232. The full scope of Defendant's interceptions and disclosures of Plaintiff Ortega's communications to Meta can only be determined through formal discovery. However, in addition to disclosing the specific searches Plaintiff performed on the Website's FAQ section, Defendant

intercepted communications about Plaintiff's past or present medical condition (such as his diabetes) and specific diabetes monitoring devices sought by Plaintiff.

233. Plaintiff Ortega has used and continues to use the same devices to maintain and access an active Facebook account and an active Google account throughout the relevant period in this case.

234. Plaintiff Ortega reasonably expected that his communications with Defendant via the Website were confidential, solely between himself and Defendant, and that such communications would not be transmitted to or intercepted by a third party.

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

236. Defendant transmitted Plaintiff Ortega's Facebook ID, computer IP address and other device and unique online identifiers to Facebook. Defendant also transmitted information such as health and medical information including Plaintiff Ortega's particular health condition, the type of medical service sought, and the fact that Plaintiff attempted to or did sign up for a trial of the FreeStyle Libre diabetes monitoring product.

237. Plaintiff Ortega never consented to the disclosure of or use of his Private Information by third parties or to Defendant enabling third parties, including Facebook and Google, to access or interpret such information. Plaintiff Ortega never consented to any third parties' receipt or use of his Private Information.

238. Notwithstanding, through the Tracking Tools embedded on Defendant's Website, Defendant transmitted Plaintiff Ortega's Private Information to, at a minimum, Facebook and Google (and likely many other third parties like Bing, Pinterest, Twitter, Yahoo and others).

239. Plaintiff Ortega would not have utilized Defendant's medical services and/or used its Website or would have paid much less for Defendant's services had he known that his Private Information would be captured and disclosed to third parties like Facebook and Google without his consent.

240. As a result, Plaintiff Ortega began receiving targeted advertisements on Facebook and Instagram related to diabetes monitoring and management, including ads for FreeStyle Libre products.

241. By making these disclosures without his consent, Defendant breached Plaintiff Ortega's privacy and unlawfully disclosed his Private Information.

242. Defendant did not inform Plaintiff Ortega that it had shared his Private Information with Facebook.

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

TOLLING

244. The applicable statutes of limitation have been tolled as a result of Defendant's knowing and active concealment and denial of the facts alleged herein.

245. Defendant secretly incorporated Tracking Tools into its Website, providing no indication to users that their sensitive personal data, including their PHI and PII, would be disclosed to unauthorized third parties.

246. Defendant had exclusive knowledge that its Tracking Tools were incorporated on its Website yet failed to disclose that fact to customers and prospective customers or inform them

that by interacting with its Website Plaintiffs' and Class Members' PHI and PII would be disclosed to third parties, such as Meta and Google.

247. Plaintiffs and Class Members could not with due diligence have discovered the full scope of Defendant's conduct because the incorporation of Tracking Tools on Defendant's Website is highly technical and there were no disclosures or other indications that would inform a reasonable consumer that Defendant was disclosing and allowing Meta or Google to intercept PHI and PII.

248. The earliest Plaintiffs and Class Members could have known about Defendant's conduct was approximately in May of 2024, when they contacted the undersigned counsel to discuss their potential claims against Defendant. Nevertheless, at all material times herein, Defendant falsely represented to Plaintiffs that their health information is not and will not be disclosed to any third party.

249. As alleged above, Defendant has a duty to disclose the nature and significance of its data disclosure practices but failed to do so. Defendant is therefore estopped from relying on any statute of limitations under the discovery rule.

CLASS ACTION ALLEGATIONS

250. Plaintiffs Nguyen, Mitchell and Ortega bring this action on behalf of themselves and on behalf of all other persons similarly situated ("the Class") pursuant to Rule 23(b)(2), 23(b)(3) and 23(c)(4) of the Federal Rules of Civil Procedure.

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

All individuals residing in the United States whose Private Information was disclosed to a third party without authorization or consent through the Meta Pixel and other third-party tracking technologies on Abbott's Website.

252. The Illinois Sub-Class that Plaintiff Mitchell seeks to represent is defined as:

All individuals residing in the State of Illinois whose Private Information was disclosed to a third party without authorization or consent through the Meta Pixel and other third-party tracking technologies on Abbott's Website.

253. The California Sub-Class that Plaintiff Ortega seeks to represent is defined as:

All individuals residing in the State of California whose Private Information was disclosed to a third party without authorization or consent through the Meta Pixel and other third-party tracking technologies on Abbott's Website.

254. The Nationwide Class, Illinois Sub-Class and California Sub-Class are collectively referred to as the "Class" unless otherwise and more specifically identified.

255. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

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

257. Numerosity, Fed R. Civ. P. 23(a)(1). The Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are hundreds of thousands of individuals whose PII and PHI may have been improperly disclosed to Facebook, and the Class is identifiable within Defendant's records.

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

- a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiffs and Class Members;

- b. Whether Defendant had duties not to disclose the Private Information of Plaintiffs and Class Members to unauthorized third parties;
- c. Whether Defendant adequately, promptly and accurately informed Plaintiffs and Class Members that their Private Information would be disclosed to third parties;
- d. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their Private Information had been compromised;
- e. Whether Defendant adequately addressed and fixed the practices which permitted the disclosure of patient Private Information;
- f. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiffs and Class Members;
- g. Whether Plaintiffs and Class Members are entitled to actual, consequential and/or nominal damages as a result of Defendant's wrongful conduct; and
- h. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of Defendant's disclosure of their Private Information.

259. Typicality, Fed. R. Civ. P. 23(a)(3). Plaintiffs' claims are typical of those of other Class Members because all had their Private Information compromised as a result of Defendant's incorporation of the Facebook Pixel, due to Defendant's misfeasance.

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

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

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

262. Policies Generally Applicable to the Class. Fed. R. Civ. P. 23(b)(2). This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

263. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure

to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

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

265. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

266. Unless a class-wide injunction is issued, Defendant may continue disclosing the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the practices complained of herein, and Defendant may continue to act unlawfully as set forth in this Complaint.

267. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

268. Issue Certification, Fed. R. Civ. P. 23(c)(4). Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to, the following:

- a. Whether Defendant owed a legal duty to not disclose Plaintiffs' and Class Members' Private Information;
- b. Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;
- c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;
- d. Whether Defendant adequately and accurately informed Plaintiffs and Class Members that their Private Information would be disclosed to third parties;
- e. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information disclosed to third parties;
- f. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

CAUSES OF ACTION

COUNT I

VIOLATIONS OF ELECTRONIC COMMUNICATIONS PRIVACY ACT ("ECPA") 18 U.S.C. § 2511(1), *et seq.* UNAUTHORIZED INTERCEPTION, USE AND DISCLOSURE (On Behalf of Plaintiffs & the Nationwide Class)

269. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

270. The ECPA prohibits the intentional interception of the content of any electronic communication. 18 U.S.C. § 2511.

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

272. 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.

273. The transmissions of Plaintiffs' Private Information to Defendant via Defendant's Website qualifies as a "communication" under the ECPA's definition in 18 U.S.C. § 2510(12).

274. The transmissions of Plaintiffs' Private Information to medical professionals qualifies as a "communication" under the ECPA's definition in 18 U.S.C. § 2510(2).

275. **Electronic Communications.** The transmission of Private Information between Plaintiffs and Class Members and Defendant via its 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).

276. **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).

277. **Interception.** The ECPA defines the interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or

other device” and “contents ... include any information concerning the substance, purport, or meaning of that communication.” 18 U.S.C. § 2510(4), (8).

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

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

- a. The cookies Defendant and Meta use to track Plaintiffs’ and Class Members’ communications;
- b. Plaintiffs’ and Class Members’ browsers;
- c. Plaintiffs’ and Class Members’ computing devices;
- d. Defendant’s web-servers and
- e. The Tracking Tools deployed by Defendant to effectuate the sending and acquisition of patient communications.

280. Whenever Plaintiffs and Class Members interacted with Defendant’s Website, Defendant, through the Tracking Tools embedded and operating on its Website, contemporaneously and intentionally disclosed, and endeavored to disclose the contents of Plaintiffs’ and Class Members’ electronic communications to third parties, including Facebook and Google, without authorization or consent, and knowing or having reason to know that the electronic communications were obtained in violation of the ECPA. 18 U.S.C. § 2511(1)(c).

281. Whenever Plaintiffs and Class Members interacted with Defendant’s Website, Defendant, through the Tracking Tools embedded and operating on its Website, contemporaneously and intentionally used, and endeavored to use the contents of Plaintiffs’ and Class Members’ electronic communications, for purposes other than providing health care services to Plaintiffs and Class Members without authorization or consent, and knowing or having reason

to know that the electronic communications were obtained in violation of the ECPA. 18 U.S.C. § 2511(1)(d).

282. Whenever Plaintiffs and Class Members interacted with Defendant's Website, Defendant, through the Tracking Tools it embedded and operated on its Website, contemporaneously and intentionally redirected and disclosed the contents of Plaintiffs' and Class Members' electronic communications while those communications were in transmission, to persons or entities other than an addressee or intended recipient of such communication, including Facebook and Google.

283. Defendant's intercepted communications include, but are not limited to, the contents of communications to and/or from Plaintiffs' and Class Members' containing their PII and PHI, including medical diagnoses and medical devices sought.

284. Through the above-described Tracking Tools and intercepted communications, this information was, in turn, used by third parties, such as Facebook and Google, to 1) place Plaintiffs in specific health-related categories based on their past, present and future health condition and 2) target Plaintiffs with particular advertising associated with Plaintiffs' specific health condition.

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

286. By intentionally using, or endeavoring to use, the contents of the electronic communications of Plaintiffs and Class Members, while knowing or having reason to know that

the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

287. Defendant intentionally used the wire or electronic communications to violate HIPAA and increase its profit margins. Defendant specifically used the Tracking Tools to track and utilize Plaintiffs' and Class Members' PII and PHI for financial gain.

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

289. Plaintiffs and Class Members did not authorize Defendant to acquire the content of their communications for purposes of invading Plaintiffs' privacy via the Tracking Tools.

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

291. **Unauthorized Purpose.** Defendant intentionally intercepted the contents of Plaintiffs' and Class Members' electronic communications for the purpose of committing a tortious or criminal act in violation of the Constitution or laws of the United States or of any State, such as Illinois—namely, violations of HIPAA, among others.

292. **Any party exception in 18 U.S.C. § 2511(2)(d) does not apply.** The party exception in § 2511(2)(d) does not permit a party that intercepts or causes interception to escape liability if the communication is intercepted for the purpose of committing any tortious or criminal act in violation of the Constitution or laws of the United States or of any State.

293. Defendant is a “party to the communication” with respect to customer communications. However, Defendant's simultaneous, unknown duplication, forwarding and interception of Plaintiffs' and Class Members' Private Information does not qualify for the party exemption.

294. Here, as alleged above, Defendant violated a provision of HIPAA, specifically 42 U.S.C. § 1320d-6(a)(3). This provision imposes a criminal penalty for knowingly disclosing IIHI to a third party. HIPAA defines IIHI as:

any information, including demographic information collected from an individual, that—(A) is created or received by a health care provider ... (B) *relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual*, and (i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.⁶⁵

295. Plaintiffs’ information that Defendant disclosed to third parties qualifies as IIHI, and Defendant violated Plaintiffs’ expectations of privacy, and constitutes tortious and/or criminal conduct through a violation of 42 U.S.C. § 1320d(6). Defendant used the wire or electronic communications to increase its profit margins. Defendant specifically used the Pixel, Google tracking codes and other third-party tracking technologies to intercept and then disclose Plaintiffs’ and Class Members’ PII and PHI for financial gain.

296. The penalty for violation is enhanced where “the offense is committed with intent to sell, transfer, or use IIHI for commercial advantage, personal gain, or malicious harm.” 42 U.S.C. § 1320d-6.

297. Defendant’s conduct violated 42 U.S.C. § 1320d-6 in that it:

- a. Used and caused to be used cookie identifiers associated with specific customers without customer authorization; and
- b. Disclosed IIHI to Facebook and Google without customer authorization.

⁶⁵ § 1320d-(6) (emphasis added).

298. Defendant's conduct would be subject to the enhanced provisions of 42 U.S.C. § 1320d-6 because Defendant's use of the Facebook and Google source code was for Defendant's commercial advantage to increase revenue from existing customers and gain new customers.

299. Healthcare customers have the right to rely upon the promises that companies make to them. Defendant accomplished its tracking and retargeting through deceit and disregard, such that an actionable claim may be made, in that it was accomplished through source code that caused Facebook Pixels and other tracking codes (including but not limited to the `_fbp`, `_ga` and `_gid` cookies) and other tracking technologies to be deposited on Plaintiffs' and Class members' computing devices as "first-party" cookies that are not blocked.

300. The Pixel, `_fbp`, `_ga`, and `_gid` cookies, which constitute programs, commanded Plaintiffs' and Class Members' computing devices to remove and redirect their data and the content of their communications with Defendant to Facebook, Google, and others.

301. Defendant knew or had reason to know that the Pixel, `_fbp`, `_ga`, and `_gid` cookies would command Plaintiffs' and Class Members' computing devices to remove, redirect, and disclose their data and the content of their communications with Defendant to Google, Facebook, and others.

302. Defendant's scheme or artifice to defraud in this action consists of: (a) the false and misleading statements and omissions in its privacy policies set forth above, including the statements and omissions recited in the claims below; (b) the placement of the invisible Meta Pixel in its Website's source code; (c) the placement of the '`_fbp`' cookie on consumer computing devices disguised as a first-party cookie on Defendant's Website rather than a third-party cookie from Meta and (d) placement of the `_ga` and `_gid` cookies on consumer computing devices

disguised as a first-party cookies on Defendant's Website rather than third-party cookies from Google.

303. Defendant acted with the intent to defraud in that it willfully invaded and took Plaintiffs' and Class Members' property rights (a) to the confidentiality of Private Information and their right to determine whether such information remains confidential and exclusive right to determine who may collect and/or use such information for marketing purposes and (b) to determine who has access to their computing devices.

304. As such, Defendant cannot viably claim any exception to ECPA liability.

305. Plaintiffs and Class Members have suffered damages as a direct and proximate result of Defendant's invasion of privacy in that:

- a. Learning that Defendant has intruded upon, intercepted, transmitted, shared, and used their IIHI (including information about their medical symptoms, health conditions and medical devices sought) for commercial purposes has caused Plaintiffs and the Class Members to suffer emotional distress;
- b. Defendant received substantial financial benefits from its use of Plaintiffs' and Class Members' IIHI without providing any value or benefit to Plaintiffs or the Class Members;
- c. Defendant received substantial, quantifiable value from its use of Plaintiffs' and Class Members' IIHI, such as understanding how people use its Website, determining what ads people see on its Website, what ads to serve to potential consumers, and who potential consumers may be, without providing any value or benefit to Plaintiffs or the Class Members;

- d. Defendant has failed to provide Plaintiffs and the Class Members with the full value of the medical services and/or devices for which they paid, which included a duty to maintain the confidentiality of their health information; and
- e. The diminution in value of Plaintiffs' and Class Members' PII and PHI and the loss of privacy due to Defendant making sensitive and confidential information, such as medical conditions and diagnoses that Plaintiffs and Class Members intended to remain private no longer private.

306. As a result of Defendant's violation of the ECPA, Plaintiffs and Class Members are entitled to all damages available under 18 U.S.C. § 2520, including statutory damages of whichever is the greater of \$100 a day for each day of violation or \$10,000, equitable or declaratory relief, compensatory and punitive damages, and attorney's fees and costs.

COUNT II
NEGLIGENCE
(On behalf of Plaintiffs & the Nationwide Class)

307. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

308. Defendant owed Plaintiffs and Class Members a duty to keep their Private Information completely confidential, and to safeguard sensitive personal and medical information.

309. Plaintiffs and Class Members had reasonable expectations of privacy in their communications exchanged with Defendant, including communications exchanged on Defendant's Website.

310. Contrary to its duties as a medical provider and data collector⁶⁶ and its express promises of confidentiality, Defendant installed its Tracking Tools to disclose and transmit to third

⁶⁶ See 815 ILCS 530/45(a); see also 815 ILCS 530/5.

parties Plaintiffs' and Class Members' communications with Defendant, including Private Information and the contents of such information.

311. These disclosures were made without Plaintiffs' or Class Members' knowledge, consent, or authorization, and were unprivileged.

312. The third-party recipients included, but may not be limited to, Facebook and Google.

313. Plaintiffs have suffered fear, anxiety and worry about the status of, and the loss of control over, their private health information.

314. As a direct and proximate cause of Defendant's unauthorized disclosures of customers' personally identifiable, non-public medical information, and communications, Plaintiffs and Class Members were damaged by Defendant's breach in that:

- a. Sensitive and confidential information that Plaintiffs and Class Members intended to remain private is no longer private;
- b. Plaintiffs and Class Members face ongoing harassment and embarrassment in the form of unwanted targeted advertisements;
- c. Defendant eroded the essential confidential nature of the provider-patient relationship;
- d. General damages for invasion of their rights in an amount to be determined by a jury;
- e. Nominal damages for each independent violation;
- f. Defendant took something of value from Plaintiffs and Class Members and derived benefit therefrom without Plaintiffs' and Class Members' knowledge or informed consent and without compensation for such data;
- g. Plaintiffs and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality;
- h. Defendant's actions diminished the value of Plaintiffs' and Class Members' Private Information; and

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

COUNT III
VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT ("CIPA"),
Cal. Penal Code § 631
(On behalf of Plaintiff Ortega & the California Sub-Class)

315. Plaintiff Ortega re-alleges and incorporates by reference the allegations above as if fully set forth herein.

316. CIPA § 631(a) imposes liability for "distinct and mutually independent patterns of conduct." *Tavernetti v. Superior Ct.*, 22 Cal. 3d 187, 192-93 (1978). Thus, to establish liability under CIPA § 631(a), a plaintiff need only establish that the defendant, "by means of any machine, instrument, contrivance, or in any other manner," does any of the following:

Intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system,

Or

Willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or 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

Uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained,

Or

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.

317. Section 631(a) is not limited to phone lines, but also applies to "new technologies" such as computers, the Internet, and email. *See Matera v. Google Inc.*, 2016 WL 8200619, at *21

(N.D. Cal. Aug. 12, 2016) (CIPA applies to “new technologies” and must be construed broadly to effectuate its remedial purpose of protecting privacy); *Bradley v. Google, Inc.*, 2006 WL 3798134, at *5-6 (N.D. Cal. Dec. 22, 2006) (CIPA governs “electronic communications”); *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589 (9th Cir. 2020) (reversing dismissal of CIPA and common law privacy claims based on Facebook’s collection of consumers’ Internet browsing history).

318. The Tracking Tools are a “machine, instrument, contrivance, or ... other manner” used to engage in the prohibited conduct at issue here.

319. At all relevant times, by employing the Tracking Tools, Defendant intentionally tapped, electrically or otherwise, the lines of internet communication between Plaintiff Ortega and California Sub-Class Members on the one hand, and Defendant’s Website on the other hand.

320. At all relevant times, Defendant aided, agreed with, employed, and conspired with Facebook, Google and other third parties to use the Tracking Tools to wiretap consumers to Defendant’s Website and to accomplish the wrongful conduct at issue here.

321. The wrongful conduct at issue occurred in the State of California, where Defendant provided its services and products to Plaintiff Ortega and other California consumers.

322. Plaintiff Ortega and other California Class members used Defendant’s Website from California.

323. Plaintiff Ortega and California Sub-Class Members did not consent to Facebook and Google’s intentional access, interception, reading, learning, recording, and collection of Plaintiff Ortega and California Sub-Class Members’ electronic communications. Nor did Plaintiff Ortega and California Sub-Class Members consent to Defendant aiding, agreeing with, employing, or otherwise enabling Facebook and Google’s conduct.

324. The violation of section 631(a) constitutes an invasion of privacy sufficient to confer Article III standing.

325. Unless enjoined, Defendant will continue to commit the illegal acts alleged here. Plaintiff Ortega continues to be at risk because he frequently uses the internet to search for information about products or services. He continues to desire to use the internet for that purpose, including for the purpose of acquiring healthcare services online. Plaintiff also continues to desire to use Defendant's Website in the future but has no practical way to know if his website communications will be monitored or recorded by Facebook or Google.

326. Plaintiff Ortega and California Sub-Class Members seek all relief available under Cal. Penal Code § 637.2, including injunctive relief and statutory damages of \$5,000 per violation.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs Nguyen, Mitchell and Ortega, on behalf of themselves and all others similarly situated, respectfully requests judgment against Abbott and that this Honorable Court grant the following:

- A. an Order certifying the Class and appointing Plaintiffs and Counsel to represent such Class;
- B. equitable relief enjoining Defendant from engaging in the wrongful conduct alleged in this Complaint pertaining to the misuse and/or disclosure of the Private Information of Plaintiffs and Class Members;
- C. injunctive relief requested by Plaintiffs, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members:

- D. an award of damages, including, but not limited to, actual, consequential, statutory, punitive, and nominal damages, as allowed by law in an amount to be determined;
- E. an award of attorneys' fees, costs and litigation expenses, as allowed by law;
- F. prejudgment interest on all amounts awarded; and
- G. such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs Nguyen, Mitchell and Ortega hereby demand that this matter be tried before a jury.

DATE: September 11, 2024

Respectfully Submitted,

/s/ Matthew J. Langley

Matthew J. Langley (ARDC No. 6337129)

David S. Almeida (ARDC No. 6285557)

Britany Kabakov (ARDC No. 6336126)

ALMEIDA LAW GROUP LLC

849 W Webster Avenue

Chicago, IL 60614

Tel: (312) 576-3024

matt@almeidalawgroup.com

david@almeidalawgroup.com

britany@almeidalawgroup.com

David DiSabato

Tyler Bean*

SIRI & GLIMSTAD LLP

745 Fifth Avenue, Suite 500

New York, NY 10151

T: 929-677-5144

ddisabato@sirillp.com

tbean@sirillp.com

**pro hac vice to be sought*

Counsel for Plaintiffs & the Classes