

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26

**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.

FRED HUTCHINSON CANCER CENTER
and UNIVERSITY OF WASHINGTON,

Defendants.

Case No.

CLASS ACTION

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 Defendants Fred Hutchinson Cancer Center (“FHCC”) and University of Washington (“UW” and together with FHCC, “Defendants”) 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 Defendants for their failure to secure and safeguard their and other patients’ personally identifiable information (“PII”) and personal health information (“PHI”), including names, Social Security numbers, addresses, phone numbers, medical history, lab results, and insurance information.

1 8. Plaintiff Irvine obtained healthcare or related services from Seattle Cancer Care
2 Alliance and FHCC.¹ As a condition of receiving services, FHCC required Plaintiff Irvine to
3 provide them with his PII/PHI.

4 9. Based on representations made by Defendants, Plaintiff Irvine believed Defendants
5 had implemented and maintained reasonable security and practices to protect his PII/PHI. With
6 this belief in mind, Plaintiff Irvine provided his PII/PHI to Defendants in connection with receiving
7 healthcare services provided by Defendants.

8 10. At all relevant times, Defendants stored and maintained Plaintiff Irvine's PII/PHI
9 on their network systems.

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

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

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

20 ***Plaintiff Barbara Twaddell***

21 14. Plaintiff Twaddell is a citizen of Washington.

22
23
24
25 ¹ Seattle Cancer Care Alliance merged with FHCC in 2022. Fred Hutch News Service Staff, *Fred
26 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>.

1 26. In the regular course of their business, Defendants collect and maintain the PII/PHI
2 of their current and former patients. Defendants require patients to provide their PII/PHI before
3 they provide medical services.

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

9 28. FHCC provided healthcare services to over 53,000 patients in 2022.¹¹

10 29. FHCC’s website and UW Medicine’s website each contain an identical Joint Notice
11 of Privacy Practices (“Privacy Policy”).¹² The Privacy Policy lists the ways Defendants say they
12 will use or disclose patients’ personal information, including for treatment, billing services, and
13 research.¹³

14 30. In the Privacy Policy, Defendants acknowledge they are “required by law to
15 maintain the privacy and security of your protected health information.”¹⁴ Defendants state they
16 “must follow the duties and privacy practices described in this notice.”¹⁵ Defendants promise they
17

18
19
20 ⁸ 2022 Annual Report, FHCC (2022), <https://www.fredhutch.org/en/about/about-the-hutch/annual-report.html#merger> (last accessed Dec. 11, 2023).

21 ⁹ Fred Hutch News Service Staff, *supra* note 1.

22 ¹⁰ *See id.*

23 ¹¹ *See 2022 Annual Report, supra* note 8.

24 ¹² *Joint Notice of Privacy Practices*, FHCC (Dec. 19, 2022),
25 <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),
26 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.*

1 “will not use or share your information other than as described here unless you tell us we can in
2 writing.”¹⁶

3 31. The Privacy Policy explains that “UW Medicine and Fred Hutch participate in
4 organized healthcare arrangements. Although these two organizations are separate healthcare
5 entities, they share patient information for treatment, payment, and operations related to the
6 organized healthcare arrangement.”¹⁷

7 32. Plaintiff and Class members are persons whose PII/PHI was collected and
8 maintained by FHCC or UW Medicine.

9 ***The Data Breach and Defendants’ Other Recent Data Breaches***

10 33. On or about November 19, 2023, FHCC discovered an unauthorized individual, or
11 unauthorized individuals, had gained access to FHCC’s network systems and the sensitive
12 information stored therein.¹⁸ According to the data breach notice on FHCC’s website, “Based on
13 the information available, the criminal group responsible is outside the United States.”¹⁹

14 34. According to FHCC, patients of UW Medicine were also impacted, “Since UW
15 Medicine clinicians also provide care to patients at Fred Hutch and some services are provided
16 across multiple Fred Hutch and UW Medicine locations, the patient data necessary to provide this
17 care is shared across systems. The cybersecurity incident specifically involved Fred Hutch systems
18 but those systems also had some UW Medicine patient data related to areas such as preventative
19 and oncology care.”²⁰

20 35. Defendants have not completed their investigation and have yet to release the exact
21 scope and scale of the Data Breach.²¹ However, the cybercriminals responsible for the Data Breach
22

23 ¹⁶ *Id.*

24 ¹⁷ *Id.*

25 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).

26 ¹⁹ *Id.*

²⁰ *Id.*

²¹ *See Notice of Information Security Incident Involving Fred Hutchinson Cancer Center*, FHCC

1 have begun attempts to extort victims of the Data Breach via threatening emails.²² In these emails,
2 the cybercriminals claim to have stolen 800,000 patient records,²³ including names, Social Security
3 numbers, addresses, phone numbers, medical history, lab results, and insurance information.²⁴

4 36. The extortion emails sent to victims of the Data Breach offers to remove the victim's
5 PII/PHI from the dark web for a fee of \$50.²⁵ FHCC has admitted that victims are receiving these
6 threatening emails.²⁶

7 37. FHCC's website notice warns victims to "remain vigilant to protect against potential
8 fraud and/or identity theft."²⁷

9 38. Despite learning of the Data Breach on or about November 19, 2023, Defendants
10 did not begin notifying impacted individuals until early December, 2023. Defendants' failure to
11 promptly notify Plaintiffs and Class members that their PII/PHI was accessed and stolen virtually
12 ensured that the unauthorized third parties who exploited those security lapses could monetize,
13 misuse, or disseminate that PII/PHI before Plaintiffs and Class members could take affirmative
14 steps to protect their sensitive information. As a result, Plaintiffs and Class members will suffer
15 indefinitely from the substantial and concrete risk that their identities will be (or already have been)
16 stolen and misappropriated.

17 39. The Data Breach is not the first data breach that Defendants have experienced in
18

19 _____
20 (Dec. 1, 2023), <https://www.fredhutch.org/en/news/releases/2023/12/notice-of-information-security-incident-involving-fred-hutchinso.html>.

21 ²² E.g., KING 5 Staff, 'DO NOT PAY IT': Fred Hutch Warns of 'Threatening Spam Emails' After
22 *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>.

23 ²³ *Id.*

24 ²⁴ E.g., Brittany Toolis, *Cancer Patients Face Blackmail Threats After Fred Hutch Data Breach*,
25 MYNORTHWEST (Dec. 8, 2023 6:38 AM), <https://mynorthwest.com/3942300/cancer-patients-face-blackmail-threats-after-fred-hutch-data-breach/>.

26 ²⁵ *Id.*

²⁶ See *Data Security Incident*, *supra* note 18.

²⁷ *Id.*

1 recent years. FHCC experienced a separate data incident between March 25, 2022, and March 26,
2 2022, in which an unauthorized person accessed an employee’s email account containing patient
3 information.²⁸ In 2018, it was discovered that the PII/PHI of approximately 974,000 UW Medicine
4 patients was exposed online and available through Google searches.²⁹ The PHI of approximately
5 3,800 UW Medicine patients was affected by a ransomware attack at a third-party vendor of UW
6 Medicine’s in 2022.³⁰

7 ***Defendants Knew that Criminals Target PII/PHI***

8 40. At all relevant times, Defendants knew, or should have known, that Plaintiffs’ and
9 all other Class members’ PII/PHI was a target for malicious actors. Indeed, FHCC admitted in its
10 website notice that “all organizations face cybersecurity risks and these kind of attacks have
11 targeted multiple healthcare institutions in the past.”³¹ Further, Defendants’ Joint Notice of Privacy
12 Practices states that Defendants will “let you know promptly if a breach occurs that may have
13 compromised the privacy or security of your information.”³²

14 41. Despite such knowledge, Defendants failed to implement and maintain reasonable
15 and appropriate data privacy and security measures to protect Plaintiffs’ and Class members’
16 PII/PHI from cyber-attacks that Defendants should have anticipated and guarded against.
17 Defendants should have been particularly aware of the possibility of a data breach because of the
18 recent data breaches they each experienced.

19
20
21 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>.

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

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

26 ³¹ *Data Security Incident*, *supra* note 18.

³² *Joint Notice*, *supra* note 12.

1 42. It is well known amongst companies that store sensitive personally identifying
2 information that sensitive information—such as the Social Security numbers (“SSNs”) and
3 medical information stolen in the Data Breach—is valuable and frequently targeted by criminals.
4 In a recent article, *Business Insider* noted that “[d]ata breaches are on the rise for all kinds of
5 businesses, including retailers Many of them were caused by flaws in . . . systems either
6 online or in stores.”³³

7 43. Cyber criminals seek out PHI at a greater rate than other sources of personal
8 information. In a 2023 report, the healthcare compliance company Protenus found that there were
9 956 medical data breaches in 2022 with over 59 million patient records exposed.³⁴ This is an
10 increase from the 758 medical data breaches which exposed approximately 40 million records that
11 Protenus compiled in 2020.³⁵

12 44. PII/PHI is a valuable property right.³⁶ The value of PII/PHI as a commodity is
13 measurable.³⁷ “Firms are now able to attain significant market valuations by employing business
14 models predicated on the successful use of personal data within the existing legal and regulatory
15 frameworks.”³⁸ American companies are estimated to have spent over \$19 billion on acquiring
16 personal data of consumers in 2018.³⁹ It is so valuable to identity thieves that once PII/PHI has
17

18 ³³ Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies*
19 *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>.

20 ³⁴ See PROTENUS, *2023 Breach Barometer*, PROTENUS.COM, [https://www.protenus.com/breach-](https://www.protenus.com/breach-barometer-report)
[barometer-report](https://www.protenus.com/breach-barometer-report) (last accessed Dec. 11, 2023).

21 ³⁵ See *id.*

22 ³⁶ See Marc van Lieshout, *The Value of Personal Data*, 457 INT’L FED’N FOR INFO. PROCESSING
23 26 (May 2015) (“The value of [personal] information is well understood by marketers who try to
24 collect as much data about personal conducts and preferences as possible...”),
https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.

25 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>.

26 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-](https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en)
[technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en](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/>.

1 been disclosed, criminals often trade it on the “cyber black-market,” or the “dark web,” for many
2 years.

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

8 46. PHI is particularly valuable and has been referred to as a “treasure trove for
9 criminals.”⁴⁰ A cybercriminal who steals a person’s PHI can end up with as many as “seven to ten
10 personal identifying characteristics of an individual.”⁴¹

11 47. All-inclusive health insurance dossiers containing sensitive health insurance
12 information, names, addresses, telephone numbers, email addresses, SSNs, and bank account
13 information, complete with account and routing numbers, can fetch up to \$1,200 to \$1,300 each
14 on the black market.⁴² According to a report released by the Federal Bureau of Investigation’s
15 (“FBI”) Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen
16 Social Security or credit card number.⁴³

17 48. Criminals can use stolen PII/PHI to extort a financial payment by “leveraging
18 details specific to a disease or terminal illness.”⁴⁴ Quoting Carbon Black’s Chief Cybersecurity
19

20 ⁴⁰ See Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAG. (Oct. 20,
21 2019), [https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-](https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon)
22 [perfcon](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.”).

23 ⁴¹ *Id.*

24 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-](https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market)
fetch-high-prices-in-the-online-black-market.

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

⁴⁴ Steager, *supra* note 40.

1 Officer, one recent article explained: “Traditional criminals understand the power of coercion and
2 extortion . . . By having healthcare information—specifically, regarding a sexually transmitted
3 disease or terminal illness—that information can be used to extort or coerce someone to do what
4 you want them to do.”⁴⁵

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

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

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

14 51. Theft of PII/PHI can have serious consequences for the victim. The FTC warns
15 consumers that identity thieves use PII/PHI to receive medical treatment, start new utility accounts,
16 and incur charges and credit in a person’s name.^{47 48}

17 52. Experian, one of the largest credit reporting companies in the world, warns
18 consumers that “[i]dentity thieves can profit off your personal information” by, among other
19

20 ⁴⁵ *Id.*

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

24 ⁴⁷ See Federal Trade Commission, *What to Know About Identity Theft*, FED. TRADE COMM’N
25 CONSUMER INFO., <https://www.consumer.ftc.gov/articles/what-know-about-identity-theft> (last
26 accessed Dec. 11, 2023).

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).

1 things, selling the information, taking over accounts, using accounts without permission, applying
2 for new accounts, obtaining medical procedures, filing a tax return, and applying for government
3 benefits.⁴⁹

4 53. Identity theft is not an easy problem to solve. In a survey, the Identity Theft
5 Resource Center found that most victims of identity crimes need more than a month to resolve
6 issues stemming from identity theft and some need over a year.⁵⁰

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

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

16 56. Theft of PII is even more serious when it includes theft of PHI. Data breaches
17 involving medical information “typically leave[] a trail of falsified information in medical records
18 that can plague victims’ medical and financial lives for years.”⁵² It “is also more difficult to detect,
19

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

24 ⁵⁰ Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RES. CTR.
25 (2021), <https://www.idtheftcenter.org/identity-theft-aftermath-study/> (last accessed Dec. 11,
26 2023).

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-](http://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf)
[content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf](http://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf).

1 taking almost twice as long as normal identity theft.”⁵³ In warning consumers on the dangers of
2 medical identity theft, the FTC states that an identity thief may use PII/PHI “to see a doctor, get
3 prescription drugs, buy medical devices, submit claims with your insurance provider, or get other
4 medical care.”⁵⁴ The FTC also warns, “If the thief’s health information is mixed with yours it
5 could affect the medical care you’re able to get or the health insurance benefits you’re able to
6 use.”⁵⁵

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

- 9
- 10 a. Changes to their health care records, most often the addition of falsified
11 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.
 - 12 b. Significant bills for medical goods and services neither sought nor received.
 - 13 c. Issues with insurance, co-pays, and insurance caps.
 - 14 d. Long-term credit problems based on problems with debt collectors
15 reporting debt due to identity theft.
 - 16 e. Serious life consequences resulting from the crime; for example, victims
17 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
18 to medical activities of the imposter; victims have been denied jobs due to
incorrect information placed in their health files due to the crime.
 - 19 f. As a result of improper and/or fraudulent medical debt reporting, victims
20 may not qualify for mortgage or other loans and may experience other
financial impacts.
 - 21 g. Phantom medical debt collection based on medical billing or other identity
information.
 - 22 h. Sales of medical debt arising from identity theft can perpetuate a victim’s
- 23

24 ⁵³ See Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk . . .*,
supra note 43.

25 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
26 Dec. 11, 2023).

⁵⁵ *Id.*

1 debt collection and credit problems, through no fault of their own.⁵⁶

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

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

10 ***Damages Sustained by Plaintiffs and Class Members***

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

20 **CLASS ALLEGATIONS**

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

23
24
25 ⁵⁶ See Dixon & Emerson, *supra* note 52.

26 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>.

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

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

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

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

14 65. The members in the Class are so numerous that joinder of all Class members in a
15 single proceeding would be impracticable. The cybercriminals that perpetrated the Data Breach
16 have stated that 800,000 persons' PII/PHI was affected in the Data Breach.⁵⁸

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

- 20 a. Whether Defendants had a duty to implement and maintain
21 reasonable security procedures and practices to protect and secure
22 Plaintiffs' and Class members' PII/PHI from unauthorized access
23 and disclosure;
- 24 b. Whether Defendants had duties not to disclose the PII/PHI of
25 Plaintiffs and Class members to unauthorized third parties;
- 26 c. Whether Defendants 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
Defendants, providing that Defendants would implement and

⁵⁸ See Toolis, *supra* note 24.

1 maintain reasonable security measures to protect and secure Class
2 members' PII/PHI from unauthorized access and disclosure;

- 3 e. Whether Defendants engaged in unfair, unlawful, or deceptive
4 practices by failing to safeguard the PII/PHI of Plaintiffs and Class
5 members;
- 6 f. Whether Defendants breached its duties to protect Plaintiffs' and
7 Class members' PII/PHI; and
- 8 g. Whether Defendants and Class members are entitled to damages and
9 the measure of such damages and relief.

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

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

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

24 70. A class action is superior to any other available means for the fair and efficient
25 adjudication of this controversy, and no unusual difficulties are likely to be encountered in the
26 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 Defendants, so it would be impracticable

1 for Class members to individually seek redress from Defendants' wrongful conduct. Even if Class
2 members could afford individual litigation, the court system could not. Individualized litigation
3 creates a potential for inconsistent or contradictory judgments, and increases the delay and expense
4 to all parties and the court system. By contrast, the class action device presents far fewer
5 management difficulties and provides the benefits of single adjudication, economy of scale, and
6 comprehensive supervision by a single court.

7 **CAUSES OF ACTION**

8 **COUNT I**
9 **NEGLIGENCE**
10 **(Against FHCC)**

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

13 72. Plaintiffs bring this claim only against FHCC.

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

16 74. FHCC knew the risks of collecting and storing Plaintiffs' and all other Class
17 members' PII/PHI and the importance of maintaining secure systems. FHCC knew of the many
18 data breaches that targeted healthcare providers in recent years and experienced a recent data
19 breach itself.

20 75. Given the nature of FHCC's business, the sensitivity and value of the PII/PHI it
21 maintains, and the resources at its disposal, FHCC should have identified the vulnerabilities to
22 their systems and prevented the Data Breach from occurring.

23 76. FHCC breached these duties by failing to exercise reasonable care in safeguarding
24 and protecting Plaintiffs' and Class members' PII/PHI by failing to design, adopt, implement,
25 control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls,
26

1 policies, procedures, protocols, and software and hardware systems to safeguard and protect
2 PII/PHI entrusted to it—including Plaintiffs’ and Class members’ PII/PHI.

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

9 78. But for FHCC’s negligent conduct or breach of the above-described duties owed to
10 Plaintiffs and Class members, their PII/PHI would not have been compromised.

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

22 **COUNT II**
23 **NEGLIGENCE PER SE**
24 **(Against FHCC)**

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

1 81. Plaintiffs bring this claim only against FHCC.

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

7 83. FHCC's duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. §
8 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted
9 by the FTC, the unfair act or practice by business, such as FHCC, of failing to employ reasonable
10 measures to protect and secure PII/PHI.

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

17 85. FHCC's violations of HIPAA Privacy and Security Rules and Section 5 of the
18 FTCA constitutes negligence per se.

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

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

23 88. It was reasonably foreseeable to FHCC that its failure to exercise reasonable care
24 in safeguarding and protecting Plaintiffs' and Class members' PII/PHI by failing to design, adopt,
25 implement, control, direct, oversee, manage, monitor, and audit appropriate data security
26

1 processes, controls, policies, procedures, protocols, and software and hardware systems, would
2 result in the release, disclosure, and dissemination of Plaintiffs' and Class members' PII/PHI to
3 unauthorized individuals.

4 89. The injury and harm that Plaintiffs and the other Class members suffered was the
5 direct and proximate result of FHCC's violations of HIPAA Privacy and Security Rules and
6 Section 5 of the FTCA. Plaintiffs and Class members have suffered (and will continue to suffer)
7 economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantial
8 increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their
9 PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from
10 unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to
11 mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their
12 PII/PHI which remains in FHCC's possession; (vi) future costs in terms of time, effort, and money
13 that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a
14 result of the Data Breach; and (vii) overpayment for the services that were received without
15 adequate data security.

16
17 **COUNT III**
BREACH OF FIDUCIARY DUTY
(Against FHCC)

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

20 91. Plaintiffs bring this claim only against FHCC.

21 92. Plaintiffs and Class members gave FHCC their PII/PHI in confidence, or gave it to
22 another entity in confidence which then gave their PII/PHI to FHCC such that FHCC was entrusted
23 with the PII/PHI, believing that FHCC or the other entity would protect that information. Plaintiffs
24 and Class members would not have provided FHCC with this information, or would not have
25 allowed FHCC to obtain this information, had they known it would not be adequately protected.
26

1 FHCC's acceptance and storage of Plaintiffs' and Class members' PII/PHI created a fiduciary
2 relationship between FHCC and Plaintiffs and Class members. In light of this relationship, FHCC
3 must act primarily for the benefit of the persons it collects the PII/PHI of, which includes
4 safeguarding and protecting Plaintiffs' and Class members' PII/PHI.

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

10 94. As a direct and proximate result of FHCC's breaches of its fiduciary duties,
11 Plaintiffs and Class members have suffered and will suffer injury, including, but not limited to: (i)
12 a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft
13 of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and
14 recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort
15 attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued
16 risk to their PII/PHI which remains in FHCC's possession; (vi) future costs in terms of time, effort,
17 and money that will be required to prevent, detect, and repair the impact of the PII/PHI
18 compromised as a result of the Data Breach; and (vii) overpayment for the services that were
19 received without adequate data security.

20
21 **COUNT IV**
BREACH OF IMPLIED CONTRACT
(Against FHCC and UW)

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

24 96. Plaintiffs bring this claim against both FHCC and UW.
25
26

1 97. In connection with receiving services from Defendants, performing services for
2 Defendants, or otherwise transacting with Defendants, Plaintiffs and all other Class members
3 entered into implied contracts with Defendants.

4 98. Pursuant to these implied contracts, Plaintiffs and Class members provided
5 Defendants with their PII/PHI. In exchange, Defendants agreed to, among other things, and
6 Plaintiffs understood that Defendants would, take reasonable measures to protect the security and
7 confidentiality of Plaintiffs' and Class members' PII/PHI, and protect Plaintiffs' and Class
8 members PII/PHI in compliance with federal and state laws and regulations and industry standards.

9 99. The protection of PII/PHI was a material term of the implied contracts between
10 Plaintiffs and Class members, on the one hand, and Defendants, on the other hand. Had Plaintiffs
11 and Class members known that Defendants would not adequately protect its current and former
12 patients' and others' PII/PHI, they would not have provided this information to Defendants.

13 100. Plaintiffs and Class members performed their obligations under the implied
14 contract when they provided Defendants with their PII/PHI and paid—directly or through their
15 insurers—for services from Defendants or performed services for Defendants.

16 101. Defendants breached their obligations under their implied contracts with Plaintiffs
17 and Class members in failing to implement and maintain reasonable security measures to protect
18 and secure their PII/PHI and in failing to implement and maintain security protocols and
19 procedures to protect Plaintiffs' and Class members' PII/PHI in a manner that complies with
20 applicable laws, regulations, and industry standards.

21 102. Defendants' breach of its obligations of its implied contracts with Plaintiffs and
22 Class members directly resulted in the Data Breach and the injuries that Plaintiffs and all other
23 Class members have suffered from the Data Breach.

24 103. Plaintiffs and all other Class members were damaged by Defendants' breach of
25 implied contracts because: (i) they paid—directly or through their insurers—for data security
26

1 protection they did not receive; (ii) they face a substantially increased risk of identity theft and
2 medical theft—risks justifying expenditures for protective and remedial services for which they
3 are entitled to compensation; (iii) their PII/PHI was improperly disclosed to unauthorized
4 individuals; (iv) the confidentiality of their PII/PHI has been breached; (v) they were deprived of
5 the value of their PII/PHI, for which there is a well-established national and international market;
6 (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach,
7 including the increased risks of identity theft they face and will continue to face; and (vii)
8 overpayment for services that were received without adequate data security.

9
10 **COUNT V**
UNJUST ENRICHMENT
(Against FHCC and UW)

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

13 105. Plaintiffs bring this claim against both FHCC and UW.

14 106. This claim is pleaded in the alternative to the breach of implied contract claim.

15 107. Plaintiffs and Class members conferred a monetary benefit upon Defendants in the
16 form of monies paid for healthcare services or other services, conferred a benefit upon Defendants
17 through performance of services, or conferred a benefit upon Defendants through other
18 transactions.

19 108. Defendants accepted or had knowledge of the benefits conferred upon it by
20 Plaintiffs and Class members. Defendants also benefitted from the receipt of Plaintiffs' and Class
21 members' PII/PHI.

22 109. As a result of Defendants' conduct, Plaintiffs and Class members suffered actual
23 damages in an amount equal to the difference in value between their payments made, or services
24 performed, with reasonable data privacy and security practices and procedures that Plaintiffs and
25

1 Class members paid for, or were paid less for their services for, and those payments without
2 reasonable data privacy and security practices and procedures that they received.

3 110. Defendants should not be permitted to retain the money belonging to Plaintiffs and
4 Class members because Defendants failed to adequately implement the data privacy and security
5 procedures for itself that Plaintiffs and Class members paid for and that were otherwise mandated
6 by federal, state, and local laws and industry standards.

7 111. Defendants should be compelled to provide for the benefit of Plaintiffs and Class
8 members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged
9 herein.

10
11 **COUNT VI**
12 **VIOLATION OF THE WASHINGTON CONSUMER PROTECTION ACT**
13 **RCW §§ 19.86.010 et seq. (“WCPA”)**
14 **(Against FHCC)**

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

17 113. Plaintiffs bring this claim only against FHCC.

18 114. Plaintiffs and FHCC are “persons” under the WCPA. RCW § 19.86.010(1).

19 115. FHCC’s sale of services to Plaintiffs and all other Class members constitutes as
20 “trade” and “commerce” under the WCPA. RCW § 19.86.010(2).

21 116. The WCPA states, “Unfair methods of competition and unfair or deceptive
22 practices in the conduct of any trade or commerce are hereby declared unlawful.” RCW §
23 19.86.020. FHCC’s failure to adequately safeguard Plaintiffs and Class members PII/PHI while
24 representing that their PII/PHI would be protected is an “unfair or deceptive practice” under the
25 WCPA.

26 117. FHCC’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 FHCC’s actions not
only harmed Plaintiffs, but harmed hundreds of thousands of other persons.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26

JURY TRIAL DEMANDED

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

Dated: December 11, 2023

Respectfully submitted,

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

BEN BARNOW*
b.barnow@barnowlaw.com
ANTHONY L. PARKHILL*
aparkhill@barnowlaw.com
RILEY W. PRINCE*
rprince@barnowlaw.com
BARNOW AND ASSOCIATES, P.C.
205 West Randolph Street, Ste. 1630
Chicago, IL 60606
Tel: 312.621.2000
Fax: 312.641.5504

**pro hac vice to be submitted*