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

AMY GARCIA, ANTHONY GIBBONS, and TAYLOR RIELY-GIBBONS, individually and on behalf of all others similarly situated, Plaintiffs, v. WASHINGTON STATE DEPARTMENT OF LICENSING, an agency of the State of Washington, Defendant.	No. 22-2-05635-5 SEA **FIRST AMENDED CLASS ACTION COMPLAINT**

Plaintiffs Amy Garcia, Anthony Gibbons, and Taylor-Riely Gibbons ("Plaintiffs"), individually and on behalf of all others similarly situated, by and through their counsel, bring this Class Action Complaint against the Defendant Washington State Department of Licensing ("DOL") and allege, upon personal knowledge as to their own actions and their counsels' investigation, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiffs and similarly situated individuals were required to provide their confidential and sensitive information to DOL to obtain licenses to conduct business in Washington. DOL failed to implement and maintain adequate security protocols in storing and/or transferring this information, and as a result, hackers stole it.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

II. JURISDICTION AND VENUE

2. This Court has jurisdiction over this cause of action under RCW 2.08.010 and RCW 4.92.090.

3. This Court has personal jurisdiction over DOL because it is a Washington State agency.

4. Venue is proper in this Court pursuant to RCW 4.12.020(3) and RCW 4.92.010(1) because a substantial part of the events or omissions giving rise to these claims occurred in King County, Washington and at least one Plaintiff resides in King County, Washington.

III. PARTIES

5. Plaintiff Amy Garcia is an individual and is a resident of Algona, King County, Washington.

6. Plaintiff Anthony Gibbons is an individual and is a resident of Kitsap County, Washington. Mr. Gibbons first applied for an appraisal license in or about 1991.

7. Plaintiff Taylor Riely-Gibbons is an individual and is a resident of Kitsap County, Washington. Mr. Riely-Gibbons first applied for an Appraisal Trainee license in or around 2013, and received his Certified General Real Estate Appraiser license in or around April 2019.

8. Defendant Washington State Department of Licensing is a Washington State agency with its main office located at 405 Black Lake Blvd SW, Olympia, Washington 98502.

IV. FACTUAL BACKGROUND

The DOL's Licensing System, POLARIS

9. DOL issues licenses for 39 types of businesses and professions, including cosmetologists, real estate brokers, bail bondsmen, professional wrestlers, architects, and driver training school instructors.[1]

[1] *Professional and Business Licensing Service Outage*, Washington State Department of Licensing, https://www.dol.wa.gov/outage/index.html (last visited Mar. 17, 2022).

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

10. DOL maintains professional and occupational licensees' information in a system known as the Professional Online Licensing and Regulatory Information System ("POLARIS").

11. For 23 different professions, POLARIS is used to process, issue, and renew license applications, accept complaints from the public against license holders, and more.

12. Prior to January 2022, Plaintiffs and the Class Members were required to provide certain information to DOL via POLARIS to obtain professional licenses. This information included, but was not limited to, full names, e-mail addresses, Social Security numbers, dates of birth, and/or driver's license or state identification numbers ("Personal Information"). In many instances, Plaintiffs and the Class Members also provided additional Personal Information as part of the licensing process, including credit card numbers, bank account numbers, routing numbers, telephone numbers, and places of employment.

13. As part of DOL's Data Governance Policy, "This policy applies to all Department of Licensing (Agency) Employees and contractors as contract allows. . . . The Agency has an obligation to protect the privacy of the customers we serve."[2]

14. DOL stated in its May 2020 Data Stewardship Report:

> The Washington State Department of Licensing is an agency of the State of Washington, a steward of data concerning the people of the state . . . Data is our principal asset, and the safety of data within the agency is an important component of the agency's strategy.[3]

15. DOL published the following privacy statement on its official website:

> **Securing your information**
>
> Keeping your information safe is so important to us, we made it a part of our purpose
>
> . . .
>
> **Securing online transactions**

---

[2] *Policy: Data Governance 1.7.1*, Washington State Department of Licensing, https://www.dol.wa.gov/privacy/docs/data-gov-policy-1-7-1.pdf (last visited Mar. 18, 2022).

[3] *Fact Sheet Explaining the DOL Data Stewardship Framework and Plan*, Washington State Department of Licensing, https://www.dol.wa.gov/privacy/docs/data-framework-leg-report.pdf (last visited Mar. 18, 2022).

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

When you complete a transaction with us online (like renewing a license or reporting the sale of a vehicle) you're using our secure online services. We verify you're who you say you are, using:

- A user name and password
- A PIN number
- A digital certificate
- Other methods of authentication

We build protections into these systems to:

- Ensure your security
- Safeguard your data
- Provide reasonable protection of private information in our possession.

You can help secure your data by adding an email address to your account. This will allow us to notify you if someone makes changes to your information.

We don't disclose your secure login information, such as a user name and password, to the public. Information you provide to us through secure services is disclosable only to the extent authorized by law.

Data sharing and security

We have full-time compliance staff assigned to this. They conduct regular investigations and audits to make sure data recipients:

- Follow our data security requirements.
- Only use the data as authorized.[4]

The Data Breach

16. On or before the week of January 24, 2022, DOL became aware of suspicious activity involving professional and occupational license information contained in the POLARIS's Professional and Business Licensing System.

17. The Seattle Times reported that January 24, 2022 was the same date that the Washington State Office of Cybersecurity also first became aware of the breach after it

[4] *Securing Your Information*, Washington State Department of Licensing, https://www.dol.wa.gov/privacy/securing-your-info.html (last visited Mar. 18, 2022).

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

"detect[ed] 'chatter' on the dark web about 'accessed' personal data from Department of Licensing."[5]

18. DOL's subsequent investigation revealed that POLARIS was accessed in the Data Breach and Personal Information for approximately 650,000 licensees was stolen, including their names, e-mail addresses, Social Security numbers, dates of birth, and/or driver's license or state identification numbers.

19. Hackers may also have acquired additional Personal Information, including credit card account numbers, bank account numbers, routing numbers, telephone numbers, and places of employment.

20. The information taken from POLARIS has already appeared on the dark web—and, indeed, its appearance on the dark web was what alerted the Office of Cybersecurity to the Data Breach in the first place. As further explained below, the dark web is a network of underground websites on which a "black market" exists for illegally-obtained personal information.

21. To date, DOL has not released any of the findings of that investigation, and has kept secret the details of the Data Breach, including the vulnerabilities the attackers exploited to steal Personal Information.

22. According to information published by the Washington Office of the Attorney General, 460,478 Washingtonians were affected by the Data Breach.[6]

The Design, Implementation, and Maintenance of the POLARIS Network Systems

[5] https://www.seattletimes.cmo/business/investigators-theives-got-access-to-data-from-650000-individuals-in-state-licensing-database/ (last visited Apr. 14, 2022).

[6] *Data Breach Notifications*, Washington State Office of the Attorney General, https://www.atg.wa.gov/data-breach-notifications (last visited Mar. 17, 2022).

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

23. In or about January 2020, DOL, via one or more third-party agents, designed and/or redesigned and then subsequently implemented the POLARIS system environments that would ultimately contain the Personal Information of Plaintiffs and the Class.[7]

24. DOL was also responsible for the day-to-day operations, monitoring, maintenance, and configuration of the POLARIS system environments. This responsibility, among others, included migrating Personal Information into POLARIS and ensuring it remained reliable, secure, and insusceptible to unauthorized access.

25. However, DOL instead designed and implemented POLARIS with inadequate safety and security protocols that were vulnerable to access by unauthorized users.

26. Following implementation, DOL failed to test, monitor, and patch vulnerabilities in POLARIS, ensuring that system remained susceptible to unauthorized access.

27. DOL's failures in this regard created an end-product that was unreasonably susceptible to unauthorized access, jeopardized the Personal Information of POLARIS users, and ultimately resulted in the Data Breach.

28. By failing to ensure that POLARIS was adequately secure, and by failing to test, monitor, and patch existing vulnerabilities in the POLARIS system environments, DOL fell short of its obligations, and also fell short of Plaintiff's and the Class Members' reasonable expectations for the protection of their Personal Information.

29. DOL was aware, or should have been aware, that POLARIS was an inadequately secure system.

30. DOL was aware, or should have been aware, that failing to test, monitor, and patch security vulnerabilities in POLARIS would jeopardize the Personal Information.

The Effect of the Data Breach on Plaintiffs

1. Amy Garcia.

---

[7] *See* Exhibit 1 (Polaris Project Management Plan Release 2), *available at*: https://waocio.secure.force.com/sfc/servlet.shepherd/version/download/0680P000007ChPjQAK?asPdf=false& (last visited Mar. 21, 2022).

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

31. DOL sent Plaintiff Amy Garcia a notice stating that her Personal Information was exposed in the Data Breach.

32. Following the Data Breach, Plaintiff experienced a substantial uptick in the number and frequency of spam email contacts to the email address she provided to DOL to obtain her professional license.

33. Also following the Data Breach, Plaintiff learned that she had become the victim of fraud as a result of an identity-thief opening a consumer tradeline in her name. Upon information and belief, but for the Data Breach, Plaintiff would not have been a victim of this crime.

34. Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to: researching the Data Breach; reviewing credit reports, credit monitoring, and financial account statements for any indications of actual or attempted identity theft or fraud; researching credit monitoring and identity theft protection services offered by DOL; dealing with unwanted spam and telephone calls, and ultimately spending time dealing with the unauthorized tradeline opened in her name.

35. Plaintiff spent at least 10 hours dealing with the Data Breach to date, valuable time she otherwise would have spent on other activities, including, but not limited to, work, recreation, or time with her family.

36. As a result of the Data Breach, Plaintiff has suffered emotional distress due to the release of her Personal Information, which she believed DOL had protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her Personal Information for purposes of identity theft and fraud. Plaintiff remains very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

37. Plaintiff suffered actual injury from having her Personal Information compromised as a result of the Data Breach including, but not limited to: (a) damage to and diminution in the

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

value of her Personal Information, a form of property that DOL obtained from Plaintiff; (b) violation of her privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft and fraud.

38. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to attempt to mitigate and address harms caused by the Data Breach.

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

2. Anthony Gibbons.

40. Plaintiff Anthony Gibbons applied for his real estate appraisal license for the first time in or about 1991. As part of the State's licensing requirements, Plaintiff Gibbons was required to provide sensitive Personal Information, including his Social Security number, address, and date of birth.

41. On or about February 23, 2022, the DOL sent Plaintiff Gibbons a letter informing him that his DOL professional license record may have been obtained by an unauthorized person.

42. Plaintiff Gibbons has already experienced the effects of the Data Breach. In March 2022, Plaintiff Gibbons received an email purporting to be an "All appraisal property document information.exe" that contained a virus. He had never before received an appraisal targeted virus or email like this before. His receipt of this email appears to be related to the release of his Personal Information in conjunction with the Data Breach.

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

44. Plaintiff suffered actual injury from having his Personal Information compromised as a result of the Data Breach including, but not limited to: (a) damage to and diminution in the value of his Personal Information, a form of property that DOL obtained from Plaintiff; (b)

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

violation of his privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft and fraud.

3. Taylor Riely-Gibbons.

45. Plaintiff Taylor Riely-Gibbons first applied for an Appraisal Trainee license in or around 2013, and received his Certified General Real Estate Appraiser license in or around April 2019. As part of the State's licensing requirements, Plaintiff Riely-Gibbons was required to provide sensitive Personal Information, including his Social Security number, address, and date of birth.

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

47. Plaintiff suffered actual injury from having his Personal Information compromised as a result of the Data Breach including, but not limited to: (a) damage to and diminution in the value of his Personal Information, a form of property that DOL obtained from Plaintiff; (b) violation of his privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft and fraud.

The Effects of the Data Breach on the Class

48. Plaintiffs' experience in connection with the Data Breach is typical of those of the Class Members.

49. Given the sensitive nature of the Personal Information stolen in the Data Breach, hackers have the ability to commit identify theft, financial fraud, and other identity-related fraud against Plaintiffs and Class Members now and into the indefinite future.

50. As a result of the Data Breach, Plaintiffs and Class Members will have to take a variety of steps to monitor for and safeguard against identity theft, and they are at a much greater risk of suffering such identity theft. In addition, these victims of the Data Breach are at a

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

heightened risk of potentially devastating financial identity theft. As the Bureau of Justice Statistics reports, identity theft causes its victims out-of-pocket monetary losses and costs the nation's economy billions of dollars every year.[8]

51. In fact, like the Plaintiffs, many victims of the Data Breach have already experienced harms as a result of the Data Breach, including, but not limited to, identity theft, financial fraud, tax fraud, unauthorized lines of credit opened in their names, medical and healthcare fraud, and unauthorized access to their bank accounts. Plaintiffs and Class Members have spent and will spend time, money, and effort dealing with the fallout of the Data Breach, including purchasing credit protection services, contacting their financial institutions, checking credit reports, and spending time and effort searching for unauthorized activity.

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

53. Consumers are injured every time their data is stolen and placed on the dark web, even if they have been victims of previous data breaches. Not only is the likelihood of identity theft increased, but the dark web is not like Google or eBay. It is comprised of multiple discrete

[8] U.S. Dept. of Justice, Bureau of Justice Statistics, *Victims of Identity Theft, 2012* (Dec. 2013), http://www.bjs.gov/content/pub/pdf/vit12.pdf (last visited Mar. 17, 2022).

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

repositories of stolen information. Each data breach puts victims at risk of having their information uploaded to different dark web databases and viewed and used by different criminal actors.

54. Exposure of this information to the wrong people can have serious consequences. Identity theft can have ripple effects, which can adversely affect the future financial trajectories of victims' lives. For example, the Identity Theft Resource Center reports that respondents to their surveys in 2018-2020 described that the identity theft they experienced affected their ability to get credit cards and obtain loans, such as student loans and mortgages.[9] For some victims, this could mean the difference between going to college or not, becoming a homeowner or not, or having to take out a high interest payday loan versus a lower-interest loan.

55. Annual monetary losses from identity theft are in the billions of dollars. According to a Presidential Report on identity theft produced in 2007:

> In addition to the losses that result when identity thieves fraudulently open accounts . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.[10]

---

[9] Identity Theft Resource Center, *2021 Consumer Aftermath Report*, https://www.idtheftcenter.org/publication/identity-theft-the-aftermath-study/ (last visited Mar. 17, 2022).

[10] FTC, *Combatting Identity Theft A Strategic Plan* (April 2007), https://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf (last visited Mar. 17, 2022).

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

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

> [A] new number probably won't solve all your problems. This is because other governmental agencies (such as the Internal Revenue Service and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify to identify your credit record. So using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security number, you shouldn't use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information isn't associated with your new number, the absence of any credit history under your new number may make it more difficult for you to get credit.[11]

57. According to the Attorney General of the United States, Social Security numbers "can be an identity thief's most valuable piece of consumer information."[12] Indeed, as explained recently:

> The ubiquity of the SSN as an identifier makes it a primary target for both hackers and identity thieves. . . . When data breaches expose SSNs, thieves can use these numbers—usually combined with other pieces of data—to impersonate individuals and apply for loans, housing, utilities, or government benefits. Additionally, this information may be sold on the black market to other hackers.[13]

---

[11] *Identity Theft and Your Social Security Number* (July 2021), Social Security Administration, https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Mar. 21, 2022).
[12] *Fact Sheet: The Work of the President's Identity Theft Task Force*, DOJ 06-636, 2006 WL 2679771 (Sep. 19, 2006).
[13] Daniel J. Marcus, *The Data Breach Dilemma: Proactive Solutions for Protecting Consumers' Personal Information*, 68 Duke L.J. 555, 564-65 (2018).

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

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

a. losing the inherent value of their Personal Information;

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

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

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

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

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

49. Even in instances where a consumer is reimbursed for a financial loss due to identity theft or fraud, that does not make that individual whole again, as there is typically significant time and effort associated with seeking reimbursement that is not refunded. The Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" relating to identity theft or fraud.[14]

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

[14] E. Harrell, U.S. Department of Justice, *Victims of Identity Theft, 2014* (revised Nov. 13, 2017), http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited Mar. 17, 2022).

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[15]

V. CLASS ACTION ALLEGATIONS

51. Class Definition. Under Civil Rule 23(a) and (b)(3), Plaintiffs bring this case as a class action against DOL on behalf of the Class preliminarily defined as follows:

> All individuals whose personal information was compromised in the data breach disclosed by the Washington State Department of Licensing in February 2022.

52. Excluded from the Class are the following: DOL and DOL's officers, and directors, and any judge to whom this case is assigned, as well as his or her staff and immediate family.

53. Plaintiffs reserve the right to amend the Class definition.

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

55. Numerosity. The proposed Class consists of at least 460,478 members—far too many to join in a single action.

56. Ascertainability. Class Members are readily identifiable from information in DOL's possession, custody, or control.

57. Typicality. Plaintiff's claims are typical of Class Members' claims, as each arise from the same Data Breach, the same alleged negligence of and/or statutory violations by DOL, and the same unreasonable manner of notifying individuals regarding the Data Breach.

58. Adequacy. Plaintiffs will fairly and adequately protect the interests of the proposed Class. Plaintiffs' interests do not conflict with those of the Class. Plaintiffs have retained counsel

---

[15] U.S Government Accountability Office Report to Congressional Requesters, *Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown* (June 2007), http://www.gao.gov/new.items/d07737.pdf (last visited Mar. 17, 2022).

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

experienced in complex class action litigation and data privacy to vigorously prosecute this action on behalf of the Class, including in the capacity as lead counsel.

59. Commonality. Plaintiffs' and Class Members' claims raise predominantly common factual and legal questions that can be answered for all Class Members through a single class-wide proceeding. For example, to resolve any Class Member's claims, it will be necessary to answer the following questions: (a) Whether DOL failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Personal Information compromised in the Data Breach; (b) Whether DOL's conduct was negligent; and (c) Whether Plaintiffs and the Class are entitled to damages and/or injunctive relief.

60. In addition to satisfying the prerequisites of CR 23(a), Plaintiffs satisfy the requirements for maintaining a class action under CR 23(b). Common questions of law and fact predominate over any questions affecting only individual Class Members, and a class action is superior to individual litigation or any other available methods for the fair and efficient adjudication of the controversy. The damages available to individual plaintiffs are insufficient to make litigation addressing DOL's privacy practices economically feasible in the absence of the class action procedure.

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

VI. CAUSES OF ACTION

FIRST CAUSE OF ACTION
NEGLIGENCE
Claim of Relief for Plaintiffs and the Class and Against Defendant DOL

62. Plaintiffs incorporate by reference all foregoing factual allegations.

63. DOL collected and transferred Personal Information from Plaintiffs and the Class and had a corresponding duty to protect such information from unauthorized access.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

64. DOL failed to inform Plaintiffs and the Class that its systems were inadequate to safeguard sensitive information and that transferring Personal Information could lead to attackers gaining access to sensitive information.

65. The sensitive nature of the Personal Information and economic value of it to hackers necessitated security practices and procedures sufficient to prevent unauthorized access to the Personal Information.

66. DOL failed to implement and maintain adequate security practices and procedures to prevent the Data Breach.

67. DOL likewise failed to test, update, and patch (including curing known vulnerabilities) the POLARIS system as necessary.

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

69. Furthermore, given the known risk of major data breaches, including the 2021 breach of the Washington State Auditor's Office, Plaintiffs and the Class are part of a well-defined, foreseeable, finite, and discernible group that was at high risk of having their Personal Information stolen.

70. DOL's duty of care arose as a result of its knowledge that individuals trusted the State to protect their confidential data that they provided to it. Only the DOL was in a position to ensure that its own protocols were sufficient to protect against the harm to Plaintiffs and the Class from a data breach of its own systems. Moreover, DOL's Data Governance Policy 1.7.1 states, "The Agency has an obligation to protect the privacy of the customers we serve."

71. DOL also had a duty to use reasonable care in protecting confidential data because it committed to comply with industry standards for the protection of Personal Information, and committed to the public to protect the privacy of information the public provided DOL.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

72. DOL knew, or should have known, of the vulnerabilities in its security practices and procedures, and the importance of adequate security to POLARIS users and the owners of sensitive data.

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

74. Consistent with RCW 4.92.100, Plaintiffs, on their own behalf and on behalf of the Class they seeks to represent, presented a Tort Claim Form to the Washington Department of Enterprise Services' Office of Risk Management for the State's tortious conduct as set forth herein. More than sixty days have elapsed after their claims were presented. *See* RCW 4.92.100.

VII. PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of the Class, request that the Court enter judgment against DOL as follows:

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

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

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

i. Prohibiting DOL from engaging in the wrongful and unlawful acts described herein;

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

ii. Requiring DOL to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and state or local laws;

iii. Requiring DOL to delete, destroy, and purge the Personal Information of Plaintiffs and Class Members unless DOL 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 DOL to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Personal Information of Plaintiffs and Class Members;

v. Prohibiting DOL from maintaining the Personal Information of Plaintiffs and Class Members on a cloud-based database;

vi. Requiring DOL 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 DOL's systems on a periodic basis, and ordering DOL to promptly correct any problems or issues detected by such third-party security auditors;

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

viii. Requiring DOL to audit, test, and train their security personnel regarding any new or modified procedures;

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

x. Requiring DOL to conduct regular database scanning and securing checks;

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

xi. Requiring DOL to establish an information security training program that 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 Personal Information, as well as protecting the Personal Information of Plaintiffs and Class Members;

xii. Requiring DOL 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 DOL to implement a system of tests to assess its employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with DOL's policies, programs, and systems for protecting Personal Information;

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

xv. Requiring DOL to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential Personal Information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. Requiring DOL to implement logging and monitoring programs sufficient to track traffic to and from DOL's servers; and

xvii. 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

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

DOL'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 report any deficiencies with compliance of the Court's final judgment;

D. An award of damages, including actual, nominal, statutory, consequential, and punitive damages, as allowed by law;

E. An award of attorney's fees, costs, and expenses, as permitted by law;

F. An award of pre-judgment and post-judgment interest, as permitted by law;

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

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

DATED this 6th day of May, 2022.

Respectfully Submitted,

/s/ Timothy W. Emery

TIMOTHY W. EMERY
WSBA No. 34078
PATRICK B. REDDY
WSBA No. 34092
EMERY REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
Phone: (206) 442-9106
Fax: (206) 441-9711
Email: emeryt@emeryreddy.com
Email: reddyp@emeryreddy.com

M. ANDERSON BERRY*
CLAYEO C. ARNOLD, A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Phone: (916) 239-4778
Fax: (916) 924-1829
Email: aberry@justice4you.com

**pro hac vice application forthcoming*

TOUSLEY BRAIN STEPHENS PLLC

By: *s/ Kim D. Stephens P.S.*
Kim D. Stephens, P.S., WSBA #11984
kstephens@tousley.com
Jason T. Dennett, WSBA #30686
jdennett@tousley.com
Kaleigh N. Powell, WSBA #52684
kpowell@tousley.com
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
Tel: 206.682.5600
Fax: 206.682.2992

Attorneys for Plaintiffs and the Proposed Class