IN THE SUPERIOR COURT OF THE STATE OF WASHINGTON
IN AND FOR THE COUNTY OF KING

ALEXANDER IRVINE and BARBARA TWADDELL, individually and on behalf of all others similarly situated, Plaintiffs, v. UNIVERSITY OF WASHINGTON, an agency of the STATE OF WASHINGTON Defendant.	Case No. CLASS ACTION COMPLAINT JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiffs Alexander Irvine and Barbara Twaddell (together, "Plaintiffs"), individually and on behalf of all others similarly situated (collectively, "Class members"), by and through their attorneys, bring this Class Action Complaint against Defendant University of Washington ("UW" or "Defendant") and complain and allege upon personal knowledge as to themselves and information and belief as to all other matters.

INTRODUCTION

1. Plaintiffs bring this class action against Defendant for its failure to secure and safeguard their and other patients' personally identifiable information ("PII") and personal health information ("PHI"), including but not limited to names, Social Security numbers, addresses, phone numbers, medical history, and insurance information.

STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

2. The University of Washington is a public university that controls and operates UW Medicine, an integrated health system.

3. On or about November 19, 2023, Fred Hutchinson Cancer Center ("FHCC"), a nonprofit organization that serves as UW Medicine's cancer program, discovered that an unauthorized party had gained access to FHCC's network systems and removed certain files, including files that contained the PII/PHI of Plaintiffs and Class members ("Data Breach").

4. FHCC's database and medical record keeping system is integrated with UW Medicine's database and record keeping system such that FHCC's database stores and maintains information for patients of UW Medicine who have never sought or received services from FHCC.

5. Defendant owed a duty to Plaintiffs and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII/PHI against unauthorized access and disclosure. Defendant breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect the PII/PHI they collect and maintain from unauthorized access and disclosure.

6. As a result of Defendant's inadequate security and breach of duties and obligations, the Data Breach occurred, and Plaintiffs' and Class members' PII/PHI was accessed and disclosed. This action seeks to remedy these failings and their consequences. Plaintiffs bring this action on behalf of themselves and all persons whose PII/PHI was exposed as a result of the Data Breach, which FHCC discovered on or about November 19, 2023.

7. Plaintiffs, on behalf of themselves and all other Class members, assert claims for negligence, negligence per se, breach of fiduciary duty, breach of implied contract, unjust enrichment, violation of the Washington Consumer Protection Act, and seek declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

PARTIES

Plaintiff Alexander Irvine

8. Plaintiff Irvine is a citizen of Washington.

9. Plaintiff Irvine obtained healthcare or related services from Seattle Cancer Care Alliance and FHCC, affiliates of UW Medicine.[1] As a condition of receiving services, FHCC required Plaintiff Irvine to provide them with his PII/PHI.

10. Based on representations made by Defendant and FHCC, Plaintiff Irvine believed Defendant had implemented and maintained reasonable security and practices to protect his PII/PHI. With this belief in mind, Plaintiff Irvine provided his PII/PHI to FHCC and Defendant in connection with receiving healthcare services provided by FHCC as an affiliate of Defendant.

11. At all relevant times, Defendant stored and maintained Plaintiff Irvine's PII/PHI on their network systems.

12. Plaintiff Irvine takes great care to protect his PII/PHI. Had Plaintiff Irvine known that Defendant does not adequately protect the PII/PHI in their possession, he would not have obtained healthcare services from Defendant or its affiliates or agreed to entrust them with his PII/PHI.

13. Plaintiff Irvine received an email from UW Medicine notifying him that the Data Breach impacted his PII/PHI.

14. As a direct result of the Data Breach, Plaintiff Irvine has suffered injury and damages including, *inter alia*, a substantial and imminent risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of his highly sensitive PII/PHI; deprivation of the value of his PII/PHI; and overpayment for services that did not include adequate data security.

[1] Seattle Cancer Care Alliance merged with FHCC in 2022. Fred Hutch News Service Staff, *Fred Hutch and Seattle Cancer Care Alliance Unite, Reshape Relationship with UW Medicine*, FHCC (Apr. 1, 2022), https://www.fredhutch.org/en/news/center-news/2022/04/fred-hutch-scca-restructure.html.

STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

15. Plaintiff Irvine submitted a tort claim form regarding the Data Breach to the Office of Risk Management on December 12, 2023. He has not received a response.

Plaintiff Barbara Twaddell

16. Plaintiff Twaddell is a citizen of Washington.

17. Plaintiff Twaddell obtained healthcare or related services from FHCC, an affiliate of UW Medicine. As a condition of receiving services, FHCC required Plaintiff Twaddell to provide them with her PII/PHI.

18. Based on representations made by Defendant and FHCC, Plaintiff Twaddell believed Defendant had implemented and maintained reasonable security and practices to protect her PII/PHI. With this belief in mind, Plaintiff Twaddell provided her PII/PHI to FHCC and Defendant in connection with receiving healthcare services provided by FHCC as an affiliate of Defendant.

19. At all relevant times, Defendant stored and maintained Plaintiff Twaddell's PII/PHI on their network systems.

20. Plaintiff Twaddell takes great care to protect her PII/PHI. Had Plaintiff Twaddell known that Defendant does not adequately protect the PII/PHI in their possession, she would not have obtained healthcare services from Defendant or its affiliates or agreed to entrust them with her PII/PHI.

21. Plaintiff Twaddell received an extortion email from the cybercriminals responsible for the Data Breach. The email contained her PII/PHI, including her medical record number, address, medical diagnosis, and insurance. The email demanded $50 in exchange for removing her data from the dark web website where it is listed for sale.

22. As a direct result of the Data Breach, Plaintiff Twaddell has suffered injury and damages including, *inter alia*, a substantial and imminent risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of her highly sensitive PII/PHI;

STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

deprivation of the value of her PII/PHI; and overpayment for services that did not include adequate data security.

23. Plaintiff Twaddell submitted a tort claim form regarding the Data Breach to the Office of Risk Management on December 12, 2023. She has not received a response.

Defendant University of Washington

24. The University of Washington is a public university formed by the State of Washington.

JURISDICTION AND VENUE

25. This Court has jurisdiction over this action pursuant to RCW 2.08.010. This action is brought as a class action on behalf of Plaintiffs and all Class members pursuant to Washington Superior Court Civil Rule 23.

26. This Court has personal jurisdiction over the University of Washington because it is a state entity authorized under the laws of the State of Washington.

27. Venue is proper in King County pursuant to RCW 4.12.020, RCW 4.12.025, and RCW 4.92.010 because the University of Washington's principal places of business are located in King County.

FACTUAL ALLEGATIONS

Overview of Defendant

28. UW Medicine is an "integrated clinical, research and learning health system" that provides primary and specialized healthcare services.[2] UW Medicine is "a family of organizations… operated or managed as part of an integrated health system."[3] Some of the organizations that form UW Medicine are legally part of the University of Washington, while

[2] *UW Medicine Overview*, UW MED., https://depts.washington.edu/uwmmktg/wp-content/uploads/2022/04/UWMedicine-Overview.pdf (last accessed Feb. 12, 2024).
[3] *Id.*

STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

others are separate.[4] UW Medicine is the only comprehensive clinical, research, and learning health system in Washington.[5]

29. FHCC "is an independent, nonprofit organization, that also serves as UW Medicine's cancer program."[6] FHCC "operates eight clinical care sites that provide medical oncology, infusion, radiation, proton therapy and related services."[7]

30. In the regular course of their business, Defendant collects and maintains the PII/PHI of current and former patients. Defendant requires patients to provide their PII/PHI before they provide medical services.

31. FHCC was established in its current form in April, 2022, "by the merger of Fred Hutchinson Cancer Research Center and Seattle Cancer Care Alliance, with the goal of bringing scientific advances to patients more quickly."[8] FHCC is now "a clinically integrated part of UW Medicine and UW Medicine's cancer program."[9] FHCC provides managerial oversight for UW Medical services that provide cancer care.[10]

32. FHCC, as an affiliate of UW Medicine, provided healthcare services to over 53,000 patients in 2022.[11]

33. FHCC's website and UW Medicine's website each contain an identical Joint Notice of Privacy Practices ("Privacy Policy").[12] The Privacy Policy lists the ways Defendant says it will

---

[4] *Id.*
[5] *See id.*
[6] *About Fred Hutchinson Cancer Center*, FHCC, https://www.fredhutch.org/en/about/about-the-hutch.html (last accessed Feb. 12, 2024).
[7] *The UW Medicine Family*, UW MED., https://www.uwmedicine.org/about/the-uwmedicine-family (last accessed Feb. 12, 2024).
[8] *2022 Annual Report*, FHCC (2022), https://www.fredhutch.org/en/about/about-the-hutch/annual-report.html#merger (last accessed Feb. 12, 2024).
[9] Fred Hutch News Service Staff, *supra* note 1.
[10] *See id.*
[11] *See 2022 Annual Report*, *supra* note 8.
[12] *Joint Notice of Privacy Practices*, FHCC (Dec. 19, 2022), https://www.fredhutch.org/content/dam/www/clinical-pdf/patient-policies/joint-notice-of-privacy-practices.pdf; *Joint Notice of Privacy Practices*, UW MED. (Dec. 19, 2022),

STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

use or disclose patients' personal information, including for treatment, billing services, and research.[13]

34. In the Privacy Policy, Defendant acknowledges it is "required by law to maintain the privacy and security of your protected health information."[14] Defendant states it "must follow the duties and privacy practices described in this notice."[15] Defendant promises it "will not use or share your information other than as described here unless you tell us we can in writing."[16]

35. The Privacy Policy explains that "UW Medicine and Fred Hutch participate in organized healthcare arrangements. Although these two organizations are separate healthcare entities, they share patient information for treatment, payment, and operations related to the organized healthcare arrangement."[17]

36. Plaintiff and Class members are persons whose PII/PHI was collected and maintained by UW Medicine or by FHCC as an affiliate of UW Medicine.

The Data Breach and Defendant's Other Recent Data Breaches

37. On or about November 19, 2023, FHCC discovered an unauthorized third-party accessed FHCC's network and the sensitive information stored therein.[18] According to the data breach notice on FHCC's website, "Based on the information available, the criminal group responsible is outside the United States."[19]

38. According to FHCC, patients of UW Medicine were also impacted, "Since UW Medicine clinicians also provide care to patients at Fred Hutch and some services are provided

---

https://www.uwmedicine.org/sites/stevie/files/2023-01/A11499.MED_.M%20-%20Notice%20of%20Privacy%20Practice%20BROCHURE%2011.01.22_a11y.pdf.

[13] *See id.*

[14] *Id.*

[15] *Id.*

[16] *Id.*

[17] *Id.*

[18] *See Data Security Incident*, FHCC (Dec. 11, 2023), https://www.fredhutch.org/en/about/about-the-hutch/accountability-impact/data-security-incident.html (last accessed Dec. 11, 2023).

[19] *Id.*

STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

across multiple Fred Hutch and UW Medicine locations, the patient data necessary to provide this care is shared across systems. The cybersecurity incident specifically involved Fred Hutch systems but those systems also had some UW Medicine patient data related to areas such as preventative and oncology care."[20]

39. The cybercriminals responsible for the Data Breach have attempted to extort victims of the Data Breach via threatening emails.[21] In these emails, the cybercriminals claim to have stolen 800,000 patient records,[22] including names, Social Security numbers, addresses, phone numbers, medical history, lab results, and insurance information.[23]

40. The extortion emails sent to victims of the Data Breach offer to remove the victim's PII/PHI from the dark web for a fee of $50.[24] FHCC has admitted that victims are receiving these threatening emails.[25]

41. The U.S. Department of Health & Human Services has reported the number of affected individuals is 890,959.[26]

42. FHCC's website notice warns victims to "remain vigilant to protect against potential fraud and/or identity theft."[27]

43. Despite learning of the Data Breach on or about November 19, 2023, neither FHCC nor UW began notifying impacted individuals until early December 2023. Defendant's failure to

---

[20] *Id.*

[21] *E.g.*, KING 5 Staff, *'DO NOT PAY IT': Fred Hutch Warns of 'Threatening Spam Emails' After Cyberattack*, KING 5 NEWS (Dec. 7, 2023 6:20 PM), https://www.king5.com/article/news/local/fred-hutch-warn-patients-threatening-emails-cyberattack/281-40365cfa-61c9-4395-91ad-2c819695d4c0.

[22] *Id.*

[23] *E.g.*, Brittany Toolis, *Cancer Patients Face Blackmail Threats After Fred Hutch Data Breach*, MYNORTHWEST (Dec. 8, 2023 6:38 AM), https://mynorthwest.com/3942300/cancer-patients-face-blackmail-threats-after-fred-hutch-data-breach/.

[24] *Id.*

[25] *See Data Security Incident*, *supra* note 18.

[26] Breach Portal, U.S. Department of Health and Human Services Office for Civil Rights, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed February 9, 2024).

[27] *See Data Security Incident*, *supra* note 18.

STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

promptly notify Plaintiffs and Class members that their PII/PHI was accessed and stolen virtually ensured that the unauthorized third parties who exploited those security lapses could monetize, misuse, or disseminate that PII/PHI before Plaintiffs and Class members could take affirmative steps to protect their sensitive information. As a result, Plaintiffs and Class members will suffer indefinitely from the substantial and concrete risk that their identities will be (or already have been) stolen and misappropriated.

44. The Data Breach is not the first data breach that Defendant or its affiliate FHCC have experienced in recent years. FHCC experienced a separate data incident between March 25, 2022, and March 26, 2022, in which an unauthorized person accessed an employee's email account containing patient information.[28] In 2018, it was discovered that the PII/PHI of approximately 974,000 UW Medicine patients was exposed online and available through Google's search engine.[29] The PHI of approximately 3,800 UW Medicine patients was affected by a ransomware attack at a third-party vendor of UW Medicine's in 2022.[30]

Defendant Knew that Criminals Target PII/PHI

45. At all relevant times, Defendant knew, or should have known, that Plaintiffs' and all other Class members' PII/PHI was a target for malicious actors. Indeed, its affiliate FHCC admitted in its website notice that "all organizations face cybersecurity risks and these kind of attacks have targeted multiple healthcare institutions in the past."[31] Further, Defendant's Joint

[28] *Notice of a Data Security Incident Involving Seattle Cancer Care Alliance Patients*, FHCC (May 25, 2022), https://www.fredhutch.org/en/news/releases/2022/06/notice-of-a-data-security-incident-involving-seattle-cancer-care.html.

[29] *See* Jessica Davis, *Health Data of 974,000 UW Medicine Patients Exposed for 3 Weeks*, HEALTH IT SEC. (Feb. 21, 2019), https://healthitsecurity.com/news/health-data-of-974000-uw-medicine-patients-exposed-for-3-weeks.

[30] Naomi Diaz, *3,800 UW Medicine Patients Affected by 3rd-Party Data Breach*, BECKER'S HEALTH IT (Oct. 7, 2022), https://www.beckershospitalreview.com/cybersecurity/3-800-uw-medicine-patients-affected-by-3rd-party-data-breach.html.

[31] *Data Security Incident*, *supra* note 18.

STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

Notice of Privacy Practices states that Defendants will "let you know promptly if a breach occurs that may have compromised the privacy or security of your information."[32]

46. Despite such knowledge, Defendant failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiffs' and Class members' PII/PHI from cyber-attacks that Defendant should have anticipated and guarded against. Defendant should have been particularly aware of the possibility of a data breach because of the recent data breaches they and their affiliates have experienced.

47. It is well known amongst companies that store sensitive personally identifying information that sensitive information—such as the Social Security numbers and medical information stolen in the Data Breach—is valuable and frequently targeted by cybercriminals. In a recent article, *Business Insider* noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers… Many of them were caused by flaws in… systems either online or in stores."[33]

48. Cybercriminals seek out PHI at a greater rate than other sources of personal information. In a 2023 report, the healthcare compliance company Protenus found that there were 956 medical data breaches in 2022 with over 59 million patient records exposed.[34] This is an increase from the 758 medical data breaches which exposed approximately 40 million records that Protenus compiled in 2020.[35]

[32] *Joint Notice*, *supra* note 12.
[33] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUS. INSIDER (Nov. 19, 2019, 8:05 AM), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.
[34] *See* PROTENUS, *2023 Breach Barometer*, PROTENUS.COM, https://www.protenus.com/breach-barometer-report (last accessed Feb. 12, 2024).
[35] *See id*.

STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

49. PII/PHI is a valuable property right.[36] The value of PII/PHI as a commodity is measurable.[37] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[38] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[39] It is so valuable to identity thieves that once PII/PHI has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

50. As a result of the real and significant value of this material, identity thieves and other cyber criminals have openly posted credit card numbers, SSNs, PII/PHI, and other sensitive information directly on various Internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be readily aggregated and become more valuable to thieves and more damaging to victims.

51. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[40] A cybercriminal who steals a person's PHI can end up with as many as "seven to ten personal identifying characteristics of an individual."[41]

---

[36] *See* Marc van Lieshout, *The Value of Personal Data*, 457 INT'L FED'N FOR INFO. PROCESSING 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible…"), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.

[37] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE.COM (April 28, 2014), http://www.medscape.com/viewarticle/824192.

[38] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD iLIBRARY (April 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[39] *See* IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

[40] *See* Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAG. (Oct. 20, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").

[41] *Id.*

STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

52. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,300 each on the black market.[42] According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[43]

53. Criminals can use stolen PII/PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[44] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion… By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[45]

54. Consumers place a high value on the privacy of that data, as they should. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[46]

---

[42] *See* SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAG. (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.

[43] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.

[44] Steager, *supra* note 41.

[45] *Id.*

[46] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFO. SYS. RSCH. 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

55. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII/PHI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

Theft of PII/PHI Has Grave and Lasting Consequences for Victims

56. Theft of PII/PHI can have serious consequences for the victim. The FTC warns consumers that identity thieves use PII/PHI to receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[47] [48]

57. Experian, one of the largest credit reporting companies in the world, warns consumers that "[i]dentity thieves can profit off your personal information" by, among other things, selling the information, taking over accounts, using accounts without permission, applying for new accounts, obtaining medical procedures, filing a tax return, and applying for government benefits.[49]

58. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that almost 20% of victims of identity misuse needed more than a month to resolve issues stemming from identity theft.[50]

---

[47] *See* Federal Trade Commission, *What to Know About Identity Theft*, FED. TRADE COMM'N CONSUMER INFO., https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Feb. 12, 2024).

[48] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 12 C.F.R. § 1022.3(g).

[49] *See* Louis DeNicola, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN (May 21, 2023), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[50] Identity Theft Resource Center, *2023 Consumer Aftermath Report*, IDENTITY THEFT RES. CTR. (2023), https://www.idtheftcenter.org/publication/2023-consumer-impact-report/ (last accessed Feb. 12, 2024).

STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

59. Theft of SSNs also creates a particularly alarming situation for victims because SSNs cannot easily be replaced. In order to obtain a new SSN, a breach victim has to demonstrate ongoing harm from misuse. Thus, a new SSN will not be provided until after the victim has already suffered harm.

60. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[51]

61. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[52] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[53] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use PII/PHI "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care." [54] The FTC also warns, "If the thief's health information is mixed with yours it could affect the medical care you're able to get or the health insurance benefits you're able to

[51] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (August 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.
[52] Pam Dixon & John Emerson, *The Geography of Medical Identity Theft*, FTC.GOV (Dec. 12, 2017), http://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf.
[53] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk . . ., supra* note 44.
[54] *See What to Know About Medical Identity Theft*, FED. TRADE COMM'N CONSUMER INFO., https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last accessed Feb. 12, 2024).

STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

use."[55]

62. A report published by the World Privacy Forum and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

a. Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.

b. Significant bills for medical goods and services neither sought nor received.

c. Issues with insurance, co-pays, and insurance caps.

d. Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.

e. Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.

f. As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.

g. Phantom medical debt collection based on medical billing or other identity information.

h. Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.[56]

63. There may also be time lags between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. On average it takes approximately three months for consumers to discover their identity has been stolen and used, but it takes some individuals up to three years to learn that information.[57]

---

[55] *Id*.
[56] *See* Dixon & Emerson, *supra* note 54.
[57] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 J. OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

64. It is within this context that Plaintiffs and Class members must now live with the knowledge that their PII/PHI is forever in cyberspace, having been stolen by criminals willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

Damages Sustained by Plaintiffs and Class Members

65. Plaintiffs and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendant's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for services that were received without adequate data security.

CLASS ALLEGATIONS

66. This action is brought and may be properly maintained as a class action pursuant to Washington Superior Court Civil Rule 23.

67. Plaintiffs bring this action on behalf of themselves and all members of the following Class of similarly situated persons:

> All United States citizens whose personally identifiable information or personal health information was accessed in the Data Breach and disclosed to unauthorized persons, including all United States residents who were sent a notice of the Data Breach.

68. Excluded from the Class are: (i) Fred Hutchinson Cancer Center and its affiliates, parents, subsidiaries, officers, agents, employees, and directors; (ii) the University of Washinton and its affiliates, parents, subsidiaries, officers, agents, employees, directors, and regents; and (iii) the judge(s) presiding over this matter and the clerks of said judge(s).

STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

69. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

70. The members in the Class are so numerous that joinder of all Class members in a single proceeding would be impracticable. The cybercriminals that perpetrated the Data Breach have stated that 800,000 persons' PII/PHI was affected in the Data Breach.[58] The U.S. Department of Health & Human Services has reported the number of affected individuals is 890,959.[59]

71. Common questions of law and fact exist as to all Class members and predominate over any potential questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

a. Whether Defendant had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiffs' and Class members' PII/PHI from unauthorized access and disclosure;

b. Whether Defendant had duties not to disclose the PII/PHI of Plaintiffs and Class members to unauthorized third parties;

c. Whether Defendant failed to exercise reasonable care to secure and safeguard Plaintiffs' and Class members' PII/PHI;

d. Whether an implied contract existed between Class members and Defendant, providing that Defendant would implement and maintain reasonable security measures to protect and secure Class members' PII/PHI from unauthorized access and disclosure;

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

f. Whether Defendant breached its duties to protect Plaintiffs' and Class members' PII/PHI; and

g. Whether Plaintiffs and Class members are entitled to damages and the measure of such damages and relief.

[58] *See* Toolis, *supra* note 24.

[59] Breach Portal, U.S. Department of Health and Human Services Office for Civil Rights, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed February 9, 2024).

STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

72. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs on behalf of themselves and all other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

73. Plaintiffs' claims are typical of the claims of the Class. Plaintiffs, like all proposed members of the Class, had their PII/PHI compromised in the Data Breach. Plaintiffs and Class members were injured by the same wrongful acts, practices, and omissions committed by Defendant, as described herein. Plaintiffs' claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

74. Plaintiffs will fairly and adequately protect the interests of the Class members. Plaintiffs are adequate representatives of the Class in that they have no interests adverse to, or that conflict with, the Class they seek to represent. Plaintiffs have retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

75. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiffs and all other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for Class members to individually seek redress from Defendant's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

CAUSES OF ACTION

COUNT I
NEGLIGENCE

76. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

77. Defendant owed a duty to Plaintiffs and all other Class members to exercise reasonable care in safeguarding and protecting their PII/PHI in its possession, custody, or control.

78. Defendant knew the risks of collecting and storing Plaintiffs' and all other Class members' PII/PHI and the importance of maintaining secure systems. UW knew of the many data breaches that targeted healthcare providers in recent years, including FHCC, its affiliate, and experienced a recent data breach itself.

79. Given the nature of UW Medicine's business, the sensitivity and value of the PII/PHI it maintains, and the resources at its disposal, Defendant should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring.

80. Defendant breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII/PHI entrusted to it—including Plaintiffs' and Class members' PII/PHI.

81. It was reasonably foreseeable to Defendant that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiffs' and Class members' PII/PHI to unauthorized individuals.

STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

82. But for Defendant's negligent conduct or breach of the above-described duties owed to Plaintiffs and Class members, their PII/PHI would not have been compromised.

83. As a result of Defendant's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiffs and all other Class members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendant's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT II
NEGLIGENCE PER SE

84. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

85. Defendant's duties arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

86. Defendant's duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by business, such as UW Medicine, of failing to employ reasonable measures to protect and secure PII/PHI.

STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

87. Defendant violated HIPAA Privacy and Security Rules and Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiffs' and all other Class members' PII/PHI and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII/PHI it obtains and stores, and the foreseeable consequences of a data breach involving PII/PHI including, specifically, the substantial damages that would result to Plaintiffs and the other Class members.

88. Defendant's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA constitutes negligence per se.

89. Plaintiffs and Class members are within the class of persons that HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to protect.

90. The harm occurring as a result of the Data Breach is the type of harm HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to guard against.

91. It was reasonably foreseeable to Defendant that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiffs' and Class members' PII/PHI to unauthorized individuals.

92. The injury and harm that Plaintiffs and the other Class members suffered was the direct and proximate result of Defendant's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA. Plaintiffs and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to

STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendant's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT III
BREACH OF FIDUCIARY DUTY

93. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

94. Plaintiffs and Class members gave UW Medicine their PII/PHI in confidence, or gave it to another entity in confidence which then gave their PII/PHI to UW Medicine such that Defendant was entrusted with the PII/PHI, believing that Defendant and FHCC would protect that information. Plaintiffs and Class members would not have provided Defendant with this information or would not have allowed Defendant to obtain this information, had they known it would not be adequately protected. Defendant's acceptance and storage of Plaintiffs' and Class members' PII/PHI created a fiduciary relationship between Defendant and Plaintiffs and Class members. In light of this relationship, Defendant must act primarily for the benefit of the persons it collects the PII/PHI of, which includes safeguarding and protecting Plaintiffs' and Class members' PII/PHI.

95. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class members upon matters within the scope of their relationship. It breached that duty by failing to properly protect the integrity of the system containing Plaintiffs' and Class members' PII/PHI, failing to comply with data security guidelines, and otherwise failing to safeguard Plaintiffs' and Class members' PII/PHI that it collected.

96. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class members have suffered and will suffer injury, including, but not limited to: (i)

STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendant's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT IV
VIOLATION OF THE WASHINGTON CONSUMER PROTECTION ACT
RCW §§ 19.86.010 et seq. ("WCPA")

97. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

98. Plaintiffs and Defendant are "persons" under the WCPA. RCW § 19.86.010(1).

99. Defendant's sale of services to Plaintiffs and all other Class members constitutes as "trade" and "commerce" under the WCPA. RCW § 19.86.010(2).

100. The WCPA states, "Unfair methods of competition and unfair or deceptive practices in the conduct of any trade or commerce are hereby declared unlawful." RCW § 19.86.020. Defendant's failure to adequately safeguard Plaintiffs and Class members PII/PHI while representing that their PII/PHI would be protected is an "unfair or deceptive practice" under the WCPA.

101. Defendant's failure to adequately safeguard Plaintiffs' and the Class members' PII/PHI is injurious to the public interest pursuant to RCW § 19.86.093(3)(a) because Defendant's actions not only harmed Plaintiffs, but harmed hundreds of thousands of other persons.

STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

102. Had Plaintiffs and Class members been aware of the omitted and misrepresented facts, i.e., that Defendant would not adequately protect their PII/PHI, Plaintiffs and Class members would not have sought services from Defendant.

103. Pursuant to RCW § 19.86.090, Plaintiffs seek actual and treble damages on behalf of themselves and all other Class members.

PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of all other members of the Class, respectfully request that the Court enter judgment in their favor and against Defendant as follows:

A. Certifying the Class as requested herein, designating Plaintiffs as Class Representative, and appointing Plaintiffs' counsel as Class Counsel;

B. Awarding Plaintiffs and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, disgorgement, and nominal damages if and as appropriate;

C. Awarding Plaintiffs and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiffs, on behalf of themselves and the Class, seek appropriate injunctive relief designed to prevent Defendant from experiencing another data breach by adopting and implementing best data security practices to safeguard PII/PHI and to provide or extend credit monitoring services and similar services to protect against all types of identity theft and medical identity theft;

D. Awarding Plaintiffs and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiffs and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiffs and the Class such other favorable relief as allowable under law.

STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury of all claims in this Class Action Complaint so triable.

Dated: February 12, 2024

Respectfully submitted,

/s/ Alexander F. Strong

Alexander F. Strong, WSBA #49839
STOBAUGH & STRONG P.C.
126 NW Canal Street, Suite 100
Seattle, WA 98107
astrong@bs-s.com
Telephone: (206) 622-3536
Facsimile: (206) 622-5759

Ben Barnow*
Anthony L. Parkhill*
Riley W. Prince*
BARNOW AND ASSOCIATES, P.C.
205 West Randolph Street, Ste. 1630
Chicago, IL 60606
b.barnow@barnowlaw.com
aparkhill@barnowlaw.com
rprince@barnowlaw.com
Tel: (312) 621-2000
Fax: (312) 641-5504

**pro hac vice* forthcoming