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

LAKISHA LEWIS and CZARINA SLAPE, individually and on behalf of all others similarly situated, Plaintiffs v. SEATTLE HOUSING AUTHORITY, Defendant	Case No. 24-2-16171-6 **FIRST AMENDED CLASS ACTION COMPLAINT**

Plaintiffs Lakisha Lewis and Czarina Slape, ("Plaintiffs") bring this Class Action Complaint ("Complaint") against Defendant Seattle Housing Authority ("SHA") as individuals and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsels' investigation, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. This class action arises out of the recent cyberattack and data breach ("Data Breach") resulting from Seattle Housing Authority's failure to implement reasonable and industry standard data security practices to protect highly sensitive data.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

2. Seattle Housing Authority is an independent public corporation that provides long-term rental housing and rental assistance to 38,365 low-income tenants in the city of Seattle.[1]

3. As part of its operations, SHA collects, aggregates, centralizes, maintains, and stores highly sensitive personal information belonging to its employees and tenants, including, but not limited to first and last names, addresses, Social Security numbers, and financial account information (collectively, "personally identifying information" or "PII").

4. On or about November 10, 2023, SHA notified the Washington State Attorney General's Office that Personal Information from approximately 753 individuals was compromised in a data security breach of its computer servers and systems. It provided notice to those individuals that same day. On or about January 16, 2024, SHA provided written notice of this incident to 31,254 additional Washington residents.

5. Plaintiffs bring this class action lawsuit individually and on behalf of a Class of similarly situated individuals, against Defendant for its failure to protect the sensitive, confidential information of individuals in the state of Washington—including their names, Social Security numbers, addresses, and financial account information ("Personal Information").

6. As a result of Defendant's conduct and the ensuing Data Breach, Plaintiffs and the members of the proposed Class have suffered actual damages, and are at imminent risk of future harm, including identity theft and fraud that would result in monetary loss. Accordingly, Plaintiffs bring suit, on their own behalf and on behalf of a Class of all others similarly situated, to seek redress for Defendant's unlawful conduct.

[1] *About Us*, Seattle Housing Authority, https://www.seattlehousing.org/about-us (last visited July 8, 2024).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

I. PARTIES

1. Plaintiff Lakisha Lewis is an individual and is a resident of King County, Washington. Ms. Lewis became a tenant of Seattle Housing Authority approximately nineteen years ago.

2. Plaintiff Czarina Slape is an individual and is a resident of King County, Washington. Mx. Slape became a tenant of Seattle Housing Authority approximately seven years ago.

3. Defendant Seattle Housing Authority is an independent public corporation with its main office located in Seattle, Washington.

II. JURISDICTION AND VENUE

4. Jurisdiction is appropriate in this Court pursuant to RCW 2.08.010.

5. This Court has personal jurisdiction over the Seattle Housing authority because it is a municipal corporation, with its principal place of business in King County, Washington.

6. Venue is proper in this Court pursuant to RCW 4.92.010(1) and RCW 4.12.020(3) because Plaintiffs reside in King County where the cause of action arose.

III. FACTUAL BACKGROUND

7. On or about October 5, 2023, SHA "became aware that certain computer servers and systems in its environment showed signs of suspicious activity" and subsequently determined that cybercriminals "took or viewed" the sensitive personal information of approximately 31,254 of its employees and tenants between August 9 and October 25, 2023 (the "Data Breach").

8. In October 2023, the NoEscape ransomware group announced it had breached SHA servers and extracted 158 GB of data, consisting of 400,000 confidential documents. NoEscape threatened to publish the data if no one came forward to negotiate. NoEscape

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

threatened SHA, stating, "After a data leak, you will have problems on a colossal scale. . . . Lawsuits, proceedings and compensation will amount to millions of dollars. . . . Time is running out."

9. SHA has acknowledged that the affected data included personal information regarding its tenants and employees. Specifically, the information may have included first and last names, addresses, Social Security numbers, and financial account information.[2] SHA has confirmed that at least 32,000 Washingtonians' Personal Information was compromised in the data breach.[3]

10. SHA investigated the Data Breach with the assistance of "cyber incident response specialists." By October 24, 2023, SHA had confirmed that its employees' information may have been impacted; and by November 9, 2023, SHA confirmed that tenant information may have been impacted by the event.[4]

11. To date, SHA has not released any of the findings of its investigation, and it has kept the details of the Data Breach, including the vulnerabilities the attackers exploited to steal Personal Information, out of the public realm.

12. Given the sensitive nature of the Personal Information stolen in the Data Breach—including names, Social Security numbers, addresses, and financial information—hackers now have the ability to commit identity theft, financial fraud, and other identity-related fraud against Plaintiffs and Class members now and into the indefinite future.

13. As a result of the Data Breach, Plaintiffs and Class members will have to take a variety of steps to monitor for and safeguard against identity theft, and they are at a much greater

---

[2] https://agportal-s3bucket.s3.amazonaws.com/databreach/BreachA26988.pdf

[3] *Id.*

[4] *Id.*

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

risk of suffering such identity theft. In addition, these victims of the Data Breach are at a heightened risk of potentially devastating financial identity theft. As the Bureau of Justice Statistics reports, identity theft causes its victims out-of-pocket monetary losses and costs the nation's economy billions of dollars every year.[5]

14. Plaintiffs and Class members have spent and will spend time, money, and effort dealing with the fallout of the Data Breach, including purchasing credit protection services, contacting their financial institutions, checking credit reports, and spending time and effort searching for unauthorized activity.

15. The Personal Information exposed in the Data Breach is highly coveted and valuable on underground or black markets. For example, a cyber "black market" exists in which criminals openly post and sell stolen consumer information on underground internet websites known as the "dark web"—exposing consumers to identity theft and fraud for years to come. Identity thieves can use the Personal Information to: (a) create fake credit cards that can be swiped and used to make purchases as if they were the real credit cards; (b) reproduce stolen debit cards and use them to withdraw cash from ATMs; (c) commit immigration fraud; (d) obtain a fraudulent driver's license or ID card in the victim's name; (e) obtain fraudulent government benefits; (f) file a fraudulent tax return using the victim's information; (g) commit medical and healthcare-related fraud; (h) access financial accounts and records; or (i) commit any number of other frauds, such as obtaining a job, procuring housing, or giving false information to police during an arrest.

[5] *See* E. Harrell, U.S. Department of Justice, *Victims of Identity Theft, 2018* (Apr. 2021), *available at* https://bjs.ojp.gov/library/publications/victims-identity-theft-2018 (last visited July 10, 2024).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

16. Consumers are injured every time their data is stolen and placed on the dark web—even if they have been victims of previous data breaches. Not only is the likelihood of identity theft increased, but the dark web is not like Google or eBay. It is comprised of multiple and discrete repositories of stolen information. Each data breach puts victims at risk of having their information uploaded to different dark web databases and viewed and used by different criminal actors.

17. Exposure of this information to the wrong people can have serious consequences. Identity theft can have ripple effects, which can adversely affect the future financial trajectories of victims' lives. For example, the Identity Theft Resource Center reports that respondents to their surveys in 2013–2016 described that the identity theft they experienced affected their ability to get credit cards, obtain loans, such as student loans or mortgages, rent an apartment or find housing.[6] For some victims, this could mean the difference between going to college or not, becoming a homeowner or not, or having to take out a high interest payday loan versus a lower-interest loan.

18. The unauthorized disclosure of Social Security numbers can be particularly damaging because Social Security numbers cannot easily be replaced. In order to obtain a new number, a person must prove, among other things, that he or she continues to be disadvantaged by the misuse. Thus, under current rules, no new number can be obtained until damage has been done. Furthermore, as the Social Security Administration warns:

> A new number probably will not solve all your problems. This is because other governmental agencies (such as the Internal Revenue Service and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Also, because credit

[6] Identity Theft Resource Center, *The Aftermath 2017*, https://www.idtheftcenter.org/images/page-docs/Aftermath_2017.pdf (last visited July 10, 2024).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

> reporting companies use the number, along with other Personal Information, to identify your credit record, using a new number will not guarantee you a fresh start. This is especially true if your other Personal Information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you will not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit card information is not associated with the new number, the absence of any credit history under the new number may make it more difficult for you to get credit.[7]

19. According to the Attorney General of the United States, Social Security numbers "can be an identity thief's most valuable piece of consumer information."[8] Indeed, as explained recently: "The ubiquity of the SSN as an identifier makes it a primary target for both hackers and identity thieves. . . . When data breaches expose SSNs, thieves can use these numbers—usually combined with other pieces of data—to impersonate individuals and apply for loans, housing, utilities, or government benefits. Additionally, this information may be sold on the black market to other hackers."[9]

20. As the result of the Data Breach, Plaintiffs and Class members are likely to suffer economic loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

---

[7] Social Security Administration, *Identity Theft and Your Social Security Number* (June 2017), available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited July 10, 2024).

[8] *Fact Sheet: The Work of the President's Identity Theft Task Force*, DOJ 06-636, 2006 WL 2679771 (Sep. 19, 2006), available at https://www.justice.gov/archive/opa/pr/2006/September/06_ag_636.html (last visited July 10, 2024).

[9] Daniel J. Marcus, *The Data Breach Dilemma: Proactive Solutions for Protecting Consumers' Personal Information*, 68 Duke L.J. 555, 564–65 (2018), available at https://scholarship.law.duke.edu/dlj/vol68/iss3/3 (last visited July 10, 2024).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

a. losing the inherent value of their Personal Information;

b. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

c. costs associated with purchasing credit monitoring, credit freezes, and identity theft protection services;

d. lowered credit scores resulting from credit inquiries following fraudulent activities;

e. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including discovering fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with the repercussions of the Data Breach; and

f. the continued imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Personal Information being in the possession of one or many unauthorized third parties.

21. Even in instances where a consumer is reimbursed for a financial loss due to identity theft or fraud, that does not make that individual whole again, as there is typically significant time and effort associated with seeking reimbursement that is not refunded. The Department of Justice's Bureau of Justice Statistics found that identity theft victims "spent an average of 14 hours resolving associated financial and credit problems."[10]

22. There may also be a significant time lag between when personal information is stolen and when it is actually misused. According to the GAO, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting

[10] E. Harrell, U.S. Department of Justice, *Victims of Identity Theft, 2018* (Apr. 2021), *available at* https://bjs.ojp.gov/library/publications/victims-identity-theft-2018 (last visited July 10, 2024).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

from data breaches cannot necessarily rule out all future harm.[11]

D. Plaintiffs' Individual Allegations

1. Lakisha Lewis

23. Plaintiff Lakisha Lewis applied to rent an apartment owned by Seattle Housing Authority approximately nineteen years ago. As part of Seattle Housing Authority's requirements for prospective tenants, Plaintiff Lewis was required to provide sensitive Personal Information, including her Social Security number, address, and financial information.

24. On or about January 16, 2024, SHA sent Plaintiff Lewis a letter informing her that her sensitive Personal Information may have been obtained by an unauthorized person.

25. Plaintiff Lewis has already experienced the effects of the Data Breach. Numerous attempts have been made to place fraudulent charges on her debit card. Ms. Lewis has also been subjected to many spam calls and text messages.

26. Given the highly sensitive nature of the information stolen in the Data Breach, Plaintiff Lewis remains at a substantial and imminent risk of future harm, including identity theft. Plaintiff Lewis will be required to expend time and effort monitoring her financial accounts and credit reports.

2. Czarina Slape

27. Plaintiff Czarina Slape applied to rent an apartment owned by Seattle Housing Authority approximately seven years ago. As part of Seattle Housing Authority's requirements for prospective tenants, Plaintiff Slape was required to provide sensitive Personal Information, including her Social Security number, address, and financial information.

---

[11] U.S. Government Accountability Office Report to Congressional Requesters, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), http://www.gao.gov/new.items/d07737.pdf (last visited July 10, 2024).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

28. On or about January 16, 2024, SHA sent Plaintiff Slape a letter informing them that their sensitive Personal Information may have been obtained by an unauthorized person.

29. Plaintiff Slape has already experienced the effects of the Data Breach. Ms. Slape has been subjected to many spam calls and text messages.

30. Given the highly sensitive nature of the information stolen in the Data Breach, Plaintiff Slape remains at a substantial and imminent risk of future harm, including identity theft. Plaintiff Slape will be required to expend time and effort monitoring their financial accounts and credit reports.

IV. CLASS ACTION ALLEGATIONS

31. Plaintiffs bring this action individually and on behalf of a class (the "Class") preliminarily defined as:

> All individuals whose personal information was compromised in the data breach disclosed by the Seattle Housing Authority on or about November 10, 2023 and January 16, 2024.

Excluded from the Class are Defendant; any agent, affiliate, parent, or subsidiary of the Defendant; any entity in which the Defendant has a controlling interest; any officer or director of the Defendant; any successor or assign of the Defendant; and any Judge to whom this case is assigned as well as his or her staff and immediate family.

32. Plaintiffs reserve the right to amend the class definition.

33. This action satisfies the numerosity, commonality, typicality, and adequacy requirements of CR 23.

a) **Numerosity.** Plaintiffs are representatives of the proposed Class reportedly consisting of at least 32,000 members—far too many to join in a single action.

b) **Ascertainability.** Class members are readily identifiable from information in Defendants' possession, custody, or control.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

c) **Typicality.** Plaintiff's claims are typical of Class members' claims as each arises from the same Data Breach, the same alleged negligence of and/or statutory violations by Defendant, and the same unreasonable manner of notifying individuals regarding the Data Breach.

d) **Adequacy.** Plaintiffs will fairly and adequately protect the interests of the proposed Class. Their interests do not conflict with Class members' interests and they have retained counsel experienced in complex class action litigation and data privacy to vigorously prosecute this action on behalf of the Class, including in the capacity as lead counsel.

e) **Commonality.** Plaintiff's 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:

A. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

B. Whether Defendant's conduct was negligent;

C. Whether Plaintiffs and the Class are entitled to damages, treble damages, and/or injunctive relief.

34. 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 an individual member, and a class action is superior to individual litigation or any other available methods for the fair and efficient

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

adjudication of the controversy. The damages available to an individual plaintiff are insufficient to make litigation addressing Defendant's privacy practices economically feasible in the absence of the class action procedure.

35. In the alternative, class certification is appropriate because Defendant 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.

V. FIRST CLAIM FOR RELIEF
Negligence
On Behalf of Plaintiffs and the Putative Class

36. Plaintiffs incorporate by reference all foregoing factual allegations.

37. Defendant SHA collected and maintained the Personal Information of tens of thousands of Washingtonians. Those individuals were required to provide their Personal Information to SHA to receive employment, housing assistance or a low-income rental. As a result, they had a reasonable expectation that SHA would protect their Personal Information.

38. It was reasonably foreseeable to Defendant SHA that its failure to implement and maintain reasonable security procedures and practices would leave the sensitive information in its systems vulnerable to breach and could thus expose the owners of that information to harm.

39. Furthermore, given the known risk of major data breaches, Plaintiffs and the Class members are part of a well-defined, foreseeable, finite, and discernible group that was at high risk of having their Personal Information stolen.

40. Defendant SHA owed a duty to Plaintiffs and members of the Class to ensure that its systems and networks—and the personnel responsible for them—adequately protected their Personal Information.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

41. Defendant SHA's duty of care arose as a result of Defendant's knowledge that individuals trusted SHA to protect their confidential data. Only SHA was in a position to ensure that its own protocols were sufficient to protect against the harm to Plaintiffs and members of the Class from a data breach of its own systems.

42. In addition, Defendant SHA had duties to use reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

43. Defendant SHA also had duties to use reasonable care in protecting confidential data because it committed to comply with industry standards for the protection of Personal Information.

44. Defendant SHA knew, or should have known, of the vulnerabilities in its systems, and the importance of adequate security for sensitive data stored in those systems.

45. By using an inadequately secure system for the transfer and storage of sensitive data, Defendant SHA breached its duties to Plaintiffs and the Class.

46. Plaintiffs and Class members have suffered harm as a result of Defendant SHA's negligence. These victims suffered diminished value of their sensitive information. Plaintiffs and members of the Class also lost control over their exposed Personal Information, which subjected each of them to a greatly enhanced risk of identity theft, credit and bank fraud, Social Security fraud, tax fraud, and a myriad of other types of fraud and theft, in addition to the time and expenses spent mitigating those injuries and preventing further injury.

47. Consistent with RCW 4.92.100, on May 14, 2024, Plaintiff Lewis, on her own behalf and on behalf of the Class she seeks to represent, presented a Tort Claim Form to Risk

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Management at SHA. More than sixty calendar days have elapsed after her claims were presented. *See* RCW 4.92.100.

48. Consistent with RCW 4.92.100, on July 12, 2024, Plaintiff Slape, on their own behalf and on behalf of the Class they seek to represent, also presented a Tort Claim Form to Risk Management at SHA. More than sixty calendar days have elapsed after their claims were presented. *See* RCW 4.92.100.

VI. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs make the following prayer for relief, individually and on behalf of the proposed Class:

A. An order certifying the proposed Class pursuant to Civil Rule 23 and appointing Plaintiffs and their counsel to represent the Class;

B. An order awarding Plaintiffs and Class members monetary relief, including actual damages;

C. Equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein and compelling Defendant to utilize appropriate methods and policies with respect to maintaining the security of its systems;

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

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

F. Leave to amend this Complaint to conform to the evidence produced at trial; and

G. Such other and further relief as this Court may deem just and proper.

//

//

//

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Dated: September 11, 2024

Respectfully submitted,

/s/ Kaleigh N. Boyd

Kaleigh N. Boyd, WSBA #52684
TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, WA 98101
Telephone: 206-682-5600
Facsimile: 206-682-2992
kboyd@tousley.com