FILED
17 DEC 11 PM 4:13
KING COUNTY
SUPERIOR COURT CLERK
E-FILED
CASE NUMBER: 17-2-23244-1 SEA

THE HONORABLE HOLLIS HILL

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

S.A., ABHI SHETH, LANDON THURMAN, and DALE DEAN, individually and on behalf of all others similarly situated, JANE AND JOHN DOES 1-10, individually and on behalf of all others similar situated, Plaintiffs, vs. WASHINGTON STATE UNIVERSITY, Defendant,	No. 17-2-23244-1 SEA (consolidated with case No.17-2-25052-0) CONSOLIDATED AMENDED CLASS ACTION COMPLAINT

Plaintiffs S.A., Abhi Sheth, Landon Thurman, and Dale Dean ("Plaintiffs"), individually and on behalf of the proposed Class defined below, bring this Class Action Complaint against Defendant Washington State University ("WSU" or "Defendant") and allege as follows upon personal knowledge, experience, information and belief, including investigation conducted by their undersigned attorneys:

I. NATURE OF THE ACTION

1. Plaintiffs bring this class action against WSU for its failure to properly secure and safeguard personally-identifiable information, including without limitation names, social

security numbers, educational and other sensitive personal information, including personal health information ("PHI"), (collectively, "Personal Information"), and for failing to provide timely, accurate and adequate notice to Plaintiffs and other Class members that their Protected Information had been stolen and precisely what types of information was stolen. Plaintiffs seek, among other things, orders requiring WSU to fully and accurately disclose the nature of the information that has been compromised and to adopt reasonably sufficient security practices and safeguards to prevent incidents like the Security Breach in the future.

2. WSU is one of the largest public research universities in Washington state. It operates a network of campuses throughout Washington. WSU Extension has offices in 39 counties across the state, which provides training and continuing education programs to thousands within the state.

3. As one of the premier research institutions and destinations for higher learning in Washington, WSU collects, stores and maintains a massive amount of personally identifiable data on Washington state citizens. WSU admittedly obtains and collects the Personal Information of Washington state citizens through direct and indirect means.

4. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and the Class Members' Personal Information, WSU assumed legal and equitable duties to those individuals. WSU knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Personal Information from disclosure. At all relevant times, Plaintiffs and the putative class have taken reasonable steps to maintain the confidentiality of their Personal Information.

5. Catastrophically to Plaintiffs and the proposed Class Members, WSU failed to adequately protect Plaintiffs' and Class Members' Personal Information from involuntary breach

and disclosure resulting in one of the largest, if not the largest, breach of Personal Information by an institution of higher learning in Washington state history. On June 9, 2017, WSU disclosed that a 8-by-10 foot safe containing a hard drive used to store backed-up files from a server used by WSU's Social and Economic Sciences Research Center had been stolen (the "Security Breach"). The hard drive contained the Personal Information of at least one million people, most if not all of whom, were unsuspecting Washington citizens. Subsequent investigation has revealed that the hard drive was stolen from a $126.00 per month storage unit at Quality Self Storage in Olympia, Washington. Upon information and belief, WSU would have been required to sign a contract, that limits the value of personal property stored, and exculpates the storage facility from any negligent acts or omissions by its principals and employees.

6. According to WSU, it first learned of the Security Breach on April 21, 2017. However, WSU waited six weeks to disclose the Security Breach to the public and individuals known to have been impacted by the Security Breach. As a result of WSU's actions, Plaintiffs and the Class Members had no idea that their Personal Information had been compromised, let alone collected, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social and financial harm.

7. The Security Breach not only reveals that WSU failed to exercise reasonable care in storing and protecting Plaintiff's and Class Members' Personal Information, it exposed the Personal Information of at least one million people to fraud and misuse by unauthorized third parties. Upon information and belief, the affected individuals face a particularly real, concrete, and actual risk of harm and future identity theft as the Personal Information contained confidential biographical information, in some cases collected over long periods of time. In addition, most if not all of the affected individuals had no idea that WSU was in possession of

their Personal Information or how it was by obtained in the first place.

II. PARTIES TO THE ACTION

8. Plaintiff S.A. is an individual and a resident of King County, Washington. Plaintiff S.A. brings this action on behalf of herself and the proposed Class defined below. She discovered that her Personal Information was compromised as a result of WSU's actions from WSU on or about June 9, 2017. She alleges she has spent significant time dealing with the consequences of the Security Breach. Plaintiff has experienced a reasonable fear of identity theft or other economic harm since learning of the Security Breach. She purchased identity theft insurance as a result of WSU's actions. The value of her personal information has depreciated due to WSU's actions.

9. Plaintiff Abhi Sheth is an individual and is a resident of Seattle, King County, Washington. Plaintiff Sheth was unemployed for approximately six months in 2009 and approximately four months in 2013 and participated in a state job-training program. On or about April 29, 2017, Plaintiff Sheth suffered a fraudulent online charge on one of his lines of credit for $196.58. Plaintiff Sheth had to file a fraud claim with the vendor. In June 2017, Plaintiff Sheth received a letter from Defendant in the mail dated June 9, 2017, notifying him that his information was compromised in the Security Breach.

10. Plaintiff Landon Thurman is an individual and is a resident of Denham Springs, Louisiana. Plaintiff Thurman was part of a research study at WSU Medical Center in 2005 and 2006 in connection with treatment he received from Seattle Children's Hospital. In or around the last week of April, 2017, Plaintiff Thurman suffered two fraudulent online charges on one of his lines of credit for $516.99. Plaintiff Thurman had to file a fraud claim with his credit card company. About a week later, Plaintiff Thurman's credit card company contacted him regarding

another fraudulent online charge. A few weeks later, Plaintiff Thurman received notification that a fraudulent account was opened and fraudulent orders totaling $537.14 were placed through a WebBank credit program. Plaintiff had to file a fraud claim with the bank. In June 2017, Plaintiff Thurman received a letter from Defendant in the mail dated June 9, 2017, notifying him that his information was compromised in the Security Breach. In early December 2017, Plaintiff Thurman received notification from an identity theft protection company that someone had attempted to apply for a new credit card using his personal information.

11. Plaintiff Dale Dean is an individual and is a resident of Buckeye, Arizona. Plaintiff Dean attended City University of Seattle and obtained his Master's Degree in or around December 2010. On or about June 23, 2017, Plaintiff Dean received a letter from Defendant in the mail dated June 9, 2017 notifying him that his information was compromised in the Security Breach. On or about June 25, 2017, Plaintiff Dean received notification that fraudulent orders totaling almost $2,000 were placed and fraudulent lines of credit were opened at Kohl's retail store. Another fraudulent line of credit was opened in Plaintiff Dean's name at an Arizona credit union on or around July 15, 2017. Plaintiff Dean's cellular telephone account also was compromised when unauthorized persons attempted to change his account password in or around August 2017.

12. *Plaintiffs will add additional Jane and John Does, who have experienced harm and damages as a result of WSU's actions.*

13. WSU is an American public research university based in Pullman, Washington. WSU is one of the largest public universities in Washington, with over 200,000 alumni worldwide. WSU's enrollment in 2016 exceeded 28,000, 80% of whom are in-state students. WSU is one of Washington's premier research universities, boasting research and development

expenditures of approximately $334.1 million in fiscal year 2016 alone.

III. JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction over the action and personal jurisdiction over the Defendant.

15. Venue is proper pursuant to RCW § 4.92.010 because, *inter alia*, the Defendant is registered to and does conduct business in this County. Given King County's size, it is possible that a majority of those receiving letters actually reside in King County.

16. Plaintiffs S.A. and Sheth have satisfied the presentment and pre-filing requirements of RCW § 4.92.006, *et seq*. Defendant has waived those statutory requirements for Plaintiffs Thurman and Dean.

IV. FACTUAL BACKGROUND

A. WSU Owed a Duty to Plaintiff and the Class to Protect the Personal Information and Failed to Do So.

17. Based on obligations created under the law, state statutes and industry standards, among other sources, WSU had a duty to adopt reasonable measures to protect Plaintiffs' and Class members' Personal Information from involuntary disclosure to third parties.

18. Catastrophically, WSU failed to adopt adequate measures to protect Plaintiffs' and Class members' Personal Information in violation of these duties. In a press release issued on June 9, 2017, WSU admitted that it failed to protect the Personal Information due to inadequate training, policies and IT storage practices:

> Washington State University (WSU) is committed to protecting the security and confidentiality of all personal information entrusted to it. Regrettably, the University recently became aware of a security incident involving certain community members' personal information.
>
> On April 21, 2017, we learned that a locked safe containing a hard drive had been stolen. The hard drive was used to store backed-up files from a server used by our

> Social & Economic Sciences Research Center (SESRC). Immediately upon learning of the theft, we initiated an internal review and notified local law enforcement.
>
> On April 26, we confirmed that the stolen hard drive contained personal information from some studies and evaluations conducted by the SESRC. As a result, we retained a leading computer forensics firm to assist in the investigation. The drive contained documents that included personal information such as names, Social Security numbers and, in some cases, personal health information. Entities that provided data to the SESRC include school districts, community colleges, and other customers.
>
> We take this incident very seriously. We are notifying impacted individuals so they can take steps to protect themselves and offering free credit monitoring and identity theft protection services to those individuals whose personal information may have been accessed. We are also notifying the entities that provided SESRC with data that included personal information.
>
> As president of Washington State University, I deeply regret that this incident occurred and am truly sorry for any concern it may cause our community. The University is taking steps to help prevent this type of incident from happening again. These steps include strengthening our information technology operations by completing a comprehensive assessment of IT practices and policies, improving training and awareness for University employees regarding best practices for handling data, and employing best practices for the delivery of IT services. [1]

19. As set forth above, WSU admits that the Security Breach occurred as a result of the theft of a hard drive containing highly sensitive and confidential personal information of at least one million individuals, most if not all of whom either currently or at one point resided in Washington. Specifically, WSU has disclosed that a significant portion of the data stolen included state education data collected by school districts, community colleges and other public agencies on students who attended high school in Washington between 1998 and 2013.[2]

---

[1] *Washington State University identifies and addresses security incident involving stolen hard drive*, accessible at wsu.edu/security-incident/ (last visited July 1, 2017).

[2] *Frequently Asked Questions, Washington State University identifies and addresses security incident involving stolen hard drive,* accessible at https://wsu.edu/security-incident/faq/#toc-i-never-gave-washington-state-university-my-information-how-did-you-get-it- (last visited July 1, 2017)

20. The Personal Information includes, but is not limited to, names, social security numbers, addresses, phone numbers, email addresses, dates of birth and other sensitive biographical information, including SAT scores, ACT scores, apprenticeship data, private career school data and personal health information that can now be misused by data thieves and other cyber criminals. The impacted individuals have been, are, and will continue to be at significant risk of identity theft and various other forms of continuing financial, personal, and social harm, for which they are entitled to legal and equitable relief. Subsequent investigation has also revealed that the hard drive contained sensitive bank account information on an unidentified number of Washington businesses. Upon information and belief, the hard drive was not encrypted and could be accessed with widely available tools found online. As a result, WSU was notified on April 21, 2017 that it could not assume any of the information was safe. However, rather than immediately notify Plaintiffs and the proposed Class, WSU hired a national public relations firm.

21. Despite the known and obvious current, continuing, and concrete risk of harm to Plaintiffs and the proposed Class, WSU's actions and omissions establish that it failed to take reasonably sufficient steps to protect the Personal Information stored on the hard drive. Subsequent investigation and reporting has revealed that the hard drive containing the Personal Information of 1,027,079 people was stolen from a self-storage locker (the "Self-Storage Locker") rented by WSU from Quality Self Storage in Olympia, Washington.[3] As recently confirmed by the Seattle Times, not only was the Self-Storage Locker accessible by anyone able

[3] The Seattle Times, *WSU gets costly lesson in theft of hard drive with more than 1 million people's personal data*, accessible at http://www.seattletimes.com/seattle-news/education/wsu-gets-costly-lesson-in-theft-of-hard-drive-with-over-1-million-social-security-numbers/ (last visited July 23, 2017).

to pass through the front gate, but the storage facility even lacked video surveillance:

> [WSU] had a backup hard drive containing confidential information — such as Social Security numbers — for 1,027,079 people.
>
> Where was it stored? In a $126-a-month, 8-by-10 self-storage locker in Olympia, inside a $159, 86-pound safe that you can buy at Home Depot.
>
> The storage facility is a few blocks from the school's Social and Economic Sciences Research Center. It conducts projects with such teasing titles as, "Higher Education Opportunities in East Jefferson County."
>
> * * *
>
> "You use a storage locker for old mattresses and crappy furniture, not personally identifiable information," says Bryan Seely, a Seattle-based cybersecurity expert. "A lot of people have access to those facilities. Once you're through the main gate you generally have access to every door in every storage unit."
>
> As for the safe, which was hauled out of the locker, says Seely, "Now you're not at the crime scene. You have all the time in the world to crack it open." [4]

22. At the time the Personal Information was stored at Quality Self Storage, WSU and/or its agents knew or should have known that the hard drive, storage facility and storage locker lacked sufficient security measures to protect the Personal Information from the risk of involuntary disclosure and/or breach, including the risk of disclosure and breach caused by the criminal acts of third parties. Moreover, they knew or should have known, that the Storage facility itself waived liability for its own negligence, and warned WSU not to store anything of value in the unit. Among other things, WSU failed (1) to take appropriate steps to safeguard the Personal Information such as encrypting the hard drive, (2) to adopt appropriate policies and procedures beforehand to prevent the Security Breach, (3) to provide timely notice to the Plaintiffs and the proposed Class once the Security Breach occurred, and (4) to provide a cogent

---

[4] *Id.*

and transparent picture of how the Security Breach occurred and its full effect on Plaintiffs and the proposed Class.

23. The Security Breach, and Plaintiffs' and the proposed Class' damage, was caused and enabled by WSU's knowing, reckless and/or negligent violation of its common law and statutory obligations to protect the Personal Information from disclosure. WSU has failed to adequately compensate Plaintiffs and the proposed Class, necessitating this lawsuit.

B. Victims of Security Breaches Suffer Real, Concrete and Actual Harm

24. WSU has acknowledged the sensitive and confidential nature of the Personal Information. To be sure, collecting, maintaining, and protecting such data is vital to many of WSU's university business purposes. WSU has acknowledged through its conduct, statements and policies[5] that the misuse or inadvertent disclosure of such data can pose major privacy and financial risks to impacted individuals, and that under state law it may not disclose and must take reasonable steps to protect such information from improper release or disclosure. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgement of its duties to keep such sensitive information private and secure, WSU failed to take appropriate steps to protect the Personal Information of Plaintiffs and the proposed Class from being compromised.

25. It is well documented that confidential, personally identifiable and/or biographic information is a highly-coveted commodity on the black market and a frequent target of data and identity thieves.

---

[5] *See University Data Policies*, Washington State University Executive Policy Manual, accessible at http://public.wsu.edu/~forms/HTML/EPM/EP8_University_Data_Policies.htm (last accessed November 26, 2017).

26. Both legitimate businesses (Google, Facebook, etc.) and criminal enterprises alike recognize the lucrative value of personally identifiable information, which is precisely the kind of information that is the subject of this case. Sensitive biographic information is now more lucrative than an individual's credit card information, which can be automatically changed, frozen and/or reissued once notice of the breach is received.[6] As one industry report recently found: "Increasingly, criminals are using biographical data gained from multiple sources to perpetrate more and larger thefts."[7] For example, in the now world-famous Target data breach, in addition to payment card information pertaining to credit and debit card holders, the hackers also stole biographical information pertaining to 70,000 customers. According to a 2017 joint study published by IBM Security and the Ponemon Institute, the average cost of a stolen record containing confidential or sensitive personal information is $141.[8]

27. According to the Federal Trade Commission, this type of information is "as good as gold" to identity thieves because, once they have the personal information, "they can drain our bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[9] It is well established that compromised personal information exposes victims to loss of reputation, loss of employment, blackmail and other negative effects such as

---

[6] *Data Breaches Happening at Record Pace, Report Finds*, accessible at http://www.nbcnews.com/business/consumer/data-breaches-happening-record-pace-report-finds-n785881 (last visited August 8, 2017).

[7] *Verizon 2014 Compliance Report*, accessible at www.cisco.com/c/dam/en_us/solutions/industries/docs/retail/verizon_pci2014.pdf (last visited July 1, 2017).

[8] IBM Security and Ponemon Institute, 2017 Cost of Data Breach Study, accessible at https://public.dhe.ibm.com/common/ssi/ecm/se/en/sel03130wwen/SEL03130WWEN.PDF (last visited August 8, 2017).

[9] FTC, *Signs of Identity Theft*, accessible at www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited July 1, 2017).

incarceration.[10] The United States Government Accountability Office noted in a June 2007 report that victims of identity theft face "substantial costs and inconveniences repairing damage to their credit records" and their "good name."[11] Moreover, stolen biographical information is regularly used to perpetrate immigration and tax fraud and to illegally obtain government benefits.

28. The FTC estimates that approximately 15 million Americans face identity theft per year [12] and, according to recent industry reporting, one in four data breach notification recipients fall victim to identity fraud.[13] A 2014 report by the Department of Justice estimated that victims of identity theft suffer a combined average loss of $1,343.[14] According to Javelin Strategy and Research, a record number of consumers — 15.4 million — suffered some form of identity fraud in 2016, an increase of two million consumers from the previous year, resulting in total fraud losses of approximately $16 billion.

29. In addition, it is well documented that — similar to toxic exposure cases — the harm caused by involuntary disclosure of personal information is continuing and the consequences can follow the affected individual for a lifetime. According to the DOJ, it normally

---

[10] *See Remsburg v. Docusearch, Inc.*, 149 N.H. 148, 816 A.2d 1001, 1008 (N.H. 2003) ("[Identity theft] often destroys a victim's ability to obtain credit from any source and may, in some cases, render the victim unemployable or even cause the victim to be incarcerated."

[11] GAO-07-737, Data Breaches and Identity Theft, accessible at http://www.gao.gov/new.items/d07737.pdf (last accessed on August 8, 2017).

[12] USA Today, *Identity theft hit an all-time high in 2016*, accessible at www.usatoday.com/story/money/personalfinance/2017/02/06/identity-theft-hit-all-time-high-2016/97398548/ (last visited July 1, 2017).

[13] 2013 Identity Fraud Report: Data Breaches Becoming Treasure Trove for Fraudsters, accessible at https://www.javelinstrategy.com/coverage-area/2013-identity-fraud-report-data-breaches-becoming-treasure-trove-fraudsters (last visited July 1, 2017).

[14] DOJ, *Victims of Identity Theft, 2014*, accessible at www.bjs.gov/content/pub/pdf/vit14.pdf (last visited July 1, 2017).

can take victims well over a year to recover from identity theft.[15] According to the FTC, identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit and personal lives.[16] Once the information has been compromised, criminals often trade the information on the black market for years. Thus, it is well documented that short-term services like credit monitoring are insufficient to make impacted individuals whole again, as it fails to account for the personal time and energy spent untangling the mess caused by identity theft or the fact that the total loss will take several years to occur.

30. Notwithstanding the volumes of publicly available information documenting the real harm done to affected individuals, and even though WSU had the resources and sophistication to adopt the best practices and industry standards, WSU was lackadaisical, cavalier, reckless or, at the very least, negligent in maintaining and protecting the Personal Information of Plaintiffs and the proposed Class. Adding insult to injury, following the breach, WSU has offered wholly insufficient relief to the affected individuals even though Plaintiffs and the proposed Class now face years of constant surveillance of their personal and financial records, the out-of-pocket costs of monitoring their credit report and bank accounts, the increased risk of identity theft and the loss of control of their basic personal privacy rights, among other harms. No doubt Plaintiffs and the proposed Class are incurring and will continue to incur future damages due to WSU's unlawful conduct, necessitating this lawsuit.

C. Plaintiff and the Class Have Suffered Damages

31. The Security Breach was a direct and proximate result of WSU's failure to

---

[15] DOJ, *Victims of Identity Theft, 2012*, accessible at https://www.bjs.gov/content/pub/pdf/vit12.pdf (last visited July 1, 2017).

[16] FTC, *Identity Theft*, accessible at www.consumer.ftc.gov/feature-0014-identity-theft (last visited July 1, 2017).

properly safeguard and protect Plaintiffs' and Class Members' Personal Information from unauthorized access and disclosure as required by various regulations, industry practices and the common law. These obligations required WSU, without limitation, to implement sufficient administrative, technical and physical safeguards to ensure the security and confidentiality of Plaintiffs' and the Class' Personal Information, and to protect against reasonably foreseeable harms and threats to the security or integrity of such Personal Information, including the foreseeable criminal acts of third parties.

32. Plaintiffs' and Class Members' Personal Information is private and sensitive in nature and was inadequately protected by WSU. WSU did not obtain Plaintiffs' and Class Members' consent to disclose their Personal Information to any other person as required by applicable law, and failed to adopt adequate safeguards in storing and protecting the Personal Information, which is indicated by WSU's decision to store the hard drive containing the Personal Information of over one million people in a self-storage unit that lacked basic security features such as video surveillance.

33. As a direct and proximate result of WSU's wrongful action and inaction, Plaintiffs and the proposed Class Members have been placed in imminent, immediate and continuing increased risk of harm of identity theft and identity fraud, requiring them to expend time and resources to mitigate the actual and potential impact of the Security Breach on their lives including without limitation by contacting their financial institutions, freezing accounts, requesting monitoring alerts from credit reporting agencies, and closely reviewing and monitoring their credit reports and IRS returns for unauthorized activity for years to come.

34. WSU's wrongful action and inaction directly and proximately caused the theft and dissemination of Plaintiffs' and the proposed Class Members' Personal Information into the

public domain, causing them to suffer and continue to suffer various personal, social and financial loss and other current, actual and imminent harms, including without limitation:

a. theft of their Personal Information;

b. deprivation of rights they possess under Washington state law;

c. imminent and certainly impending injury flowing from potential fraud and identity theft;

d. the untimely and inadequate notification of the Security Breach;

e. the improper disclosure of Personal Information;

f. lost privacy;

g. ascertainable losses in the form of out-of-pocket expenses, lost value, harm to reputation and the value of time reasonably incurred to remedy or mitigate the effects of the involuntary disclosure of Personal Information; and

h. the various other forms of personal, financial, legal and social injuries without limitation that have occurred or are reasonably certain to occur in the future.

35. WSU has acknowledged through its statements and conduct, albeit inadequately, that its wrongful actions and inaction has caused actual and potential harm to Plaintiffs and the proposed Class Members by offering them one year of low quality credit monitoring and identity theft protection services, despite the fact that it is well known and acknowledged by government and industry leaders that the damage and fraud from the Security Breach is ongoing and takes years to fully develop.

36. However, rather than seek to fully and fairly compensate Plaintiffs and the proposed Class in good faith, WSU has chosen to save costs by offering inadequate relief while refusing to fully and accurately disclose the nature of information that was compromised. Indeed,

WSU would rather pay exorbitant fees to private consultants and PR firms than fully and fairly compensate Plaintiffs and the proposed Class. Thus, Plaintiffs and the proposed Class are left to their own devices to try to protect themselves from the personal, financial and social consequences of the Security Breach, for which they bear no fault and could have done nothing beforehand to prevent. The appropriate relief owed by WSU to Plaintiffs and the proposed Class is ascertainable and should be determined by the trier of a fact.

37. As the Personal Information of Plaintiffs and the proposed Class has been stolen and disseminated into the public domain where there is a well-established national and international black market for such Personal Information, Plaintiffs and the proposed Class have an undeniable interest in insuring that WSU adopt appropriate safeguards to ensure that their information is secure and will remain secure in the future.

V. CLASS ACTION ALLEGATIONS

38. Plaintiffs seek relief in their individual capacities and as representatives of all others who are similarly situated. Pursuant to the Washington Civil Rules, Plaintiffs seek certification of a class consisting of all persons whose Personal Information was compromised in the Security Breach disclosed by Washington State University on June 9, 2017 ("Nationwide Class"). In the alternative, Plaintiffs seek the certification of a class consisting of all persons currently residing in the State of Washington whose Personal Information was compromised in the Security Breach disclosed by Washington State University on June 9, 2017 ("Washington Class"). These classes are collectively referred to herein as the "Class." Plaintiffs reserve the right to amend these class definitions.

39. Excluded from the Class is WSU; any agent, affiliate, parent or subsidiary of WSU; any entity in which WSU has a controlling interest; any officer or director of Defendant;

and any successors and assigns of WSU. Also excluded are any judge to whom this case is assigned, including his or her court personnel, and attorneys in the case, and the foregoing individuals' immediate family members.

40. **Numerosity**. The members of the Class are so numerous that the joinder of all members is impractical. WSU has acknowledged that the Personal Information of over one million people was stolen in the Security Breach. The Seattle Times reported that the exact number is 1,027,079. This is too many people to join in a single action. Although the Washington Class may be slightly smaller, on information and belief the Washington Class consists of thousands of members, at a minimum, and as joinder of all would be impracticable, also satisfies the numerosity requirement.

41. **Commonality and Predominance**. Plaintiffs' and Class Members' claims raise predominantly common factual and legal questions that can be answered for all Class Members through a single class-wide proceeding. For example, to resolve any Class Member's claims, it will be necessary to answer the following questions. The answer to each off these questions will necessarily be the same for each Class Member.

a. Whether WSU unlawfully used, maintained, stored, lost and/or disclosed the Personal Information;

b. Whether WSU failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Security Breach;

c. Whether WSU unreasonably delayed in notifying affected individuals of the Security Breach and whether the belated notice was adequate;

d. Whether WSU's conduct was negligent;

e. Whether WSU's conduct in connection with the Security Breach and notification thereof violated Washington law; and

f. Whether Plaintiffs as the Class are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

42. **Ascertainability.** The names of all the Class Members are readily ascertainable from information in Defendant's possession, custody, or control. Appropriate notice can be accomplished through a combination of media and online methods.

43. **Typicality**. Plaintiffs' claims are typical of those other Class Members as each arises from the same Security Breach, the same alleged negligence of and/or statutory violations by Defendant, and the same unreasonable manner of notifying individuals regarding the Security Breach.

44. **Adequacy of Representation**. The Class Plaintiffs will fairly and adequately represent and protect the interests of the members of the Class. Their interests do not conflict with Class Members' interests and they have retained experienced counsel that will vigorously prosecute this action on behalf of the Class.

45. **Superiority of Class Action**. A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all Class Members is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of claims. There will be no difficulty in the management of this action as a class action.

46. In addition to satisfying the prerequisites of CR 23(a), Plaintiffs satisfy the requirements for maintaining a class action under CR 23(b). Common questions of law and fact predominate over any questions affecting only individual members and a class action is superior

to individual litigation or any other available methods for the fair and efficient adjudication of the controversy. Damages for any individual class member are insufficient to justify the cost of individual litigation, such that, in the absence of class treatment, WSU's violations of law inflicting substantial damages in the aggregate would go un-remedied.

47. In the alternative, class certification is appropriate because WSU has acted or refused to act on grounds generally applicable to the Class, thereby making final injunctive relief appropriate with respect to the members of the Class as a whole.

VI. CLAIMS FOR RELIEF

FIRST CLAIM FOR RELIEF
Negligence
(On behalf of Plaintiffs and the Class)

48. Plaintiffs incorporate all preceding allegations as if set forth in full herein.

49. By obtaining and storing Plaintiffs' and Class Members' Personal Information, WSU undertook and owed a duty to Plaintiffs and Class Members to exercise reasonable care to secure and safeguard that information, to prevent disclosure of that information, to guard the information from theft, and to detect any attempted or actual breach of its IT systems.

50. WSU admitted, assumed, acknowledged and agreed through its statements, conduct, policies and/or procedures that Plaintiffs' and Class Members' Personal Information was private and confidential, and that it should exercise reasonable care to protect the Personal Information.

51. WSU breached its duty to Plaintiffs and the Class Members to adequately protect and safeguard this information, including by storing the data in an unencrypted form on a highly vulnerable device susceptible to a security breach, by knowingly disregarding industry standards, despite obvious risk to the impacted parties, and by allowing the Security Breach to occur. WSU

failed to provide adequate supervision and oversight of the Personal Information, despite the publicized risks and foreseeable harm to the impacted individuals of breach, which permitted a third party to unlawfully obtain the information for actual and potential dissemination into the public domain where there is a well-established national and international black market for such Personal Information.

52. In the alternative, WSU also owed a duty of care to adopt appropriate safeguards to protect the Personal Information of Plaintiffs and Class Members based on industry standards, applicable laws, regulations or rules.

53. In the alternative, WSU also owed a duty of care to protect and safeguard the Personal Information based on a special relationship that existed between WSU and the Plaintiffs and Class Members.

54. Due to WSU's acts and omissions described in this Complaint, including without limitations its failure to exercise reasonable care to adequately protect Plaintiff's and Class member's Personal Information from being accessed, disseminated, stolen and/or misused, and continuing failure to share crucial, complete information with Plaintiffs and Class members in a timely manner, WSU unlawfully breached its duties of care to Plaintiffs and Class members while it was within WSU's possession and control.

55. WSU improperly and inadequately safeguarded the Personal Information of Plaintiffs and Class members in deviation from standard industry rules, regulations and practices at the time of the unauthorized disclosure. Neither Plaintiffs nor Class members contributed to the Security Breach and subsequent misuse of their Personal Information as described in this Complaint.

56. WSU's failure to use appropriate measures to protect Plaintiff's and Class

members' Personal Information as described in the Complaint created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of Plaintiffs' and Class members' personal information.

57. The facts presently known indicate that WSU was lackadaisical, cavalier, reckless or, at the very least, negligent in storing and protecting the Personal Information of Plaintiffs and the proposed Class. WSU's conduct departed from all reasonable standards of care, including, but not limited to: (1) failing to adequately protect the Personal Information, (2) failing to conduct regular security audits; (3) failing to provide adequate and appropriate supervision of persons having access to Plaintiff's and Class members' Personal Information; (4) storing the Personal Information at an off-campus self-storage facility that lacked basic security features such as video surveillance; and (5) failing to provide Plaintiffs and Class members with timely sufficient notice that their sensitive Personal Information had been compromised. The full nature of WSU's negligence can only be identified after a thorough investigation into the facts and events surrounding the Security Breach.

58. As a direct and proximate result of WSU's acts or failures to act, Plaintiffs and the Class have suffered personal, financial, social and compensable injury that is continuing, including, but not limited to, the kind of damages alleged herein arising from the misuse of sensitive personal information, fraud and/or identity theft, which has already occurred or may take months if not years to discover given the far-reaching, adverse, and detrimental consequences of identity theft and loss of privacy. The nature of other forms of financial damage and injury may take years to detect and the potential scope can only be assessed after a thorough investigation into the facts and events surrounding the Security Breach.

59. As a result of WSU's negligent acts and omissions, Plaintiffs and Class members

have suffered compensable damages, including the value of their Personal Information, ongoing, imminent and certainly impending threat of identity theft, actual identity theft, fraud and abuse resulting in monetary loss and economic harm, loss of confidentiality of the stolen confidential data, the illegal sale of the compromised data on the black market, expenses and time spent on credit monitoring and identity theft insurance, time spent scrutinizing bank statements, credit card statements and credit reports, disruption to their lives and fear of future identity theft, the reasonable value of decreased credit scores and ratings, lost work time and other economic and non-economic harm. Plaintiffs and Class members have been damaged in an amount to be proven at trial. It is foreseeable that Class members may have, and will suffer emotional distress as a result of this breach.

60. It was reasonably foreseeable that WSU's failure to implement and maintain adequate and reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Security Breach, WSU's unreasonable delay in notifying affected individuals of the Security Breach, and WSU's continuing inadequate notice would result in the Plaintiffs' and Class members' injuries.

SECOND CLAIM FOR RELIEF
Violation of Washington Data Breach Disclosure Law
(On behalf of Plaintiffs and the Class)

61. Plaintiffs incorporate all preceding allegations as if set forth in full herein.

62. Plaintiffs allege additionally and alternatively that RCW § 19.255.010 provides that "[a]ny person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized

person." Similarly, RCW § 42.56.590 provides that: [a]ny agency that owns or licenses data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not secured. Notice is not required if the breach of the security of the system is not reasonably likely to subject consumers to a risk of harm. The breach of secured personal information must be disclosed if the information acquired and accessed is not secured during a security breach or if the confidential process, encryption key, or other means to decipher the secured information was acquired by an unauthorized person."

63. The Security Breach resulted in an "unauthorized acquisition of computerized data that compromise[d] the security, confidentiality, [and] integrity of personal information maintained" by WSU and, therefore, WSU experienced a "breach of [its] security of [its] system," as defined by RCW § 19.255.010(4) and RCW § 42.56.590.

64. Under RCW § 19.255.010 and RCW § 42.56.590, WSU was required to disclose the Security Breach "immediately following discovery," and "in the most expedient time possible and without unreasonable delay."

65. The law imposes an affirmative duty on WSU to timely disclose the unauthorized access and theft of the Personal Information to Plaintiffs and the Class members so that they can take appropriate measures, mitigate damage, protect against adverse consequences and thwart future fraud and misuse of the Personal Information. WSU failed to disclose the Security Breach immediately after discovering the Security Breach and waited an unreasonable amount of time before notifying all affected individuals. WSU unreasonably delayed informing Plaintiffs and

Class members of the Security Breach after it knew or should have known it occurred.

66. WSU breached statutory and common law duties to notify Plaintiffs and Class members of the unauthorized access by waiting an unreasonable amount of time after learning of the breach to notify Plaintiffs and Class members and then by failing to provide Plaintiffs and Class members with sufficient information regarding the breach. To date, WSU has failed to provide sufficient information to Plaintiffs and Class members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiffs and Class members.

67. WSU's failure to provide notice immediately after discovering the breach, and provide Plaintiffs and Class members with the information they need to protect themselves, is a violation of RCW § 19.255.010 and RCW § 42.56.590.

68. Plaintiffs and Class members have suffered harm as a result of WSU's acts and omissions and been damaged in an amount to be proven at trial.

69. Additionally, Plaintiffs and Class members are entitled to injunctive relief under RCW § 19.255.010 and RCW § 42.56.590 in the form of an order requiring WSU to (1) amend its security policies to ensure that Personal Information of third parties is never stored at an off-campus self-storage facility again; (2) engage third-party security auditors and internal security personnel to review their security policies and systems on a periodic basis to detect and correct any vulnerabilities; (3) regularly audit, test and train its personnel who make security decisions involving Personal Information regarding any industry standards and any new and modified procedures; (4) routinely conduct regular internal security training and education to support, maintain and establish policies and procedures for the safe and secure storage and protection of sensitive information in the future; and (5) meaningfully disclose to all Class members precisely

what information was compromised, the threats they face as a result of their Personal Information being compromised and the steps which should be taken to protect themselves.

THIRD CLAIM FOR RELIEF
Violation of RCW 42.48 et seq.
(On behalf of Plaintiffs and the Class)

70. Plaintiffs incorporate all preceding allegations as if set forth in full herein.

71. RCW § 42.48.020 and RCW § 42.84.040 prohibit "state agencies" and "research professionals" from unlawful disclosure of individually identifiable information.

72. RCW § 42.48.010(1) defines "individually identifiable" as any record containing "information which reveals or can likely be associated with the identity of the person or persons to whom the record pertains."

73. Under RCW § 42.48.050, a state agency or research professional that violates any provision of RCW 42.48 is liable for civil penalties in the amount of $10,000 per violation, per claimant.

74. In the Security Breach, WSU compromised and improperly disclosed the "individually identifiable" information of over one million people without their knowledge or consent in violation of RCW 42.48 *et seq*. Each such disclosure was a violation of RCW § 42.48.050. Thus, WSU is liable to Plaintiffs and the Class members under RCW § 42.48.050 in the amount of $10,000 for each such violation, per claimant.

FOURTH CLAIM FOR RELIEF
Violation of the Washington Consumer Protection Act
(On behalf of Plaintiffs and the Class)

75. Plaintiffs incorporate all preceding allegations as if set forth in full herein.

76. WSU is a "person" within the meaning of the Washington Consumer Protection Act (the "Act") and conducts "trade" or "commerce" within the meaning of the RCW §

19.86.010.

77. The Act is expressly intended to protect individuals like Plaintiffs and Class members from unfair and deceptive practices in Washington. They are "persons" within the meaning of RCW § 19.86.010(1).

78. WSU's failure to promptly and fully disclose the Security Breach to Plaintiffs and the Class members, and compensate the same, within a reasonable time after learning of the breach constitutes unlawful, unfair and/or deceptive practices that offends public policy, including as set forth in the foregoing state laws, and prevents Plaintiffs and Class members from taking all necessary steps to protect themselves against current, imminent and future harm.

79. WSU's failure to safeguard the Personal Information of Plaintiffs and the Class members constitutes unlawful, unfair and/or deceptive practices that offend public policy, including as set forth in the foregoing state laws, and including because WSU held itself out as providing a secure environment for storage of Personal Information and financially benefited from that representation through grants and public and private funding, but then failed to take commercially reasonable steps to protect the Personal Information with which it was entrusted.

80. WSU's failure to fully disclose the details of the Security Breach to the victims and WSU's offer of inadequate relief including one year of basic credit monitoring services, constitutes unlawful, unfair and/or deceptive practices that offend public policy within the meaning of the Act, including as set forth in the foregoing state laws. Among other things, WSU's failure to disclose all material information prevents Plaintiffs and Class members from taking all necessary steps to protect themselves against current, imminent and future harm. In addition, WSU's offer of inadequate relief despite knowing the true risk of harm to Plaintiffs and the Class is deceptive, unlawful and creates a false sense of security and misrepresents the true

nature of past, current and future harm and/or risk of harm to Plaintiffs and the Class.

81. WSU's failure to safeguard the Personal Information disclosed in the Security Breach, and its failure to provide timely and complete notice of the Security Breach to the victims, causes substantial injury to Plaintiffs and Class members, is not outweighed by any countervailing benefits to consumers or competitors, and is not reasonably avoidable by consumers.

82. WSU's failure to safeguard the Personal Information disclosed in the Security Breach, and its failure to provide timely and complete notice of the Security Breach to the victims, is unfair because these acts and practices are immoral, unethical, oppressive, and/or unscrupulous.

83. WSU's unfair acts or practices occurred in its trade or business and have injured and are capable of injuring a substantial portion of the public. WSU's general course of conduct as alleged herein is injurious to the public interest, and the acts complained of herein are ongoing and/or have a substantial likelihood of being repeated.

84. As a direct and proximate result of WSU's unfair acts and practices, Plaintiffs and Class members suffered injury in fact.

85. Plaintiffs and Class members have been damaged and have suffered and will continue to suffer ascertainable losses as a direct result of WSU's wrongful and deceptive acts and omissions in violation of public policy as described herein in an amount to be proven at trial, including without limitation the lost value of their Personal Information, ongoing, imminent and certainly impending threat of identity theft, actual identity theft, fraud and abuse resulting in monetary loss and economic harm, loss of privacy and/or confidentiality, the illegal sale of the compromised data on the black market, expenses and time spent on credit monitoring, harm to

reputation, the out-of-pocket cost of identity theft insurance, distraction and loss of work time to address the consequences of the Security Breach, lost value of personal information, time spent scrutinizing bank statements, credit card statements and credit reports and consulting with professionals, the reasonable value of lost work time and decreased credit scores and ratings and various other forms of economic and non-economic harm.

86. Plaintiffs and Class members are entitled to an order enjoining the conduct complained of herein and ordering WSU to take remedial measures to prevent similar data breaches; actual damages in an amount to be proven at trial; treble damages pursuant to RCW § 19.86.090; costs of suit, including reasonable attorneys' fees; and such further relief as the Court may deem proper.

FIFTH CLAIM FOR RELIEF
Breach of Fiduciary Duty
(On behalf of Plaintiffs and the Class)

87. Plaintiffs incorporate all preceding allegations as if set forth in full herein.

88. By obtaining, storing and using Plaintiffs' and Class members' Personal Information without the knowledge of Plaintiffs or the Class members, WSU placed itself in a position of trust in relation to Plaintiffs and Class members and assumed fiduciary duties to Plaintiffs and Class members.

89. WSU was in a superior position to know the true state of facts about the inadequacy of its security measures and stands in a fiduciary or quasi-fiduciary relationship with Plaintiffs and Class members. Among other things, this fiduciary or quasi-fiduciary relationship required WSU to exercise the utmost standard of due care in protecting the Personal Information from disclosure and criminal acts of third parties. The fiduciary or quasi-fiduciary relationship also required WSU to disclose the insufficient nature of its security measures to Plaintiffs and

Class members and to deal honestly with Plaintiffs and Class members after it learned of the Breach. WSU admits that it was entrusted with the Personal Information of Plaintiffs and Class members and that it owed duties to Plaintiffs and Class members to ensure the Personal Information would be protected from all times.

90. WSU breached its fiduciary or quasi-fiduciary duty by failing to use sufficient measures to protect Plaintiffs' and Class members' Personal Information from hackers and by failing to provide timely and adequate notice of the breach.

91. Plaintiffs and Class members have been harmed and will continue to be harmed for years to come as a foreseeable result of WSU's breach of duty. Plaintiffs and Class members have suffered damages and are entitled to full and fair compensation in an amount to be proven at trial.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the proposed Class, respectfully request the following relief:

1. An Order certifying the proposed Class pursuant to Civil Rule 23 and appointing Plaintiffs and undersigned counsel to represent the Class;

2. An Order expediting discovery to determine the full nature, scope and extent of the Personal Information that was compromised;

3. Equitable relief enjoining WSU from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class members' Personal Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class members;

4. Equitable relief compelling WSU to disclose to Class members fully and with

specificity the nature and type of the data compromised in the Security Breach and other information required under the laws cited herein, such that Plaintiffs and the Class can take sufficient steps to adequately protect themselves;

5. Equitable relief compelling WSU to utilize appropriate methods and policies with respect to data collection, storage and safety practices in the future;

6. Equitable relief requiring restitution and disgorgement of funds wrongfully acquired in connection with WSU's collection, storage and use of Plaintiffs' and the Class' Personal Information;

7. An Order awarding Plaintiff and Class members monetary relief, including without limitation actual, exemplary, general, punitive and statutory damages and penalties in an amount to be determined at trial;

8. An award of damages and/or statutory penalties under RCW 42.48.050 in the amount of $10,000 multiplied by the number of individuals whose Personal Information was compromised;

9. An award of costs of suit and attorneys' fees, as allowable by law;

10. An Order creating a common fund to provide adequate monetary relief for the Class;

11. An award of pre- and post-judgment interest, as provided by law;

12. Leave to amend this Complaint to conform to the evidence produced at or before trial; and

13. Such other and further relief as this Court may deem just and proper and as equity and justice may require.

Dated this 11th day of December, 2017

MIX SANDERS THOMPSON PLLC
/s/ *Michael K. Rhodes*
Michael K. Rhodes, WSBA No. 41911
1425 5th Ave., Ste. 2200
Seattle, WA 98101
Telephone: 206.971.9601
Email: mrhodes@mixsanders.com

BENDER LAW, PLLC
/s/ *Rachel R. Bender*
Rachel R. Bender, WSBA #50619
1001 Fourth Ave, Ste 3200
Seattle, WA 98154
Telephone: 206.577.7987
Email: rachel@bender-law.com

TOUSLEY BRAIN STEPHENS PLLC
By: *s/ Kim D. Stephens*
Kim D. Stephens, WSBA #11984
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
Telephone: 206.682.5600
Fax: 206.682.2992
Email: kstephens@tousley.com

AHDOOT AND WOLFSON, PC
By: *s/ Tina Wolfson*
Tina Wolfson, *Pro Hac Vice*
10728 Lindbrook Drive
Los Angeles, CA 90024-3102
Telephone: 310.474.9111
Fax: 310.474.8585
Email: twolfson@ahdootwolfson.com

Attorneys for Plaintiffs and the Class

CERTIFICATE OF SERVICE

I, Ashton Acker, certify that on the 11th day of December, 2017 I caused to be served a true and correct copy of the foregoing CONSOLIDATED CLASS ACTION COMPLAINT via the method indicated below and addressed to the following:

Rachel Bender
Bender Law PLLC
1001 4th Ave Ste 3200
Seattle, WA 98154-1003
Counsel for Plaintiffs and Class
☐Legal Messenger
☐U.S. Mail
☐Hand Delivered
☐Facsimile
☒E-mail to rachel@bender-law.com
☐Express Delivery
☒KCLGR 30 electronic service

Paul Karlsgodt
Casie Collignon
Baker Hostetler
1801 California Street Ste. 4400
Denver, CO 80202-2662
Counsel for Washington State University
☐Legal Messenger
☐U.S. Mail
☐Hand Delivered
☐Facsimile
☒E-mail to: pkarlsgodt@bakerlaw.com
ccollignon@bakerlaw.com
☐Express Delivery
☒KCLGR 30 electronic service

Kim D. Stephens
Tousley Brain Stephens PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
Counsel for Plaintiffs and Class
☐Legal Messenger
☐U.S. Mail
☐Hand Delivered
☐Facsimile
☒E-mail to kstephens@tousley.com
☐Express Delivery
☒KCLGR 30 electronic service

Randal Gainer
Baker & Hostetler LLP
999 3rd Ave. Ste. 3600
Seattle, WA 98104-4040
Counsel for Washington State University
☐Legal Messenger
☐U.S. Mail
☐Hand Delivered
☐Facsimile
☒E-mail to rgainer@bakerlaw.com
☐Express Delivery
☒KCLGR 30 electronic service

Tina Wolfson
Ahdoot and Wolfson, PC
1016 Palm Avenue
West Hollywood, CA 90069
Counsel for Plaintiffs and Class
☐Legal Messenger
☐U.S. Mail
☐Hand Delivered
☐Facsimile
☒E-mail to twolfson@ahdootwolfson.com
☐Express Delivery
☒KCLGR 30 electronic service

I certify under penalty of perjury under the laws of the state of Washington that the foregoing is true and correct.

s/Ashton Acker
Mix Sanders Thompson, PLLC
1420 Fifth Avenue, 22nd Floor
Seattle, WA 98101
Tel: 206-521-5989