SUPERIOR COURT OF THE STATE OF WASHINGTON
FOR KING COUNTY

ALEXANDER IRVINE and BARBARA TWADDEL, individually and on behalf of all others similarly situated, Plaintiffs, v. UNIVERSITY OF WASHINGTON, Defendant.	No. 24-2-03365-3 SEA NOTICE OF REMOVAL TO SUPERIOR COURT CLERK

TO: The Clerk of the Superior Court of the State of Washington for King County

NOTICE IS HEREBY GIVEN, pursuant to 28 U.S.C. § 1446(d), that on March 4, 2024, defendant University of Washington ("UW") filed in the United States District Court for the Western District of Washington, a Notice of Removal of the above entitled action. A copy of the Notice of Removal is attached hereto.

YOU ARE ALSO ADVISED that contemporaneous with the filing of the attached copy of the Notice of Removal, the Superior Court of Washington for King County ceased

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

to have jurisdiction over this action and may proceed no further unless and until the case is remanded.

Dated: March 4, 2024

s/ Erin K. Earl
David B. Robbins, Bar No. 13628
DRobbins@perkinscoie.com
Susan D. Fahringer, Bar No. 21567
SFahringer@perkinscoie.com
Todd M. Hinnen, Bar No. 27176
THinnen@perkinscoie.com
Matthew P. Gordon, Bar No. 41128
MGordon@perkinscoie.com
Erin K. Earl, Bar No. 49341
EEarl@perkinscoie.com
Ellie F. Chapman, Bar No. 55881
EChapman@perkinscoie.com

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Telephone: 206.359.8000
Facsimile: 206.359.9000

Counsel for Defendant University of Washington

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

ALEXANDER IRVINE and BARBARA TWADDEL, individually and on behalf of all others similarly situated, Plaintiffs, v. UNIVERSITY OF WASHINGTON, an agency of the STATE OF WASHINGTON, Defendant.	No. 2:24-cv-296 NOTICE OF REMOVAL

In December 2023, Alexander Irvine and Barbara Twaddell (the "*Irvine* plaintiffs") filed a complaint in King County Superior Court against the Fred Hutchinson Cancer Center ("Fred Hutch") and the University of Washington ("UW") asserting claims based on a data security incident Fred Hutch suffered ("*Irvine I*"). After their claims were removed to this Court and other lawyers were appointed to lead the class, the *Irvine* plaintiffs vigorously contested the leadership order and this Court's jurisdiction. In the midst of remand briefing, the *Irvine* plaintiffs filed a second complaint in state court making the exact same allegations, but against UW only ("*Irvine II*"). The *Irvine* plaintiffs then cited the new state-court complaint to this Court as a reason the Court should remand their pending claims. UW is now removing *Irvine II* pursuant to 28 U.S.C. § 1453(b) so that all of the *Irvine* plaintiffs' claims can proceed together. Although the basis for removal may not be immediately apparent on the face of the *Irvine II* complaint because it names

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

UW (a state governmental entity) as the only defendant, courts look beyond the face of the complaint when assessing jurisdiction under the Class Action Fairness Act ("CAFA"), particularly when, as here, doing so is necessary to thwart a tactical ploy to attempt to avoid federal court. If the Court denies the *Irvine* plaintiffs' pending motion to remand, these additional claims should proceed here. If the Court grants their pending motion to remand, these claims should also be remanded.

I. Background

1. The *Irvine* plaintiffs allege that sometime on or before November 19, 2023, a foreign group of "cybercriminals" breached Fred Hutch's network and "gained access" to information about Fred Hutch and UW patients. *See* Ex. A ¶¶ 3, 37–39 ("*Irvine II* Compl."). They do not allege that UW's network was breached, and FHCC's press release, which they cite, states that "there is no evidence that the UW-based system was impacted."[1] *Id.* ¶ 37.

2. The first two class action complaints related to the incident were filed by other plaintiffs and their attorneys on December 8, 2023 (in King County Superior Court) and on December 10, 2023 (in this Court). *See* Complaint at 1, *Arneson v. Fred Hutchinson Cancer Research Center*, No. 2:24-cv-00033 (W.D. Wash. Jan. 8, 2024), Dkt. 1-2; Complaint at 1, *Doe v. Fred Hutchinson Cancer Center*, No. 2:23-cv-01893 (W.D. Wash. Dec. 10, 2023), Dkt. 1.

3. The *Irvine* plaintiffs filed the third class action complaint, *Irvine I*, on December 11, 2023 in King County Superior Court. *See* Complaint, *Irvine v. Fred Hutchinson Cancer Center,* No. 2:24-cv-00030 (W.D. Wash. Jan. 8, 2024), Dkt. 1-2 ("*Irvine I* Compl.").

4. Other class action complaints were filed in or removed to this Court thereafter, and several attorneys representing plaintiffs with cases pending in this Court moved to consolidate the cases and to appoint a Plaintiffs' Steering Committee to lead the litigation. *See* Unopposed Joint Motion to Consolidate Related Cases & Unopposed Joint Motion to Appoint Interim Class

[1] https://www.fredhutch.org/en/about/about-the-hutch/accountability-impact/notice-to-our-patients-of-data-security-incident.html (last visited March 4, 2024).

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

Counsel, *Doe v. Fred Hutchinson Cancer Center*, No. 2:23-cv-01893 (W.D. Wash. Dec. 29, 2023), Dkts. 5, 6.

5. The Court granted both motions and ordered any additional cases arising out of "the same or similar operative facts" consolidated and subject to the authority of the Plaintiffs' Steering Committee. *See* Order Granting Joint Motion to Consolidate Related Cases & Order Granting Joint Motion to Appoint Interim Class Counsel, *Doe v. Fred Hutchinson Cancer Center*, No. 2:23-cv-01893 (W.D. Wash. Jan. 5, 2024), Dkts. 9, 10.

6. On January 8, 2024, Fred Hutch removed *Irvine I* to this Court. *See* Notice of Removal, *Irvine v. Fred Hutchinson Cancer Center,* No. 2:24-cv-00030 (W.D. Wash. Jan. 8, 2024), Dkt. 1. In accordance with the Court's order, *Irvine I* was consolidated with the other cases.

7. The *Irvine* plaintiffs' first act in federal court was to move to vacate the order appointing the Plaintiffs' Steering Committee, which did not include their attorneys. *See* Plaintiffs Alexander Irvine and Barbara Twaddell's Motion to Vacate Order, *In re Fred Hutchinson Cancer Center Data Security Litig.*, No. 2:23-cv-01893 (W.D. Wash. Jan. 12, 2024), Dkt. 13. About two weeks later, they moved to remand their individual case and argued in a footnote that the Court should dismiss or remand every other plaintiff's claims too. *See* Plaintiffs Alexander Irvine and Barbara Twaddell's Motion to Remand at 1 n.1, *In re Fred Hutchinson Cancer Center Data Security Litig.*, No. 2:23-cv-01893 (W.D. Wash. Jan. 24, 2024), Dkt. 36.

8. At a status conference on January 25, 2024, the Court asked whether any counsel was aware of any other case that would be filed. All counsel, including the *Irvine* plaintiffs' counsel, responded that they were not.

9. Fred Hutch, the Plaintiffs' Steering Committee, and UW responded to the *Irvine* plaintiffs' motion to remand *Irvine I* on February 12, 2024. In its response, UW agreed to proceed in this Court and expressly waived Eleventh Amendment immunity "for claims arising out of the instant cyberattack against Fred Hutch to the same extent its sovereign immunity is waived in state court." UW's Response to Motion to Remand at 2, *In re Fred Hutchinson Cancer Center Data*

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

Security Litig., No. 2:23-cv-01893 (W.D. Wash. Feb. 12, 2024), Dkt. 47; *see also Coll. Sav. Bank v. Fla. Prepaid Postsecondary Educ. Expense Bd.*, 527 U.S. 666, 675–76 (1999) ("[W]e will find a waiver either if the State voluntarily invokes our jurisdiction, or else if the State makes a clear declaration that it intends to submit itself to our jurisdiction.") (internal quotation marks and citations omitted); *Does v. Univ. of Washington*, No. C16-1212JLR, 2016 WL 5792693, at *5 (W.D. Wash. Oct. 4, 2016) (holding that "the Assistant Attorney General conducting this litigation on behalf of UW has the authority to waive the State's sovereign immunity with respect to this suit").

10. That same day, contrary to their representation at the status conference, the *Irvine* plaintiffs filed a second complaint in King County Superior Court on behalf of the same class ("*Irvine II*"). *See* Ex. A. The named plaintiffs, factual allegations, class definition, class action allegations, and relief requested are all the same as in *Irvine I*. And the causes of action are identical to claims they had already asserted. The only material difference between the two complaints is that in *Irvine II* the plaintiffs assert claims against UW only and omit the two claims they had already asserted against UW in *Irvine I*.

11. In *Irvine I*, the plaintiffs asserted six claims against Fred Hutch: (1) negligence, (2) negligence *per se*, (3) breach of fiduciary duty, (4) breach of implied contract, (5) unjust enrichment, and (6) a violation of the Washington Consumer Protection Act. *See Irvine I* Compl. ¶¶ 71–119. But they asserted only their implied contract and unjust enrichment claims against UW. *See id.* In *Irvine II*, the plaintiffs brought the negligence, negligence *per se*, breach of fiduciary duty, and Washington Consumer Protection Act claims against UW. *See* Ex. A ¶¶ 76–103.

12. A comparison of the *Irvine* plaintiffs' complaints is attached as an exhibit to the Declaration of Erin K. Earl in support of this Notice of Removal. *See* Earl Decl., Ex. 1.

13. *The Irvine* plaintiffs have not explained why they represented to the Court and the parties at the January 25, 2024 status conference that they were unaware of additional cases that would be filed. Their silence is particularly notable given that they now allege they "submitted a

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

tort claim form regarding the Data Breach to the Office of Risk Management on December 12, 2023," more than a month before the status conference. Ex. A ¶ 15. And the *Irvine* plaintiffs have offered no persuasive explanation for why they sought to add these identical claims against UW by filing an entirely new complaint in a different court rather than seeking leave to amend *Irvine I* or amending as of right at an appropriate time. *See* Fed. R. Civ. P. 15(a).

14. But the *Irvine* plaintiffs cited the new complaint as a reason the Court should remand a few days later, suggesting that *Irvine II* is merely a tactical ploy to bolster otherwise weak support for their position that the Court should remand the pending cases. *See Irvine* Plaintiffs' Reply in Support of Motion to Remand at 4, *In re Fred Hutchinson Cancer Center Data Security Litig.*, No. 2:23-cv-01893 (W.D. Wash. Feb. 16, 2024), Dkt. 50.

II. The Court has original jurisdiction over these claims under CAFA

15. The Court has original jurisdiction under CAFA if (1) the case is a class action, (2) the parties are minimally diverse, (3) at least one primary defendant is not a state governmental entity, (4) the proposed classes include at least 100 members, and (5) the amount in controversy aggregated across all members of the proposed classes exceeds $5 million. 28 U.S.C. § 1332(d)(2), (5).

A. The claims are part of a class action.

16. CAFA defines a "class action" as "any civil action filed under rule 23 of the Federal Rules of Civil Procedure or similar State statute or rule of judicial procedure authorizing an action to be brought by 1 or more representative persons as a class action." 28 U.S.C. § 1332(d)(1)(B).

17. In each complaint, the *Irvine* plaintiffs ask to represent a class of individuals under Washington Superior Court Civil Rule 23. *See Irvine I* Compl. ¶ 61; Ex. A ¶ 66. Therefore, the *Irvine* plaintiffs' claims are part of a "class action."

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

B. The Court may look beyond the face of the complaint when assessing jurisdiction, and should do so here to prevent gamesmanship meant to avoid federal jurisdiction under CAFA.

18. "CAFA's primary objective" is to "ensur[e] 'Federal court consideration of interstate cases of national importance.'" *Standard Fire Ins. v. Knowles*, 568 U.S. 588, 595 (2013) (citation omitted). Thus, "CAFA's 'provisions should be read broadly, with a strong preference that interstate class actions should be heard in federal court.'" *Dart Cherokee Basin Operating Co., LLC v. Owens*, 574 U.S. 81, 89 (2014) (citation omitted).

19. In furtherance of Congress's objectives, courts have consistently rejected efforts to evade federal jurisdiction under CAFA. *See, e.g., Standard Fire Ins.*, 568 U.S. at 596 (2013) (holding that a named plaintiff's stipulation to seek less than $5 million on behalf of the class does not divest a federal court of CAFA jurisdiction); *Broadway Grill, Inc. v. Visa Inc.*, 856 F.3d 1274, 1279 (9th Cir. 2017) (holding that after a case is removed under CAFA plaintiffs may not "amend their class definition, add or remove defendants, or add or remove claims in such a way that would alter the essential jurisdictional analysis").

20. Thus, when plaintiffs attempt to use artful pleading to avoid CAFA, courts may "look beyond the complaint to determine whether the putative class action meets the jurisdictional requirements." *Rodriguez v. AT&T Mobility Servs. LLC*, 728 F.3d 975, 981 (9th Cir. 2013).

21. In particular, several courts have held that when a plaintiff attempts to divide a single class action across multiple lawsuits in an effort to evade CAFA, the court may look beyond the four corners of a particular complaint and treat the separate suits as a single class action. *See Freeman v. Blue Ridge Paper Prods., Inc.*, 551 F.3d 405 (6th Cir. 2008) (reversing district court's remand of five cases among which plaintiffs divided their claims in an attempt to keep the amount in controversy below $5 million in each); *Sanders v. Kia Am. Inc.*, No. 8:23-cv-00486-JVS(KESx), 2023 WL 3974966 (C.D. Cal. June 13, 2023) (considering parties in already pending federal class action along with parties in later-filed state court action in holding that minimal diversity and amount in controversy requirements were satisfied); *Simon v. Marriott Int'l*, No. PWG-19-2879,

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

2019 WL 4573415 (D. Md. Sept. 20, 2019) (holding that data breach claims brought in state court by plaintiffs who were already part of pending federal class action were properly considered part of a single class action); *Proffitt v. Abbott Labs*, No. 2:08-cv-151, 2008 WL 4401367, at *5 (E.D. Tenn. Sept. 23, 2008) (holding that court had jurisdiction over 11 cases among which plaintiffs divided their claims in an attempt to evade CAFA's amount in controversy threshold); *see also Vodenichar v. Halcón Energy Props., Inc.*, 733 F.3d 497, 508–10 (3d Cir. 2013) (holding that when the "same representative plaintiffs filed two complaints on behalf of an identically-defined putative class arising from the same factual allegations . . . Plaintiffs' actions were no different than a situation where a party amends a pleading" so both complaints were part of the same class action).[2]

22. That is what happened here. Filing this new complaint, rather than amending *Irvine I*, is the *Irvine* plaintiffs' latest effort to sidestep this Court. Their divvying up of claims and parties to multiply the proceedings is precisely what CAFA was meant to avoid, and is plain gamesmanship intended to evade or influence this Court's ruling on their pending motion to remand. The Court should look beyond the four corners of the *Irvine II* complaint and see it for what it is: a continuation of the same class action that is already pending in this Court.

C. CAFA's minimal diversity requirement is satisfied.

23. Both Fred Hutch and UW are parties to that single class action (spanning both complaints).

24. Fred Hutch is a nonprofit corporation with its principal place of business in Washington. It is therefore a citizen of Washington. 28 U.S.C. § 1332(c)(1).

[2] The Ninth Circuit has held that somewhat different considerations apply in the *mass* action context, where there are no "competing claims to represent the same class of plaintiffs," the "concerns that overlapping or identical claims would be litigated in multiple jurisdictions" are not present, and CAFA's "fairly narrow" mass-action provision expressly precludes defendants from consolidating multiple smaller actions into a single "mass action eligible for removal under CAFA." *Tanoh v. Dow Chem. Co.*, 561 F.3d 945, 953–54 (9th Cir. 2009). In that context—when plaintiffs "expressly elect[] not to proceed as a class"—Congress's concerns about "abusing the class action device" that animate CAFA simply "do not apply." *Id.* at 954.

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

25. The *Irvine* plaintiffs seek to represent a class of "[a]ll United States citizens whose personally identifiable information or personal health information was accessed in the Data Breach and disclosed to unauthorized persons, including United States residents who were sent a notice of the Data Breach." *See* Ex. A ¶ 67.

26. Fred Hutch is one of the premier cancer centers in the United States, and one of only two National Cancer Institute-Designated cancer centers in the Northwest.[3] Citizens of states other than Washington (*i.e.*, individuals who reside in those states and intend to stay there) routinely travel to Fred Hutch to seek care. In fact, Fred Hutch even offers housing where out-of-state patients can live during treatment.[4] Upon information and belief, at least one of these out-of-state patients' information was accessed in the data breach and is a member of the class.[5]

27. In addition, Fred Hutch's Director of Enterprise Analytics has represented that some of the information involved in the breach related to individuals who are not patients of UW or Fred Hutch but who were patients of institutions located in states other than Washington that forwarded laboratory specimens to Fred Hutch. *See* Declaration of Britni Bethune ¶ 7, *In re Fred Hutchinson Cancer Center Data Security Litig.*, No. 2:23-cv-01893 (W.D. Wash. Feb. 12, 2024), Dkt. 46-1. At least one of these individuals is likely domiciled in a state other than Washington because individuals generally seek medical laboratory testing at facilities near where they live and intend to remain. *See* 28 U.S.C. § 1332(d)(2)(A).

28. Therefore, CAFA's minimal diversity requirement is satisfied.

[3] https://www.cancer.gov/research/infrastructure/cancer-centers/find

[4] https://www.fredhutch.org/en/patient-care/patient-services/housing/south-lake-union-house.html

[5] In addition, Fred Hutch sent at least tens of thousands of notification letters to out-of-state addresses. *See* Declaration of Anthony Parkhill ¶ 4 & Ex. 1, *In re Fred Hutchinson Cancer Center Data Security Litig.*, No. 2:23-cv-01893 (W.D. Wash. Jan. 24, 2024). A patient's address is insufficient to establish citizenship, and the Ninth Circuit has thus far declined to adopt a presumption that an address is prima facie evidence of citizenship, but it is some evidence of citizenship.

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

D. Fred Hutch is a primary defendant and is not a state governmental entity.

29. CAFA jurisdiction is not available for "any class action in which . . . the primary defendants are States, State officials, or other governmental entities against whom the district court may be foreclosed from ordering relief." 28 U.S.C. § 1332(d)(5)(A).

30. "[B]y using the word 'the' before the words 'primary defendants' rather than the word 'a,'" Congress provided that CAFA's state governmental entity exemption applies "only if *all* primary defendants" are state governmental entities. *Singh v. Am. Honda Fin. Corp.*, 925 F.3d 1053, 1068 (9th Cir. 2019) (quoting *Vodenichar v. Halcon Energy Props., Inc.*, 733 F.3d 497, 506 (3d Cir. 2013) (emphasis added)).[6]

31. A primary defendant "is a 'principal, fundamental, or direct' defendant." *Singh*, 925 F.3d at 1068 (citation omitted). In evaluating a defendant's status, the Court should "consider whether the defendant is sued directly or alleged to be directly responsible for the harm to the proposed class or classes, as opposed to being vicariously or secondarily liable," and should compare "the defendant's potential exposure to the class relative to the exposure of other defendants." *Id.* These considerations are not exhaustive, and the Court's analysis should be practical. *Id.* at 1068.

32. Fred Hutch is the primary defendant because the *Irvine* plaintiffs allege that they obtained "healthcare or related services from [Fred Hutch]," they have a direct relationship with Fred Hutch, the foreign group of cybercriminals allegedly accessed the information they provided to Fred Hutch, and the exfiltrated information was stored on Fred Hutch's systems. *See* Ex. A ¶¶ 9, 17, 37–39.

33. The *Irvine* plaintiffs do not allege that they were UW patients, nor do they allege any wrongdoing by UW. In fact, the *only* connection between the cyberattack on Fred Hutch's

[6] The language the Ninth Circuit interpreted in *Singh* comes from another CAFA provision (28 U.S.C. § 1332(d)(4)(B)), which is adjacent to the state governmental entity exemption, 28 U.S.C. § 1332(d)(5)(A). But "identical words and phrases within the same statute should normally be given the same meaning," and that principle "is doubly appropriate" here because the provisions were enacted "at the same time." *Powerex Corp. v. Reliant Energy Servs., Inc.*, 551 U.S. 224, 232 (2007).

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

network and UW as alleged in the complaint is that UW shared with Fred Hutch certain "patient data necessary to provide . . . care," and the cybercriminals may have accessed some of that information from Fred Hutch's systems. Ex. A ¶ 38. But the *Irvine* plaintiffs do not allege that any of this data was *the Irvine Plaintiffs'* data. In fact, the only connection between either *Irvine* plaintiff and UW alleged in the complaint is that UW Medicine sent plaintiff Irvine an email about the incident. *See id.* ¶ 13.

34. These allegations demonstrate that UW is, at most, a secondary defendant. Although the *Irvine* plaintiffs' theory of liability for UW is not clear, because the data was in Fred Hutch's possession and the cyberattack was on Fred Hutch's system, any potential liability for UW depends on a threshold finding that Fred Hutch is somehow at fault for the cyberattack's exfiltration of data and is thus liable. If Fred Hutch is determined to have employed adequate measures to protect data in its possession and to simply have been the victim of a crime, no claim could lie against UW. This confirms that UW is a secondary defendant. *See Singh*, 925 F.3d at 1069 (holding that a defendant whose liability depended on a "threshold finding" that other defendants "acted unlawfully" was a secondary defendant).

35. Because Fred Hutch is a primary defendant, the Court would have jurisdiction even if UW were also a primary defendant, which for the reasons stated above it is not. *See Singh*, 925 F.3d at 1068.

E. The proposed classes include at least 100 members.

36. To have jurisdiction under CAFA, the Court must ensure that "the number of members of all proposed plaintiff classes in the aggregate is not less than 100." 28 U.S.C. § 1332(d)(5)(B).

37. The *Irvine* plaintiffs seek to represent a class of "[a]ll United States citizens whose personally identifiable information or personal health information was accessed in the Data Breach and disclosed to unauthorized persons, including United States residents who were sent a notice of the Data Breach." *See* Ex. A ¶ 67.

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

38. The *Irvine* plaintiffs allege that at least 800,000 individuals were affected. *Id.* ¶ 70. In addition, a Cyber Notification and Data Management consultant hired by Fred Hutch has represented that the number of potential class members is likely even higher. *See* Declaration of Bradley J. Bartram ¶ 7, *In re Fred Hutchinson Cancer Center Data Security Litig.*, No. 2:23-cv-01893 (W.D. Wash. Feb. 12, 2024), Dkt. 46-2.

39. This means that the proposed class includes well in excess of 100 members.

F. CAFA's amount in controversy requirement is satisfied.

40. Under CAFA, the Court has jurisdiction over any class action "in which the matter in controversy exceeds the sum or value of $5,000,000." 28 U.S.C. § 1332(d)(2). In making this determination under CAFA, the Court must aggregate the claims of every person who falls within the *Irvine* plaintiffs' proposed class definition. 28 U.S.C. § 1332(d)(6), (d)(1)(D).

41. The *Irvine* plaintiffs seek the following relief: "monetary relief, including actual damages, statutory damages, punitive damages, restitution, disgorgement, and nominal damages" in addition to injunctive relief, including "implementing best data security practices to safeguard PII/PHI and to provide or extend credit monitoring services." Ex. A at 24, ¶¶ B–C.

42. Three companies offering identity protection services—Equifax, LifeLock, and Experian—advertise credit-monitoring services ranging in price from $4.95 to $24.99 per month.[7] The cost of providing only two months of credit-monitoring services to 800,000 people (the minimum alleged to be part of the class) at the lowest advertised rate ($4.95 per month) is $7.92 million. Based on the *Irvine* plaintiffs' allegations and settlements in similar data breach litigation, it is likely that at least two months of credit-monitoring services is at stake here.

43. The *Irvine* plaintiffs' other categories of damages and any attorneys' fees would increase the amount in controversy further.

[7] Equifax ($4.95/month), available at https://www.equifax.com/personal/products/value-product-comparison/, last visited Feb. 28, 2024; Norton LifeLock ($11.99/month), available at https://lifelock.norton.com/#planschart, last visited Feb. 28, 2024; Experian ($24.99/month), available at https://www.experian.com/protection/creditlock/, last visited Feb. 28, 2024.

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

44. UW denies liability and disputes that the *Irvine* plaintiffs are entitled to any of these remedies, but in evaluating the amount in controversy, UW must assume that the allegations in the complaint are true. *See Jauregui v. Roadrunner Transp. Servs., Inc.*, 28 F.4th 989, 993 (9th Cir. 2022) (recognizing that "the defendant is being asked to use the plaintiff's complaint—much of which it presumably disagrees with—to estimate the amount in controversy").

III. Removal is otherwise proper

45. Removal is timely. Plaintiffs filed *Irvine II* and served UW with the summons and complaint on February 12, 2024. UW is removing on March 4, 2024, which is 21 days after the complaint was served. *See* 28 U.S.C. § 1446(b)(1) (defendant may remove within 30 days after service); *Murphy Bros, Inc. v. Michetti Pipe Stringing, Inc.*, 526 U.S. 344, 347–48 (1999) (holding that removal clock starts upon formal service of the summons and complaint).

46. This Court is in the judicial district and division in which *Irvine II* was pending. 28 U.S.C. § 1446(a).

47. UW will notify the *Irvine* plaintiffs and the King County Superior Court in writing of this removal promptly after filing. 28 U.S.C. § 1446(d).

IV. Conclusion

48. This Court has jurisdiction and removal is proper under 28 U.S.C. § 1453(b).

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

Dated: March 4, 2024

By: s/ *Erin K. Earl*
s/ *David B. Robbins*
s/ *Susan D. Fahringer*
s/ *Todd M. Hinnen*
s/ *Matthew P. Gordon*
s/ *Ellie Chapman*

David B. Robbins, Bar No. 13628
Susan D. Fahringer, Bar No. 21567
Todd M. Hinnen, Bar No. 27176
Matthew P. Gordon, Bar No. 41128
Erin K. Earl, Bar No. 49341
Ellie Chapman, Bar No. 55881
Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Telephone: +1.206.359.8000
Facsimile: +1.206.359.9000
DRobbins@perkinscoie.com
SFahringer@perkinscoie.com
THinnen@perkinscoie.com
MGordon@perkinscoie.com
EEarl@perkinscoie.com
EChapman@perkinscoie.com

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101
Telephone: +1.206.359.8000
Facsimile: +1.206.359.9000

Counsel for Defendant University of Washington

CERTIFICATE OF SERVICE

I certify under penalty of perjury that on March 4, 2024, I caused to be electronically filed the foregoing document with the Clerk of the Court using the CM/ECF system, which will send a notification of the filing to the email addresses indicated on the Court's Electronic Mail Notice List.

Dated: March 4, 2024

s/ Erin K. Earl
Erin K. Earl

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

Exhibit A

FILED
2024 FEB 12 03:37 PM
KING COUNTY
SUPERIOR COURT CLERK
E-FILED
CASE #: 24-2-03365-3 SEA

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

JS 44 (Rev. 04/21)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

ALEXANDER IRVINE and BARBARA TWADDELL, individually and on behalf of all others similarly situated

(b) County of Residence of First Listed Plaintiff King County
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Alexander F. Strong, Stobaugh & Strong P.C.,
126 NW Canal Street, Suite 100, Seattle, WA 98107
Tel. (206) 622-3536 / Email: astrong@bs-s.com

DEFENDANTS

UNIVERSITY OF WASHINGTON, an agency of the STATE OF WASHINGTON

County of Residence of First Listed Defendant King County
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*
Erin K. Earl, Perkins Coie LLP,
1201 Third Avenue, Suite 4900, Seattle, WA 98101
Tel.: (206) 359-8510 / Email: EEarl@perkinscoie.com

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☒ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☒ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☒ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit (15 USC 1681 or 1692)
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

INTELLECTUAL PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

V. ORIGIN *(Place an "X" in One Box Only)*

- ☐ 1 Original Proceeding
- ☒ 2 Removed from State Court
- ☐ 3 Remanded from Appellate Court
- ☐ 4 Reinstated or Reopened
- ☐ 5 Transferred from Another District *(specify)*
- ☐ 6 Multidistrict Litigation - Transfer
- ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. §§ 1332(d), 1441, 1446, 1453

Brief description of cause:
Data breach class action

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions):

JUDGE See Notice of Related Cases DOCKET NUMBER See Notice of Related Cases

DATE 3/4/2024

SIGNATURE OF ATTORNEY OF RECORD /s/ Erin K. Earl

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I.(a) Plaintiffs-Defendants. Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) County of Residence. For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) Attorneys. Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. Jurisdiction. The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below**; NOTE: federal question actions take precedence over diversity cases.**)

III. Residence (citizenship) of Principal Parties. This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. Nature of Suit. Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: Nature of Suit Code Descriptions.

V. Origin. Place an "X" in one of the seven boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.

VI. Cause of Action. Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service.

VII. Requested in Complaint. Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. Related Cases. This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.

CERTIFICATE OF SERVICE

I certify under penalty of perjury that on March 4, 2024, I caused the following to be served the foregoing NOTICE OF REMOVAL TO SUPERIOR COURT CLERK by the method(s) indicated:

Alexander F. Strong
Stobaugh & Strong P.C.
126 Canal Street, Suite 100
Seattle, WA 98107
astrong@bs-s.com

___ Via hand delivery
_X_ Via U.S. Mail, 1st Class, Postage Prepaid
___ Via Overnight Delivery
___ Via Facsimile
_X_ Via Email
___ Other: _____

Ben Barnow
Anthony L. Parkhill
Riley W. Prince
Barnow & Associates, P.C.
205 West Randolph Street, Ste. 1630
Chicago, IL 60606
bbarnow@barnowlaw.com
aparkhill@barnowlaw.com
rprince@barnowlaw.com

___ Via hand delivery
_X_ Via U.S. Mail, 1st Class, Postage Prepaid
___ Via Overnight Delivery
___ Via Facsimile
_X_ Via Email
___ Other: _____

DATED this 4th day of March, 2024.

s/ Erin K. Earl
Erin K. Earl, Bar No. 49341
EEarl@perkinscoie.com

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000