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

SAMUEL ZEWDY EMANO, MONTE SUNDREA HOLT, SARAH RAINBOW CARDENAS, JOANN TRUSSELL, TARA HAMLIN and DAVID BELTRAN, individually and on behalf of all others similarly situated, Plaintiffs, v. PORT OF SEATTLE, Defendant.	No. 25-2-11500-3 SEA **CONSOLIDATED CLASS ACTION COMPLAINT**

Plaintiffs Samuel Zewdy Emano, Monte Sundrea Holt, Sarah Rainbow Cardenas, Joann Trussell, Tara Hamlin, and David Beltran, by and through undersigned counsel ("Plaintiffs"), bring this Consolidated Class Action Complaint ("Complaint") against the Port of Seattle ("Port" or "Defendant"), individually and on behalf of all others similarly situated. Plaintiffs allege, upon personal knowledge as to their own actions and their counsels' investigation, and on information and belief as to all other matters, as follows:

SUMMARY OF ACTION

1. This case arises from a data breach at the Port of Seattle, a municipal corporation that "runs a world-class seaport and international airport,"[1] including Seattle-Tacoma

[1] *Commission*, THE PORT OF SEATTLE, https://www.portseattle.org/about/commission (last accessed June 5, 2025).

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

International Airport[2] ("SeaTac Airport") and Fishermen's Terminal.[3]

2. In or around August 24, 2024, the Port was the target of a ransomware attack by a criminal group, Rhysida (the "Data Breach"). As a result of the attack, sensitive personal information of nearly 148,000 individuals—primarily current and former Port and airport employees and contractors—was exfiltrated.

3. The compromised data included first and last names, dates of birth, Social Security numbers, driver's license or other government-issued identification numbers, and, in some cases, medical information (collectively, "Private Information").

4. Rhysida has since made some of the data available publicly.[4]

5. Although the Port identified the breach in August 2024, it did not begin notifying affected individuals until April 2, 2025—more than seven months later.

6. To date, the Private Information remains in the hands of cybercriminals and is susceptible to misuse, including identity theft and related fraud.

7. The Data Breach was a direct result of the Port's failure to implement reasonable cybersecurity safeguards to protect its data systems against unauthorized intrusions.

8. Armed with the Private Information obtained in the Data Breach, cybercriminals can open financial accounts, take out loans, obtain government benefits, file fraudulent tax returns, receive driver's licenses with another person's photograph, and provide false information to police during an arrest.

9. Put differently, as a result of the Data Breach, Plaintiffs and Class Members suffered concrete harm, including but not limited to: (i) invasion of privacy; (ii) theft of their

---

[2] *Seattle-Tacoma International Airport*, PORT OF SEATTLE, https://www.portseattle.org/sea-tac (last accessed June 5, 2025).

[3] *Fishermen's Terminal*, PORT OF SEATTLE, https://www.portseattle.org/maritime/fishermen-terminal (last accessed June 5, 2025).

[4] Security Week, *Port of Seattle Says 90,000 People Impacted by Ransomware Attack,* available at https://www.securityweek.com/port-of-seattle-says-90000-people-impacted-by-ransomware-attack// (last accessed June 5, 2025).

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

Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of the benefit of the bargain; (vi) nominal damages; and (vii) the ongoing and increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and subject to further unauthorized disclosures due to Defendant's failure to implement adequate safeguards.

10. In sum, this action seeks to remedy the harm suffered by Plaintiffs and Class Members as a result of the August 24, 2024 Data Breach, and address the present and pressing need for meaningful improvements to the Port's data security practices so that individuals' personal information is no longer left vulnerable to unauthorized access or disclosure.

JURISDICTION AND VENUE

11. The Superior Court of King County has personal jurisdiction over the Port because it conducts substantial business in King County, Washington, and maintains its principal office within the county.

12. Venue is proper in King County Superior Court under RCW 4.12.025 because a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in King County.

PARTIES

13. Plaintiff Joann Trussell is a resident and citizen of King County, Washington.

14. Plaintiff David Beltran is a resident and citizen of King County, Washington.

15. Plaintiff Tara Hamlin is a resident and citizen of Snohomish County, Washington.

16. Plaintiff Samuel Zewdy Emano is a resident and citizen of King County, Washington.

17. Plaintiff Monte Sundrea Holt is a resident and citizen of King County, Washington.

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

18. Plaintiff Sarah Rainbow Cardenas is an individual and resident of King County, Washington.

19. The Port of Seattle is a municipal corporation organized under the laws of the State of Washington, with its principal office located in King County, Washington.

FACTUAL ALLEGATIONS

Defendant's Business

20. Established in 1911, the Port of Seattle is a municipal corporation responsible for owning and managing Seattle-Tacoma International Airport and Fisherman's Terminal.[5] The Port also owns two cruise ship terminals, a grain terminal, real estate assets, and, through its partnership with the Northwest Seaport Alliance, marine cargo terminals.[6]

21. Plaintiffs and Class Members are current and former employees and contractors of the Port and airport.

22. In the course of their relationship with Defendant, Plaintiffs and Class Members provided sensitive personal information, including, but not limited to: first and last name, date of birth, Social Security number, driver's license or other government identification card number, and medical information.[7]

23. Upon information and belief, Defendant represented that it would safeguard the Private Information and comply with applicable data privacy and security obligations, including those imposed by federal and state law, as well as its own internal policies.

24. Indeed, Plaintiffs and Class Members relied on Defendant to keep their Private Information secure, reasonably expecting that such sensitive data, particularly government-issued identifiers and medical information, would be protected against unauthorized access and disclosure.

---

[5] PORT OF SEATTLE, https://www.portseattle.org (June 5, 2025).

[6] *Id.*

[7] *Port Cyberattack, Archive*, PORT OF SEATTLE, https://www.portseattle.org/news/port-cyberattack-archive (last accessed June 5, 2025).

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

The Data Breach

25. On or about September 13, 2024, Defendant issued a public notice stating that, on August 24, 2024, it had identified system outages consistent with a cyberattack. Defendant confirmed that the incident was a ransomware attack perpetrated by a criminal organization known as The Rhysida Group[8]--a well-known group for encrypting data on victims' computer systems and threatening to publicly release the stolen information unless a ransom is paid.[9]

26. In response, Defendant engaged forensic specialists and law enforcement to investigate the breach and assist with data recovery. The investigation determined that the unauthorized actor "accessed and downloaded some personal information from Port systems, primarily legacy."[10]

27. The system outages were caused by a ransomware attack on Defendant's system, and the outages persisted from August 24, 2024, through August 31, 2024, which had significant impacts on travelers and airport operations. Thousands of travelers experienced delays and disruptions at SeaTac Airport as critical systems, including internet, phone, and email, were taken offline. These outages led to long lines and manual processing of passenger information, particularly affecting international travelers.[11]

28. While Defendant posted an announcement on its website acknowledging the system outages on the same day of the incident—at or around 9:45 a.m. PST on August 24, 2024—and continued to provide updates until most systems were restored on August 31, 2024,

---

[8] September 13, 2024, Update on Cyberattack, PORT OF SEATTLE, available at https://www.portseattle.org/news/port-cyberattack-archive (last accessed June 5, 2025)

[9] CISA, FBI, and MS-ISAC Release Advisory on Rhysida Ransomware, AMERICA'S CYBER DEFENSE AGENCY, https://www.cisa.gov/news-events/alerts/2023/11/15/cisa-fbi-and-ms-isac-release-advisory-rhysida-ransomware (last visited June 5, 2025).

[10] *Id.*

[11] KOMO News Staff, *Thousands of travelers, airport operations impacted by Port of Seattle cyberattack*, KOMONEWS, (Aug. 25, 2024), https://komonews.com/news/local/port-of-seattle-hit-by-potential-cyberattack-still-impacting-airport-operations-cyber-attack-airport-flying-airplanes-seattle-tacoma-sea-travel-sunday-operations-urges-outage-airlines (last visited May 12, 2025).

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

Defendant failed to promptly disclose any information regarding the Data Breach.[12]

29. On September 13, 2024—approximately three weeks after the cyberattack—Defendant made its first public statement confirming the occurrence of the Data Breach caused by a ransomware attack on August 24, 2024, consistent with the previously reported system outages. However, its public announcement still failed to disclose the types of information compromised, the individuals impacted, or the total number of affected persons.[13] As a result, the public remained largely uninformed and confused about the nature and extent of the incident, intensifying their anxiety and depriving them of an early opportunity to mitigate the repercussions of the Data Breach.

30. Defendant also publicly stated it declined to pay the ransom demand, making it likely that the sensitive PII of Plaintiffs and Class Members has already been, or will soon be, publicly disclosed.[14]

31. In a ransomware attack the attackers use software to encrypt data on a compromised network, rendering it unusable and demanding payment to restore control over the network.[15]

32. Companies should treat ransomware attacks as any other data breach incident because ransomware attacks don't just hold networks hostage, "ransomware groups sell stolen data in cybercriminal forums and dark web marketplaces for additional revenue."[16] As cybersecurity expert Emisoft warns, "[a]n absence of evidence of exfiltration should not be construed to be evidence of its absence . . . the initial assumption should be that data may have been exfiltrated."

---

[12] *Supra* note 7.

[13] *Id.*

[14] *Id.*

[16] *Ransomware: The Data Exfiltration and Double Extortion Trends*, *available at* https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends

[16] *Ransomware: The Data Exfiltration and Double Extortion Trends*, *available at* https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends

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

33. An increasingly prevalent form of ransomware attack is the "encryption+exfiltration" attack in which the attacker encrypts a network and exfiltrates the data contained within.[17] In 2020, over 50% of ransomware attackers exfiltrated data from a network before encrypting it.[18] Once the data is exfiltrated from a network, its confidential nature is destroyed and it should be "assume[d] it will be traded to other threat actors, sold, or held for a second/future extortion attempt."[19] And even where companies pay for the return of data attackers often leak or sell the data regardless because there is no way to verify that copies of the data are destroyed.[20]

34. Indeed, Rhysida has since made some of the data available publicly.[21]

35. It was not until around April 2, 2025, more than seven months after the Data Breach initially happened, that Defendant began to notify Plaintiffs and Class Members of the Data Breach (the "Notice Letter") that:

> On August 24, 2024, the Port identified system outages consistent with a cyberattack. The Port promptly initiated its incident response processes.
>
> . . .
>
> The threat actors accessed and downloaded some personal information from Port systems, primarily legacy ones used for employee, contractor and parking data. The Port holds very little information about airport or maritime passengers, and systems processing payments were not affected.
>
> We have determined that around August 24, 2024, the threat actors accessed and downloaded some personal information from the Port networks, mostly for current and former Port and other airport employees and contractors. Within these downloaded files, the Port identified the following personal information that may have been involved for impacted individuals: first and last name, date of birth, Social Security number (or last four digits of Social Security number), driver's

[17] *The chance of data being stolen in a ransomware attack is greater than one in ten*, *available at* https://blog.emsisoft.com/en/36569/the-chance-of-data-being-stolen-in-a-ransomware-attack-is-greater-than-one-in-ten/

[18] 2020 Ransomware Marketplace Report, available at https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report

[19] *Id*.

[20] *Id*.

[21] *Supra* note 4.

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

> license or other government identification card number, and medical information.[22]

36. Defendant's public statements and Notice Letter amount to no real disclosure at all, as they fail to adequately inform Plaintiffs and Class Members with any degree of specificity about the nature, scope, and severity of the Data Breach. For example, omitted from the Notice Letter are details regarding the root cause of the Data Breach, the specific vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. Without this information, Plaintiffs' and Class Members' ability to mitigate the resulting harm is severely diminished.

37. Moreover, in its Notice Letter, Defendant fails to specify whether Defendant contacted Class Members to determine if their information had been misused, whether Defendant was interested in learning about any misuse, or whether it created a way for Class Members to report such misuse.

38. However, upon information and belief, before the Data Breach, Defendant made promises and representations to Plaintiffs and Class Members that the PII collected as part of Defendant's business operations would be kept safe, confidential, and that the privacy of that information would be maintained.

39. For instance, Defendant explicitly provides the following notice on its website for consumers using their parking reservation system:

> To process a reservation, the Port will collect and store personal information including your name, address, phone number, email, and vehicle license plate. […]
>
> The Port will use commercially reasonable technology and security policies, rules, and measures to protect your personal information that the Port has received from you from unauthorized access and improper use. The Port will not sell or rent your personal information to third parties.[23]

---

[22] The "Notice Letter". A sample copy is available at https://www.portseattle.org/news/port-cyberattack-archive (last accessed June 5, 2025).

[23] *See Terms and Conditions*, SEATTLE-TACOMA INTERNATIONAL AIRPORT, available at https://reservesea.portseattle.org/book/SEA/Content/Terms+and+Conditions (last visited June 5, 2025).

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

40. Furthermore, Defendant had obligations under the Federal Trade Commission Act (FTCA), contract, common law, and industry standards to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

41. However, Defendant failed to implement reasonable security measures to protect Plaintiffs' and Class Members' Private Information, resulting in its exposure.

42. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information has been, or is likely to be, sold on the dark web, consistent with the *modus operandi* of cybercriminals—an outcome Defendant itself acknowledged was likely in its public statement issued on September 13, 2024.[24]

The Data Breach Was Foreseeable

43. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in industries holding significant amounts of personally identifiable information ("PII") preceding the date of the breach.

44. At all relevant times, Defendant knew, or should have known, that Plaintiffs' and Class Members' Private Information was a target for malicious actors. Despite such knowledge, Defendant failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiffs' and Class Members' Private Information from cyberattacks that Defendant should have anticipated and guarded against.

45. The targeted attack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the Private Information of employees like Plaintiffs and Class Members.

Defendant Fails to Comply with FTC Guidelines

46. The Federal Trade Commission ("FTC") has promulgated numerous guides for

[24] *Port Cyberattack, Archive*, PORT OF SEATTLE, https://www.portseattle.org/news/port-cyberattack-archive (last accessed June 5, 2025).

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

businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should factor into all business decision-making.

47. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[25] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[26]

48. The FTC further recommends that companies not maintain PII longer than necessary for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

49. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

50. Defendant failed to properly implement basic data security practices.

---

[25] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited March 31, 2025).

[26] *Id*.

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

51. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to employees' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

52. Defendant was at all times fully aware of its obligation to protect the Private Information of current and former employees. Defendant was also aware of the significant repercussions that would result from its failure to do so.

53. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

54. The above frameworks are applicable industry standards for employers, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the data breach.

55. A victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into

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

disclosing additional confidential or personal information through means such as spam phone calls, text messages, or phishing emails.

56. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[27]

57. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

58. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.

59. Moreover, theft of Private Information is gravely serious because Private Information is an extremely valuable property right.[28]

60. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this

---

[27] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited March 31, 2025).

[28] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3–4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

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

obvious risk-to-reward analysis illustrates beyond doubt that Private Information has considerable market value.

61. It must also be noted there may be a substantial time lag—measured in years—between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

62. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

63. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiffs and Class Members are at an increased risk of fraud and identity theft for their lifetimes.

64. Thus, Plaintiffs and Class Members must vigilantly monitor their financial and medical accounts for their lifetimes.

65. Private Information can sell for as much as $363 per record according to the Infosec Institute.[29] Private Information is particularly valuable because criminals can use it to target victims with frauds and scams. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

66. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[30] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[31] Each of these fraudulent

[29] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited March 31, 2025).

[30] *Identity Theft and Your Social Security Number*, Social Security Administration (2018), available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited March 31, 2025).

[31] *Id*.

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

activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

67. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

68. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[32]

69. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[33]

70. There is also an active and robust legitimate marketplace for PII. In 2019, the data brokering industry was worth roughly $200 billion.[34] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.

---

[32] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited March 31, 2025).

[33] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited March 31, 2025).

[34] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/

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

71. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and its rarity has been lost, thereby causing additional loss of value.

72. Defendant breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately encrypt or redact Private Information stored in internat accessible locations;

c. Failing to employ multi-factor authentication and to limit access to Private Information to only essential employees;

d. Failing to properly monitor its own data security systems for existing intrusions or for large volumes of data being transferred.

e. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;

f. Failing to train its employees in the proper handling of systems containing Private Information and maintain adequate security practices;

g. Failing to ensure the confidentiality and integrity of electronic PII it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

h. Failing to implement technical policies and procedures for electronic information

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

systems that maintain electronic PII to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

i. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

j. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

k. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PII in violation of 45 C.F.R. § 164.306(a)(2);

l. Failing to protect against reasonably anticipated uses or disclosures of electronic PII that are not permitted under the privacy rules regarding individually identifiable information in violation of 45 C.F.R. § 164.306(a)(3);

m. Failing to ensure compliance with HIPAA security standard rules by its workforce in violation of 45 C.F.R. § 164.306(a)(4);

n. Failing to train all members of its workforce effectively on the policies and procedures regarding PII as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of PII, in violation of 45 C.F.R. § 164.530(b);

o. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;

p. Failing to adhere to industry standards for cybersecurity as discussed above; and

q. Otherwise breaching its duties and obligations to protect Plaintiffs' and Class Members' Private Information.

73. Defendant negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access Defendant's computer

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

network and systems which contained unsecured and unencrypted Private Information.

74. Accordingly, as outlined below, Plaintiffs and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiffs and the Class Members also lost the benefit of the bargain they made with Defendant.

Defendant's Response to the Data Breach is Inadequate to Protect Plaintiffs and the Class

75. Defendant failed to inform Plaintiffs and Class Members of the Data Breach in time for them to protect themselves from identity theft.

76. Defendant stated that it discovered the Data Breach in August 2024. However, Defendant did not start *directly* notifying affected individuals until April 2025, eight months later. Even then, Defendant provided only vague information about exactly what types of Private Information were accessed and Defendant failed to disclose how long cybercriminals had access to its network. As a result, Plaintiffs and Class Members are unsure as to the scope of information that was compromised and the risks they face.

77. Defendant's failure to timely notify the victims of its Data Breach meant that Plaintiffs and Class Members were unable to take affirmative measures to prevent or mitigate the resulting harm.

Plaintiffs' and Class Members' Damages

78. Given the sensitivity of the Private Information involved in this Data Breach, Plaintiffs and Class Members have all suffered damages and will face a substantial risk of additional injuries for the rest of their lives. Yet, to date, Defendant has merely offered to provide victims of the Data Breach with limited, abbreviated subscriptions to identity monitoring services. This does nothing to compensate Plaintiffs or Class Members for many of the injuries they have already suffered. Nor will it prevent additional harm from befalling Plaintiffs and Class Members as a result of the Data Breach. And at the conclusion of these limited subscriptions, victims will be required to pay for such services out of their own pockets.

79. Plaintiffs and Class Members have been damaged by the compromise of their

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

Private Information in the Data Breach.

80. Plaintiffs' and Class Members' Private Information was compromised in the Data Breach and are now in the hands of the cybercriminals who accessed Defendant's computer system.

81. Since being notified of the Data Breach, Plaintiffs have spent time dealing with the impact of the Data Breach, valuable time Plaintiffs otherwise would have spent on other activities, including but not limited to work and/or recreation.

82. Due to the Data Breach, Plaintiffs anticipate spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. This includes changing passwords, cancelling credit and debit cards, and monitoring their accounts for fraudulent activity.

83. Plaintiffs' and Class Members' Private Information was compromised as a direct and proximate result of the Data Breach.

84. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been placed at a present, imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

85. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been forced to spend time dealing with the effects of the Data Breach.

86. Plaintiffs and Class Members face a substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

87. Plaintiffs and Class Members face a substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiffs and Class Members.

88. Plaintiffs and Class Members may also incur out-of-pocket costs for protective

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

measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

89. Plaintiffs and Class Members also suffered a loss-of-value in their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

90. Plaintiffs and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiffs and Class Members were undercompensated for employment, as transmitting their Private Information to Defendant was intended to be accompanied by adequate data security that complied with industry standards but was not. Part of the compensation Plaintiffs and Class Members should have received from Defendant was adequate security of its computer system(s) to protect Plaintiffs' and Class Members' Private Information. Thus, Plaintiffs and the Class Members were not fully compensated and did not get the value of the services to which they agreed.

91. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time monitoring their accounts and sensitive information for misuse.

92. Plaintiffs and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

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

e. Contacting financial institutions and closing or modifying financial accounts; and

f. Closely reviewing and monitoring Social Security number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for the rest of their lives.

93. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including, but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password-protected.

94. Further, as a result of Defendant's conduct, Plaintiffs and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life, including what ailments they suffer, whether physical or mental—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

95. As a direct and proximate result of Defendant's actions and inactions, Plaintiffs and Class Members have suffered anxiety, emotional distress, loss of time, loss of privacy, and are at an increased risk of future harm.

Plaintiff Joann Trussell's Experience

96. On information and belief, at time of the Data Breach—on or about August 24, 2024—Defendant retained Plaintiff Joann Trussell's (for purposes of this section, "Plaintiff") Private Information in its system, including her name, Social Security number, and date of birth. Plaintiff has never worked for Defendant and is not aware of how Defendant obtained her Private Information.

97. Plaintiff received the Notice of Data Breach Letter by U.S. mail from Defendant. According to her Notice Letter, Plaintiff's Private Information, including her name, Social Security number, and date of birth, was improperly accessed and obtained by unauthorized third

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

parties. She is uncertain which parts of her less private information were breached since Defendant indicated in its notices that names, addresses, and demographic information were included in the breach.

98. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, monitoring her financial accounts, changing passwords, and implementing extra security on her computers. Plaintiff spent significant time dealing with the Data Breach, which is valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

99. Plaintiff suffered actual injury from having her Private Information compromised as a result of the Data Breach, including, but not limited to: (i) invasion of privacy; (ii) theft of her Private Information; (iii) lost or diminished value of her Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) statutory damages; (vii) nominal damages; and (viii) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

100. Following the Data Breach, Plaintiff has experienced a spike in spam or fraudulent phone calls, text messages, and emails.

101. Since the Data Breach, Plaintiff has received alerts from publicly available credit monitoring products that her Private Information has been found on the dark web.

102. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the Data Breach's occurrence.

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

103. Plaintiff anticipates spending considerable time on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

104. As a result of the Data Breach, Plaintiff is at present risk and will continue to be at increased risk of identity theft and fraud for her lifetime.

105. Plaintiff has a continuing interest in ensuring that her Private Information which, on information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

106. On or about April 11, 2025, Plaintiff sent a Notice of Tort Claim to Defendant consistent with RCW 4.96.020.

107. On May 12, 2025, Defendant denied Plaintiff's Notice of Tort Claim.

Plaintiff David Beltran's Experience

108. Plaintiff David Beltran (for purposes of this section, "Plaintiff") provided Defendant with his sensitive Private Information as a condition of becoming a contractor of Defendant. Plaintiff received Notice of the Data Breach around April 3, 2025, informing him that his sensitive information was part of Defendant's Data Breach, including his "Full Name; Full Birth Date; Partial Social Security Number."

109. Since becoming aware of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, monitoring his financial accounts, changing passwords, and implementing extra security on his computers. Plaintiff spent significant time dealing with the Data Breach, which is valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

110. Plaintiff suffered actual injury from having his Private Information compromised as a result of the Data Breach, including, but not limited to: (i) invasion of privacy; (ii) theft of his Private Information; (iii) lost or diminished value of his Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data

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

Breach; (v) loss of benefit of the bargain; (vi) statutory damages; (vii) nominal damages; and (viii) the continued and certainly increased risk to his Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

111. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

112. Plaintiff anticipates spending considerable time on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

113. As a result of the Data Breach, Plaintiff is at present risk and will continue to be at increased risk of identity theft and fraud for his lifetime.

114. Plaintiff has a continuing interest in ensuring that his Private Information which, on information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

115. On or about April 15, 2025, Plaintiff sent a Notice of Tort Claim to Defendant consistent with RCW 4.96.020.

116. On May 12, 2025, Defendant denied Plaintiff's Notice of Tort Claim.

Plaintiff Tara Hamlin's Experience

117. Plaintiff Tara Hamlin (for purposes of this section, "Plaintiff") was a prospective employee of Defendant. At the time of the Data Breach—on or about August 24, 2024—Defendant retained Plaintiff's full name, date of birth, contact information, Social Security number, and other Private Information in its system.

118. In order to be considered for employment by Defendant, Plaintiff was required to provide her Private Information to Defendant.

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

119. Plaintiff received the Notice of Data Breach Letter by U.S. mail from Defendant. According to her Notice Letter, Plaintiff's Private Information, including her name, Social Security number, and date of birth, was improperly accessed and obtained by unauthorized third parties. She is uncertain which parts of her less private information were breached since Defendant indicated in its notices that names, addresses, and demographic information were included in the breach.

120. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, monitoring her financial accounts, changing passwords, and implementing extra security on her computers. Plaintiff spent significant time dealing with the Data Breach, which is valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

121. Plaintiff suffered actual injury from having her Private Information compromised as a result of the Data Breach, including, but not limited to: (i) invasion of privacy; (ii) theft of her Private Information; (iii) lost or diminished value of her Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) statutory damages; (vii) nominal damages; and (viii) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

122. Following the Data Breach, Plaintiff has suffered a substantial uptick in spam calls, text messages, and emails.

123. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the Data Breach's occurrence.

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

124. Plaintiff anticipates spending considerable time on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

125. As a result of the Data Breach, Plaintiff is at present risk and will continue to be at increased risk of identity theft and fraud for her lifetime.

126. Plaintiff has a continuing interest in ensuring that her Private Information, which, on information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

127. On or about April 9, 2025, Plaintiff sent a Notice of Tort Claim to Defendant consistent with RCW 4.96.020.

128. On or about May 12, 2025, Defendant denied Plaintiff Hamlin's claim.

Plaintiff Samuel Zewdy Emano's Experience

129. Plaintiff Samuel Zewdy Emano (for purposes of this section, "Plaintiff") is a contractor who provides licensed limousine transportation services at SeaTac Airport, a facility operated by Defendant.

130. To provide transportation service at SeaTac Airport, Defendant required Plaintiff to annually renew an authorization sticker, a process that mandated the submission of Plaintiff's sensitive and confidential PI.

131. During Plaintiff's most recent renewal process, he was informed that he had an outstanding ticket that needed to be resolved before the renewal could be completed. However, when he attempted to address the issue, the system showed no record of the ticket. Through communication with Defendant's representatives in or around March 2025, Plaintiff was informed of the Data Breach and that the resulting system outage was the reason the ticket could not be located or resolved.

132. Since becoming aware of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, monitoring his financial accounts, changing passwords, and implementing extra security on his computers. Plaintiff spent

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

significant time dealing with the Data Breach, which is valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

133. Plaintiff suffered actual injury from having his Private Information compromised as a result of the Data Breach, including, but not limited to: (i) invasion of privacy; (ii) theft of his Private Information; (iii) lost or diminished value of his Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) statutory damages; (vii) nominal damages; and (viii) the continued and certainly increased risk to his Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

134. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

135. Plaintiff anticipates spending considerable time on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

136. As a result of the Data Breach, Plaintiff is at present risk and will continue to be at increased risk of identity theft and fraud for his lifetime.

137. Plaintiff has a continuing interest in ensuring that his Private Information which, on information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

138. On or about April 4, 2025, Plaintiff sent a Notice of Tort Claim to Defendant consistent with RCW 4.96.020.

139. On May 12, 2025, Defendant denied Plaintiff's Notice of Tort Claim.

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

Plaintiff Monte Sundrea Holt's Experience

140. Plaintiff Monte Sundrea Holt (for purposes of this section, "Plaintiff") is not aware of ever providing his Social Security number directly to Defendant. Around ten years ago Plaintiff applied for and was in preemployment screening/training for a commercial airline that operates out of Sea-Tac Airport; however, upon information and belief he was never formally employed by the airline nor the Defendant.

141. Since the time of the Data Breach Plaintiff has been notified—via credit monitoring provided as an ancillary service to a credit card— that his PI was found and exposed on the dark web. Additionally, since the Data Breach, Plaintiff has experienced a significant increase in spam communications, including unsolicited calls, text messages, emails, and other forms of contact.

142. As a result of the significant increase in spam communications to his phone Plaintiff had to change his phone number.

143. Since becoming aware of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, monitoring his financial accounts, changing passwords, and implementing extra security on his computers. Plaintiff spent significant time dealing with the Data Breach, which is valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

144. Plaintiff suffered actual injury from having his Private Information compromised as a result of the Data Breach, including, but not limited to: (i) invasion of privacy; (ii) theft of his Private Information; (iii) lost or diminished value of his Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) statutory damages; (vii) nominal damages; and (viii) the continued and certainly increased risk to his Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains

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

backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

145. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

146. Plaintiff anticipates spending considerable time on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

147. As a result of the Data Breach, Plaintiff is at present risk and will continue to be at increased risk of identity theft and fraud for his lifetime.

148. Plaintiff has a continuing interest in ensuring that his Private Information which, on information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

149. On or about April 12, 2025, Plaintiff sent a Notice of Tort Claim to Defendant consistent with RCW 4.96.020.

150. On May 12, 2025, Defendant denied Plaintiff's Notice of Tort Claim.

Plaintiff Sarah Rainbow Cardenas' Experience

151. Plaintiff Sarah Rainbow Cardenas (for purposes of this section, "Plaintiff") regularly uses SeaTac Airport. In order to travel through SeaTac Airport, Plaintiff was required to submit certain personal information, such as her government identification information, to Defendant's system. However, she is not aware of ever providing her Social Security number directly to Defendant and has never been employed by them. As a result of the Data Breach, Plaintiff received several dark web alerts from her credit monitoring service, Aura, in or around January 2025, indicating that her personal information had been exposed on the dark web. Additionally, since the Data Breach, Plaintiff has experienced a significant increase in spam communications, including unsolicited calls, text messages, emails, and other forms of contact.

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

152. Furthermore, after the Data Breach, Plaintiff has noticed a substantial uptick in loan application advertisements arriving by mail, many of which indicate that she was preapproved for loans or credit she never applied for, or solicited her to apply for new lines of credit.

153. Since becoming aware of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, monitoring her financial accounts, changing passwords, and implementing extra security on her computers. Plaintiff spent significant time dealing with the Data Breach, which is valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

154. Plaintiff suffered actual injury from having her Private Information compromised as a result of the Data Breach, including, but not limited to: (i) invasion of privacy; (ii) theft of her Private Information; (iii) lost or diminished value of her Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) statutory damages; (vii) nominal damages; and (viii) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

155. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the Data Breach's occurrence.

156. Plaintiff anticipates spending considerable time on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

157. As a result of the Data Breach, Plaintiff is at present risk and will continue to be

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

at increased risk of identity theft and fraud for her lifetime.

158. Plaintiff has a continuing interest in ensuring that her Private Information which, on information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

159. On or about April 21, 2025, Plaintiff sent a Notice of Tort Claim to Defendant consistent with RCW 4.96.020.

160. On May 12, 2025, Defendant denied Plaintiff's Notice of Tort Claim.

CLASS ALLEGATIONS

161. Plaintiffs bring this nationwide class action on behalf of themselves and others similarly situated, pursuant to Civil Rule 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

162. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

> **All individuals residing in the United States whose Private Information was accessed and/or acquired by an unauthorized party as a result of the Data Breach discovered by Defendant Port of Seattle in August 2024 (the "Class").**

163. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers, and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

164. Plaintiffs reserve the right to modify or amend the definition of the proposed Class or add necessary sub-classes before the Court determines whether certification is appropriate.

165. Numerosity: Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are thousands of individuals who were notified by Defendant of the Data Breach. The identities of Class Members are ascertainable through Defendant's records, Class Members' records, publication notice, self-identification, and other

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

means.

166. Commonality: Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiffs and Class Members;

b. Whether Defendant had duties not to disclose the Private Information of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendant had duties not to use the Private Information of Plaintiffs and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the Private Information of Plaintiffs and Class Members;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their Private Information had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their Private Information had been compromised;

h. 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;

i. Whether Defendant adequately addressed and fixed the vulnerabilities that permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiffs and Class Members;

k. Whether Defendant violated the statutes invoked herein;

l. Whether Plaintiffs and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

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

m. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

n. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and ongoing harm faced as a result of the Data Breach.

167. Typicality: Plaintiffs' claims are typical of those of other Class Members because all had their Private Information compromised as a result of the Data Breach, due to Defendant's misfeasance. Likewise, the relief to which Plaintiffs are entitled is typical of the Class because Defendant has acted and refused to act on grounds generally applicable to the Class. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

168. Adequacy: Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that Plaintiffs have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs and their counsel seek no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiffs have suffered are typical of other Class Members. Plaintiffs have also retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

169. Superiority: Compared to all other available means of fair and efficient adjudication of the claims of Plaintiffs and the Class, a class action is the most superior. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of the complex and extensive litigation necessitated by Defendant's conduct. It would be virtually impossible for members of the Class individually to effectively redress the wrongs done to them. Even if the members of the Class could afford such individual litigation, the court system could not. Individualized litigation presents a risk of inconsistent or contradictory judgments. Individualized litigation increases the delay and

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

expense to all parties and the court system due to the complex legal and factual issues of the case. 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. Members of the Class can be readily identified and notified based on, *inter alia*, Defendant's records and databases.

CLAIMS FOR RELIEF

COUNT I

NEGLIGENCE

(On Behalf of Plaintiff and the Class)

170. Plaintiffs re-allege and incorporate by reference herein all of the allegations included in the paragraphs above.

171. Plaintiffs and Class Members were required to submit their Private Information to Defendant in order to receive employment from Defendant.

172. Plaintiffs and Class Members entrusted their Private Information to Defendant on the premise and reasonable expectation that Defendant would safeguard their information, use their Private Information for business purposes only, and that Defendant would securely maintain the Private Information so that it would not be accessible to or able to be exfiltrated by cybercriminals.

173. Defendant has full knowledge of the sensitivity of the Private Information it collected and maintained, and the types of harm that Plaintiffs and Class Members could and would suffer if the Private Information were wrongfully disclosed.

174. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the Private Information of Plaintiffs and Class Members involved an unreasonable risk of harm to Plaintiffs and Class Members, even if the harm occurred through the criminal acts of a third party.

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

175. Plaintiffs and Class Members were the foreseeable victims of any inadequate safety and security practices. Plaintiffs and Class Members had no ability to protect their PII that was in Defendant's possession. As such, a special relationship existed between Defendant and Plaintiffs and the Class.

176. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the Private Information of Plaintiffs and Class Members in Defendant's possession was adequately secured and protected.

177. Defendant's duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's conduct or misconduct exposes another to risk or defeats protections put in place to guard against it, or where the parties are in a special relationship. *See* RESTATEMENT (SECOND) OF TORTS § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

178. Defendant also had a duty to exercise appropriate clearinghouse practices to remove Private Information it was no longer required to retain.

179. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the Private Information of Plaintiffs and Class Members.

180. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiffs and Class Members. That special relationship arose because Plaintiffs and Class Members entrusted Defendant, either directly or indirectly, with their confidential Private Information, a necessary part of obtaining employment from Defendant.

181. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiffs or Class Members.

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

182. A breach of security, unauthorized access, and resulting injury to Plaintiffs and Class Members was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

183. Defendant knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiffs and Class Members, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendant's systems.

184. Defendant's own conduct created a foreseeable risk of harm to Plaintiffs and Class Members. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of the Private Information of Plaintiffs and Class Members, including basic encryption techniques freely available to Defendant.

185. Defendant was in a position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

186. Defendant had and continues to have a duty to adequately disclose that the Private Information of Plaintiffs and Class Members within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

187. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the Private Information of Plaintiffs and Class Members.

188. Defendant has admitted that the Private Information of Plaintiffs and Class Members was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

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

189. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiffs and Class Members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the Private Information of Plaintiffs and Class Members during the time the Private Information was within Defendant's possession or control.

190. Defendant improperly and inadequately safeguarded the Private Information of Plaintiffs and Class Members in deviation from standard industry rules, regulations, and practices at the time of the Data Breach.

191. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the Private Information of Plaintiffs and Class Members in the face of increased risk of theft.

192. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of Private Information.

193. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove the Private Information it was no longer required to retain pursuant to regulations.

194. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiffs and Class Members the existence and scope of the Data Breach.

195. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and the Nationwide Class, the Private Information of Plaintiffs and Class Members would not have been compromised.

196. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiffs and Class Members and the harm, or risk of imminent harm, suffered by Plaintiffs and the Class. The Private Information of Plaintiffs and Class Members was lost and accessed as the proximate result of Defendant's

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

failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

197. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its current and former employees and vendors, which is recognized by laws and regulations including but not limited to HIPAA, the FTC Act, and common law. Defendant was in a superior position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

198. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes (or may constitute) "protected health information" within the meaning of HIPAA.

199. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

200. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and Class Members.

201. Defendant's violation of Section 5 of the FTC Act constitutes negligence.

202. Plaintiffs and Class Members are within the class of persons that the FTC Act

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

was intended to protect.

203. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and Class Members.

204. Defendant's duty to act reasonably in collecting, storing, and maintaining the Private Information, and to use reasonable care in protecting such information arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information that it either affirmatively acquires, maintains, or stores. Industry standards require Defendant to exercise reasonable care with respect to Plaintiffs and Class Members by implementing reasonable data security measures that do not create a foreseeable risk of harm to Plaintiffs and Class Members. Industry best practices put the onus of adequate cybersecurity on the entity most capable of preventing a Data Breach. In this case, Defendant was the only entity that could adequately protect the data that it solicited, collected, and stored.

205. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to control how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and continuing consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized

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

disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information of Plaintiffs and Class Members; and (viii) present and continuing costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

206. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

207. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered and will suffer the continued risk of exposure of their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

208. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members are entitled to recover actual, consequential, and nominal damages.

COUNT II

UNJUST ENRICHMENT

(On behalf of Plaintiffs and the Class)

209. Plaintiffs re-allege and incorporate by reference herein all of the allegations included in the paragraphs above. Notwithstanding, Plaintiffs bring this claim in the alternative to any claim for breach of contractual obligations.

210. Defendant benefited from receiving Plaintiffs' and Class Members' Private Information by its ability to retain and use that information for its own benefit. Defendant understood this benefit.

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

211. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information.

212. Defendant was also enriched by the value of Plaintiffs' and Class Members' Private Information. Private Information has independent value as a form of intangible property. Defendant also derives value from this information because it allows Defendant to operate its business and generate revenue.

213. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

214. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

215. Defendant acquired the monetary benefit and Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

216. Had Plaintiffs and Class Members known that Defendant had not secured their Private Information, they would not have agreed to provide their Private Information to Defendant.

217. Plaintiffs and Class Members have no adequate remedy at law.

218. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to control how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized

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

use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in their continued possession and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

219. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm. Defendant should be compelled to disgorge into a common fund or constructive trust for the benefit of Plaintiffs and Class Members, proceeds that it unjustly received from them.

COUNT III

BREACH OF IMPLIED CONTRACT

(On Behalf of Plaintiffs and the Class)

220. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

221. When Plaintiffs and Class Members provided their Private Information to Defendant in exchange for employment, they entered implied contracts with Defendant under which Defendant agreed to reasonably protect such information.

222. Defendant solicited, offered, and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

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

223. In entering such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, including the Federal Trade Commission Act, and adhered to industry standards.

224. Plaintiffs and Class Members provided labor to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

225. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

226. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that they adopted reasonable data security measures.

227. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

228. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their Private Information.

229. As a direct and proximate result of Defendant's breach of the implied contracts, Class Members sustained damages as alleged here, including the loss of the benefit of the bargain.

230. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered because of the Data Breach.

231. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

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

COUNT IV

INVASION OF PRIVACY

(On Behalf of Plaintiffs and the Class)

232. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

233. Plaintiffs and Class Members had a legitimate expectation of privacy regarding their highly sensitive and confidential PI and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

234. Defendant owed a duty to its current and former employees, contractors, and consumers, including Plaintiffs and Class Members, to keep this information confidential.

235. The unauthorized acquisition (i.e., theft) by a third party of Plaintiffs' and Class Members' PI is highly offensive to a reasonable person.

236. The intrusion was into a place or thing which was private and entitled to be private. Plaintiffs and Class Members disclosed their sensitive and confidential information to Defendant, but did so privately, with the intention that their PI would be kept confidential and protected from unauthorized disclosure. Plaintiffs and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization. The Data Breach constitutes intentional interference with Plaintiffs' and Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

237. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

238. Defendant acted with a knowing state of mind when it failed to notify Plaintiffs and Class Members in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

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

239. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and Class Members.

240. As a proximate result of Defendant's acts and omissions, the private and sensitive PI of Plaintiffs and Class Members was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and Class Members to suffer damages.

241. Furthermore, on information and belief, Plaintiffs' and Class Members' PI has already been published—or will be published imminently—by cybercriminals on the dark web.

242. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members since their PI is still maintained, despite its inadequate cybersecurity system and policies, on Defendant's compromised servers.

243. Plaintiffs and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the PI of Plaintiffs and Class Members.

244. In addition to injunctive relief, Plaintiffs, on behalf of themselves and the other Class Members, also seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

COUNT V

VIOLATION OF WASHINGTON DATA BREACH NOTIFICATION LAW

RCW 42.56.590, et seq.

245. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

246. Under RCW 42.56.590(2), "[a]ny agency that maintains or possesses data that may include personal information that the agency does not own or license shall notify the owner

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

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."

247. Specifically, under RCW 42.56.590(8), "[n]otification to affected individuals must be made in the most expedient time possible, without unreasonable delay, and no more than thirty calendar days after the breach was discovered."

248. Further, under RCW 42.56.590(7), "[a]ny agency that is required to issue a notification pursuant to this section to more than five hundred Washington residents as a result of a single breach shall notify the attorney general of the breach no more than thirty days after the breach was discovered."

249. Upon information and belief, RCW 42.56.590 applies to Defendant because Defendant qualifies as an "agency" within the meaning of the statute and does not own nor license the PI in question. Instead, the owners and/or licensees of the PI are the Plaintiffs and Class Members. The PI in question qualifies as "personal information" under the definition set forth in RCW 42.56.590(10), as the compromised data includes, but is not limited to, individuals' full names, dates of birth, driver's license numbers, and the last four digits of their Social Security numbers.

250. Therefore, Defendant was required to notify Plaintiffs and Class Members—the owners or licensees of the PI at issue—of the Data Breach "immediately following discovery," as mandated by RCW 42.56.590(2), and "no more than thirty calendar days after the breach was discovered," pursuant to RCW 42.56.590(8). Yet, Defendant failed to do so.

251. Although Defendant issued a public statement about the Data Breach on September 13, 2024—approximately three weeks after its initial discovery on August 24, 2024—the announcement failed to include critical details, such as the types of information that had been compromised and who was affected. This general disclosure did not constitute the individual notice pursuant to RCW 42.56.590(6).

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

252. In fact, Defendant appears to have delayed providing direct notice to affected individuals until around April 2, 2025—more than seven full months after the Data Breach occurred.

253. In addition, the Data Breach at issue affected approximately 71,000 Washington residents, which substantially exceeds the threshold of five hundred individuals specified in RCW 42.56.590(7).

254. Thus, Defendant is in plain violation of RCW 42.56.590 for failing to promptly notify Plaintiffs and Class Members—the owners of the PI at issue—following discovery of the breach.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, request that the Court enter judgment in their favor and grant the following relief:

A. For an Order certifying the Classes, and appointing Plaintiffs and their Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiffs and Class Members, and enjoining Defendant from refusing to issue prompt, complete, and accurate disclosures to Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiffs, including, but not limited to, injunctive and other equitable relief necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable

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

regulations, industry standards, and federal, state, or local laws;

iii. requiring Defendant to delete, destroy, and purge the Private Information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiffs and Class Members;

v. prohibiting Defendant from maintaining the Private Information of Plaintiffs and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and security checks;

xi. requiring Defendant to establish an information security training program that

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

includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling Private Information, as well as protecting the Private Information of Plaintiffs and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis, to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate

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

Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to submit the report of any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including but not limited to, actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

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

Dated this 11th day of June, 2025.

s/Kaleigh N. Boyd
Kaleigh N. Boyd, WSBA No. 52684
TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
Telephone: (206) 682-5600
Email: kboyd@tousley.com

Timothy W. Emery, WSBA No. 34078
Patrick B. Reddy, WSBA No. 34092
Brook Garberding, WSBA No. 37140
EMERY REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, Washington 98101
Telephone: (206) 442-9106
Email: emeryt@emeryreddy.com
Email: reddyp@emeryreddy.com
Email: brook@emeryreddy.com

M. Anderson Berry, WSBA No. 63160
Gregory Haroutunian*
Michelle Zhu*
CLAYEO C. ARNOLD
A PROFESSIONAL CORPORATION
865 Howe Avenue
Sacramento, California 95825
Telephone: (916) 239-4778
Email : aberry@justice4you.com
Email : gharoutunian@justice4you.com
Email: mzhu@justice4you.com

Jeff Ostrow*
KOPELOWITZ OSTROW P.A.
1 W. Las Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Telephone: (954) 525-4100
Email: ostrow@kolawyers.com

Gary M. Klinger*
John J. Nelson*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
402 W Broadway, Suite 1760
San Diego, California 92101
Telephone: (858) 209-6941
Email: jnelson@milberg.com

Janelle N. Bailey, WSBA No. 54586
WASHINGTON INJURY LAW
1905 Queen Anne Avenue North, Suite 300
Seattle, Washington 98109
Telephone: (206) 960-4522
Email: Litigation@WashingtonInjuryLaw.com

Leigh S. Montgomery,* Texas Bar No. 24052214
EKSM, LLP
4200 Montrose Blvd., Suite 200
Houston, Texas 77006
Telephone: (888) 350-3931
Email: lmontgomery@eksm.com
Email: service@eksm.com

**Pro Hac Vice forthcoming*

Attorneys Plaintiffs and the Proposed Class

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