FILED
2025 MAR 20 12:21 PM
KING COUNTY
SUPERIOR COURT CLERK
E-FILED
CASE #: 25-2-04060-7 SEA

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

BENJAMIN FITCH, JORDAN ARONSON, and, KATHRYN ROYSE individually and on behalf of all others similarly situated, Plaintiffs, v. SEATTLE PUBLIC SCHOOLS, a Washington school district; FEDERAL WAY PUBLIC SCHOOLS, a Washington school district; CARRUTH COMPLIANCE CONSULTING, INC., a foreign profit corporation; and DOES 1-20, as yet unknown Washington entities, Defendants.	No. 25-2-04060-7 SEA **FIRST AMENDED CLASS ACTION COMPLAINT**

Plaintiffs Benjamin Fitch, Jordan Aronson, and Kathryn Royse (together, "Plaintiffs"), individually and on behalf of all others similarly situated, by and through their counsel, bring this First Amended Class Action Complaint against Defendants Seattle Public Schools ("SPS"), Federal Way Public Schools ("FWPS") and Carruth Compliance Consulting, Inc. ("CCC") (together, "Defendants") and allege, upon personal knowledge as to their own actions and their counsel's investigation, and upon information and belief as to all other matters, as follows:

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

I. INTRODUCTION

1. This class action arises out of the recent data breach ("Data Breach") on CCC's network which resulted in the unauthorized access of highly sensitive data.

2. Plaintiffs and Class Members were required to provide Defendants with their confidential and sensitive information to participate in retirement savings plans.

3. Defendants failure to maintain adequate security protocols in storing and/or transferring Plaintiffs and Class Members confidential and sensitive information, allowed, hackers to infiltrate CCC's computer systems and steal Plaintiffs' and Class Members' highly sensitive personally identifiable information ("PII") and protected health information ("PHI") (PII and PHI are herein together referred to as "Personal Information" or "PI").

II. JURISDICTION AND VENUE

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

5. This Court has personal jurisdiction over SPS because it is a school district of the State of Washington.

6. This Court has personal jurisdiction over FWPS because it is a school district of the State of Washington.

7. This Court has jurisdiction over CCC because it is a foreign profit corporation that is licensed to do business, and regularly transacts business, in the State of Washington.

8. Venue is proper in this Court pursuant to RCW 4.12.020(3) and RCW 4.92.010(1) because the cause action arose in King County, Washington.

9. Federal jurisdiction is inappropriate under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(4)(A), because: (a) greater than two-thirds of the putative Class Members are residents of Washington, or were residents of Washington, at all times relevant to this matter; (b) SPS is a Washington school district that regularly transacts business within Washington; (c) CCC is a foreign profit corporation licensed to do business in Washington; (d) the alleged conduct of

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

Defendants occurred within Washington; (e) the injuries to Plaintiffs and the Class occurred within Washington; and (f) during the three-year period preceding the filing of this action, no other class action has been filed asserting the same or similar factual allegations against Defendants on behalf of the same persons. Alternatively, federal jurisdiction is inappropriate under the Class Action Fairness Act because: (a) pursuant to 28 U.S.C. § 1332 (d)(4)(B), more than two-thirds of the Class reside in Washington; and (b) pursuant to 28 U.S.C. § 1332(2), the amount in controversy does not exceed the sum or value of $5,000,000, exclusive of interest and costs.

III. PARTIES

10. Plaintiff Benjamin Fitch is an individual and is a resident of Shoreline, King County, Washington.

11. Plaintiff Jordan Aronson is an individual and resident of Shoreline, King County, Washington.

12. Defendant Seattle Public Schools is a school district of the State of Washington with its main office located at 2445 3rd Avenue S, Seattle, Washington 98134.

13. Defendant Federal Way Public Schools is a school district of the State of Washington with its main office located at 33330 8th Ave South, Federal Way, Washington 98005.

14. Defendant Carruth Compliance Consulting, Inc. is a foreign profit corporation that is registered to, and does, transact business in King County, Washington.

15. Plaintiffs are currently unaware of the true names and capacities of the defendants sued herein under fictitious names Does 1-20, inclusive, and therefore sues such defendants by such fictitious names. Plaintiffs will seek leave to amend this Complaint to allege the true names and capacities of the fictitiously named defendants when their true names and capacities have been ascertained. Plaintiffs are informed and believe, and thereon allege, each of the fictitiously

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

named defendants is legally responsible in some manner for the events and occurrences alleged herein, and for the damages suffered by Plaintiffs and the Class.

IV. FACTUAL BACKGROUND

Defendants' Business

16. SPS is the largest K-12 school system in Washington State, serving approximately 49,226 students with approximately 6,486 school-based staff.[1] SPS has engaged CCC since 2008 as a third-party administrator for its employees and former employees retirement savings plans.[2]

17. On information and belief, as part of its business practices, and as a condition of employment, SPS requires employees to provide sensitive Personal Information to SPS.

18. SPS made promises and representations to Plaintiffs and Class Members that their Personal Information collected as part of SPS's business operations would be kept safe, confidential, and that the privacy of that information would be maintained.[3]

19. Specifically, SPS's *Data Privacy Policy* provides that:

> It is the policy of the Seattle School Board that District employees and other authorized individuals are responsible for maintaining an environment where student, parent/guardian, volunteer, and employee information, data, and/or records are protected. Data and/or records means any personally identifiable information collected or maintained for district purposes, including in whatever form it is communicated (e.g., verbal, electronic, or paper).
>
> All activities involving information, data, and/or records, including the creation, content, maintenance, access, release, use, retention, and destruction of information, data, and/or records, must follow applicable federal and state laws and the district's policies and procedures. Third parties who are granted access to personally identifiable information are also required to comply with all laws and district policies and procedures.
>
> District employees and other authorized individuals with access to personally identifiable information have the responsibility of protecting it and must take precautions to protect the visibility and accessibility of the information. Employees should be aware of their surroundings and/or type of communications used when discussing sensitive or confidential information verbally or in writing. Any

[1] *See* About Seattle Public Schools, www.seattleschools.org/about/ (last visited Feb. 10, 2025).
[2] *See* https://www.seattleschools.org/news/carruth-data-breach (last visited Feb. 10, 2025).
[3] *See* "Data Privacy" https://www.seattleschools.org/about/school-board/policies/6501-data-privacy/ (last visited Feb. 10, 2025).

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

perceived or confirmed information, data, and/or record breach must be reported immediately.[4]

20. FWPS is a K-12 school system in Washington State, serving approximately 21,000 students with approximately 3,000 school-based staff.[5]

21. FWPS has engaged CCC as a third-party administrator for its employees and former employees retirement savings plans.[6] It is unclear as to how long FWPS has engaged CCC as a third-party administrator, however FWPS has indicated "This data breach potentially impacts all employees who have been employed by Federal Way Public Schools dating back to the late 1990's, regardless of whether they had a 403(b) account" indicating that FWPS may have engaged CCC since at least the late 1990s.[7]

22. On information and belief, as part of its business practices, and as a condition of employment, FWPS requires employees to provide sensitive Personal Information to FWPS.

23. FWPS made promises and representations to Plaintiffs and Class Members that their Personal Information collected as part of FWPS' business operations would be kept safe, confidential, and that the privacy of that information would be maintained.[8]

24. CCC provides third-party administrative services to public school districts including management of retirement savings plans.[9]

25. On information and belief, CCC collects and maintains the PI of current and past SPS employees, including Plaintiffs and Class Members, including, but not limited to their full names, Social Security numbers, financial account information, driver's license numbers, W-2

---

[4] *Id*.
[5] *See* https://www.fwps.org/ (last visited Mar. 17, 2025).
[6] *See* https://www.fwps.org/carruth-update (last visited Mar. 17, 2025).
[7] *Id.*
[8] *See generally* FWPS' Rights and Responsibilities Handbook which incorporates a variety of data privacy obligations and commitments available at https://www.fwps.org/departments/office-of-equity/rights-and-responsibilities-handbook (last visited Mar. 18, 2025).
[9] *See* https://www.zoominfo.com/c/carruth-compliance-consulting-inc/15403476 (last visited Feb. 10, 2025).

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

information, medical billing information, tax filings, and additional information necessary for CCC to administer retirement savings plans.

26. Plaintiffs and Class Members directly or indirectly entrusted CCC with sensitive and confidential PI, which includes information that is static and can be used to commit a myriad of financial crimes.

27. Due to the highly sensitive and personal nature of the information Defendant's acquire, store, and otherwise have access to, Defendants, upon information and belief, promised to among other things: comply with industry standards regarding data security and the protection of PI; comply with all state and federal laws regarding the protection of PI; keep PI private; and to timely and directly notify individuals if their PI has been disclosed without authorization.

28. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PI, Defendants assumed legal and equitable duties, and knew or should have known that they were responsible for protecting Plaintiff's and Class Members' PI from unauthorized disclosure.

29. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PI.

30. Plaintiffs and Class Members relied on Defendants to implement and follow adequate data security policies and protocols, to keep their PI safe and secure, to use the respective PI solely for business purposes, and to prevent the unauthorized disclosures of the PI.

The Data Breach

31. On or about January 13, 2025, CCC published the following notice on its website ("Notice"):

> **What Happened?** On December 21, 2024, CCC identified suspicious activity that impacted the operability of certain computer systems within our environment. Upon becoming aware of the activity, we immediately began working with third-party specialists to investigate the activity, confirm its impact on our systems, and to determine the scope and extent of the information affected by the activity. The

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

> investigation determined that certain systems on our network were accessed without authorization between December 19, 2024, and December 26, 2024, and during that time, certain files were copied from our systems. CCC then conducted a review to determine what data was potentially copied without authorization. On January 13, 2025, CCC provided notice of this event.
>
> **What Information Was Involved?** The information related to individuals that was potentially affected by this event includes their name and a combination of information, including: Social Security number and financial account information. In more limited circumstances, the information could include individuals' driver's license number, W-2 information, medical billing information (but not medical records), and tax filings.[10]

32. Upon information and belief, the cyber-attack was expressly designed to gain access to private and confidential information of specific individuals, including the immutable Personal Information of Plaintiffs and Class Members.

33. Plaintiffs believe their Personal Information was, or will likely be, posted and/or sold on the dark web by cybercriminals so that they can cash in on their ill-gotten gains.

34. Due to Defendants' inadequate and insufficient data security measures, Plaintiffs and Class Members now face an increased risk of fraud and identity theft and must live with that threat forever.

35. Since the Data Breach happened, Plaintiffs have experienced a significant increase in stress due to concern that their PI has been exposed. This Data Breach has forced Plaintiffs to investigate the Data Breach and will necessitate additional monitoring and investigation for potential identity theft.

36. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' PI, Defendants assumed legal and equitable duties, and knew, or should have known, that they were responsible for protecting Plaintiffs' and Class Members' PI from unauthorized disclosure.

[10] *See* Notice of Data Security Event, http://www.ncompliance.com (last visited Feb. 10, 2025).

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

37. Defendants had obligations created by contract, industry standards, statutory and common law, and their own promises and representations made to Plaintiffs and Class Members, to keep their PI confidential, and to protect it from unauthorized access and disclosure.

38. Plaintiffs and Class Members reasonably relied on Defendants' sophistication to keep their sensitive PI confidential, to maintain adequate network security, to use the information for business purposes only, and to make only authorized disclosures of their Personal Information.

39. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and data breaches of major companies preceding the date of the Data Breach.

40. Defendants knew or should have known that these attacks were common and foreseeable. In 2024, there were 2,850 data breaches, a significant increase above the prior record set in 2021, wherein 1,862 data breaches occurred. Of the 2,850 data breaches, there were approximately 1,246,573,396 victim notices issued, a 211 percent increase from 2023.[11]

41. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets, so they are aware of and prepared for a potential attack. As one report explained, "[e]ntities like smaller municipalities . . . are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[12]

42. The increase in such attacks, and the resulting risk of future attacks, was widely known to the public and to anyone in the Defendants' industry, including Defendants.

Defendants Did Not Use Reasonable Security Procedures

43. Despite this knowledge, Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive, non-encrypted, and non-redacted

[11] *See* Identity Theft Resource Center, 2024 Data Breach Annual Report (Jan. 2025), https://www.idtheftcenter.org/publication/2024-data-breach-report/ (last visited Feb. 10, 2025).

[12] *See* FBI, Secret Service Warn of Targeted, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited Feb. 10, 2025).

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

information they were maintaining for Plaintiffs and Class Members, causing Plaintiffs' and Class Members' PI to be exposed.

44. To prevent and detect cyber-attacks, Defendants could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls, including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have written access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full Office Suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling the Remote Desktop Protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and

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

logical separation of networks and data for different organizational units.[13]

45. To prevent and detect cyber-attacks, Defendants could and should have implemented the following measures, as recommended by the United States Cybersecurity & Infrastructure Agency:

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks.
- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters and keep them updated to reduce malicious network traffic.[14]

46. To prevent and detect cyber-attacks, Defendants could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets
- Apply the latest security updates
- Use threat and vulnerability management
- Perform regular audit
- Remove privileged credentials

Thoroughly investigate and remediate alerts
- Prioritize and treat commodity malware infections as potential full compromise.

Include IT Pros in security discussions
- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely.

Build credential hygiene
- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords.

Apply principle of least-privilege

---

[13] *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.

[14] *See* Cybersecurity & Infrastructure Security Agency, *Protecting Against Ransomware* (Apr. 11, 2019), https://www.cisa.gov/news-events/news/protecting-against-ransomware (last visited Feb. 10, 2025).

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

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[15]

47. Given that Defendants were storing the PI of Plaintiffs and Class Members, Defendants could and should have implemented all the above measures to prevent and detect cyber-attacks.

48. The occurrence of the Data Breach indicates that Defendants failed to adequately implement one or more of the above measures to prevent "hacking" attacks, resulting in the Data Breach and the exposure of the PI of an undisclosed amount of current and former consumers, including Plaintiffs and Class Members.

Securing PI and Preventing Data Breaches

49. Defendants breached their obligations to Plaintiffs and Class Members and/or were otherwise negligent and reckless because they failed to properly maintain and safeguard their computer systems and data. Defendants' 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 protect Plaintiffs' and Class Members' PI;

c. Failing to properly monitor their own data security systems for existing intrusions; and

[15] *See* Microsoft Threat Intelligence, *Human-operated ransomware attacks: A preventable disaster* (Mar. 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Feb. 10, 2025).

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

d. Failing to adhere to industry standards for cybersecurity.

50. Defendants could have prevented this Data Breach by properly securing and encrypting the PI of Plaintiffs and Class Members. Alternatively, Defendants should have implemented and executed proper data disposal protocols to ensure that any data that was no longer necessary or outdated was removed and destroyed.

51. Defendants' negligence in safeguarding the PI of Plaintiffs and Class Members was exacerbated by the repeated warnings and alerts directed to governments and businesses to protect and secure sensitive data.

52. Despite the prevalence of public announcements of data breaches and data security compromises, Defendants failed to take appropriate steps to protect the PI of Plaintiffs and Class Members from being compromised.

Defendants Failed to Comply with FTC Guidelines

53. The Federal Trade Commission (FTC") has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

54. 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.[16] 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

[16] Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Feb. 10, 2025).

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

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.[17]

55. The FTC further recommends that companies not maintain PI longer than is needed 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.

56. 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 Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

57. Defendants failed to properly implement basic data security practices.

58. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' PI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

59. Defendants were always fully aware of their obligation to protect the PI of Plaintiffs and Class Members. Defendants were also aware of the significant repercussions that would result from their failure to do so.

Defendants Failed to Comply with Industry Standards

60. Several best practices have been identified that, at a minimum, should be implemented by entities like Defendants, including but not limited to, educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backing up data;

[17] *Id*.

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

and limiting which employees can access sensitive data. Defendants failed to follow these industry-best practices.

61. Other best cybersecurity practices include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding critical points. Defendants failed to follow these cybersecurity best practices, including failing to train their staff.

62. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

Value of Personally Identifiable Information

63. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[18] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government-issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[19]

64. The PI of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, PI can be sold at a price ranging from $40 to $200, and bank details

[18] 17 C.F.R. § 248.201 (2013).
[19] *Id*.

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

have a price range of $50 to $200.[20] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[21] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[22]

65. Social Security numbers, for example, are among the worst kind of PI to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[23]

66. Moreover, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

67. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link

---

[20] *See Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Feb. 10, 2025).

[21] *See Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Feb. 10, 2025).

[22] *See In the Dark*, VPNOverview (2019), https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Feb. 10, 2025).

[23] Social Security Administration, *Identity Theft and Your Social Security Number*, https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Feb. 10, 2025).

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

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."[24]

68. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x in price on the black market."[25]

69. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security number, Driver's License number, and tax information.

70. Among other forms of fraud, identity thieves may use Social Security numbers to obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

71. Moreover, the fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and between when PI is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

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

[24] *See* Bryan 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-millionsworrying-about-identity-theft (last visited Feb. 10, 2025).

[25] *See* Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Feb. 10, 2025).

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

the harm resulting from data breaches cannot necessarily rule out all future harm. [26]

72. The PI stolen in the Data Breach has significant value, as PI is a valuable property right. [27] Sensitive PII can sell for as much as $363 per record, according to the Infosec Institute.[28]

73. There is also an active, robust, and legitimate marketplace for PI. In 2019, the data brokering industry was worth roughly $200 billion.[29] In fact, the data marketplace is so sophisticated that consumers can sell their non-public information directly to a data broker, who in turn aggregates the information and provides it to marketers or app developers.[30] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $60.00 a year.[31]

74. As a result of the Data Breach, Plaintiffs' and Class Members' PI, which has an inherent market value in both legitimate and black markets, has been damaged and diminished by its unauthorized release to third-party actors, to whom it holds significant value. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the PI is now readily available, and the rarity of Plaintiffs' and Class Members' PI has been lost, thereby causing additional loss of value.

---

[26] *See* Government Accountability Office, *Report to Congressional Requesters*, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf (last visited Feb. 10, 2025).

[27] *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)).

[28] *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 Feb. 10, 2025).

[29] *See* David Lazarus, *Shadowy Data Brokers Make the Most of Their Invisibility Cloak* (Nov. 5, 2019), https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited Feb. 10, 2025).

[30] *See, e.g.*, https://datacoup.com/; https://worlddataexchange.com/about (last visited Feb. 10, 2025).

[31] *See* Computer & Mobile Panel, NIELSEN, https://computermobilepanel.nielsen.com/ui/US/en/sdp/landing (last visited Feb. 10, 2025).

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

75. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the PI of Plaintiffs and Class Members, including names, driver's license numbers, Social Security numbers, and tax information, and of the foreseeable consequences that would occur if Defendants' data security systems and networks were breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

76. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Since the Data Breach, Plaintiffs have experienced a significant uptick in spam calls, text messages, and emails. Beyond the stress and anxiety this situation has caused, Plaintiffs have already devoted and anticipated continuing to devote countless hours to the vigilant monitoring of their identity and financial accounts to mitigate any potential harm. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

77. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants' server(s) and computer network, amounting to potentially tens of thousands of individuals' detailed PI, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

78. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the PI of Plaintiffs and Class Members, including, but not limited to, failing to encrypt sensitive PI, failing to redact sensitive PI, keeping unencrypted and unredacted sensitive PI in internet-facing environments, and failing to delete sensitive PI that the Defendants had no reasonable business purpose for continuing to maintain. The ramifications of Defendants' failure to safeguard the PI of Plaintiffs and Class Members are long-lasting and severe. Once PI is stolen, fraudulent use of that information and damage to victims may continue for years.

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

V. PLAINTIFF-SPECIFIC ALLEGATIONS

Plaintiff Fitch's Experience

79. Plaintiff Fitch is, and at all relevant times has been, a resident and citizen of Shoreline, Washington.

80. Plaintiff Fitch is, and at all relevant times has been an employee of SPS.

81. Plaintiff Fitch provided his PI to Defendants, directly or indirectly, as a condition of employment and receiving retirement benefits.

82. In providing his PI to Defendants, Plaintiff Fitch trusted that Defendants would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law.

83. Plaintiff Fitch is very careful about storing and sharing his PI.

84. Plaintiff Fitch first learned of the Data Breach after receiving an email regarding the Data Breach from SPS, advising that his PI was compromised in the Data Breach.

85. Since the Data Breach Plaintiff Fitch has received a significant amount of suspicious spam emails, phone calls, and texts.

86. Plaintiff Fitch has received notification that his PI was found on the dark web.

87. As a result of the Data Breach, Plaintiff Fitch has been forced to spend time dealing with and responding to the direct consequences of the Data Breach. This is uncompensated time that has been lost forever and cannot be recaptured.

88. Plaintiff Fitch suffered actual injury from having his PI compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PI, a form of property that Defendant maintained belonging to Plaintiff; (b) violation of his privacy rights; (c) the theft of his PI; and (d) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

89. As a result of the Data Breach, Plaintiff Fitch has also suffered emotional distress as a result of the release of the PI, which he believed would be protected from unauthorized access

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

and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his PI for purposes of identity theft and fraud. Plaintiff Fitch is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

Plaintiff Aronson's Experience

90. Plaintiff Aronson is, and at all relevant times, has been a resident and citizen of Shoreline, Washington.

91. Plaintiff Aronson is, and at all relevant times has been an employee of SPS.

92. Plaintiff Aronson provided her PI to Defendants, directly or indirectly, as a condition of employment and receiving retirement benefits.

93. In providing her PI to Defendants, Plaintiff Aronson trusted that Defendants would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law.

94. Plaintiff Aronson is very careful about storing and sharing her PI.

95. Plaintiff Aronson first learned of the Data Breach after receiving an email regarding the Data Breach from SPS, advising that her PI was compromised in the Data Breach.

96. As a result of the Data Breach, Plaintiff Aronson has been forced to spend time dealing with and responding to the direct consequences of the Data Breach. This is uncompensated time that has been lost forever and cannot be recaptured.

97. Plaintiff Aronson suffered actual injury from having her PI compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her PI, a form of property that Defendant maintained belonging to Plaintiff; (b) violation of her privacy rights; (c) the theft of her PI; and (d) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

98. Aa result of the Data Breach, Plaintiff Aronson has also suffered emotional distress as a result of the release of her PI, which she believed would be protected from unauthorized access and disclosure, including stress about unauthorized parties viewing, selling, and/or using

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

her PI for purposes of identity theft and fraud. Plaintiff Aronson is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

Plaintiff Royse's Experience

99. Plaintiff Royse is, and at all relevant times, has been a resident and citizen of Auburn, Washington.

100. Plaintiff Royse is, and at all relevant times has been an employee of FWPS.

101. Plaintiff Royse provided her PI to Defendants, directly or indirectly, as a condition of employment and receiving retirement benefits.

102. In providing her PI to Defendants, Plaintiff Royse trusted that Defendants would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Plaintiff Aronson is very careful about storing and sharing her PI.

103. Plaintiff Royse first learned of the Data Breach after receiving an email regarding the Data Breach from FWPS, advising that her PI was compromised in the Data Breach.

104. As a result of the Data Breach, Plaintiff Royse has been forced to spend time dealing with and responding to the direct consequences of the Data Breach. This is uncompensated time that has been lost forever and cannot be recaptured.

105. Plaintiff Royse suffered actual injury from having her PI compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her PI, a form of property that Defendant maintained belonging to Plaintiff; (b) violation of her privacy rights; (c) the theft of her PI; and (d) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

106. Aa result of the Data Breach, Plaintiff Royse has also suffered emotional distress as a result of the release of her PI, which she believed would be protected from unauthorized access and disclosure, including stress about unauthorized parties viewing, selling, and/or using her PI for purposes of identity theft and fraud. Plaintiff Royse is very concerned about identity

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

theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

VI. CLASS ACTION ALLEGATIONS

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

> All individuals residing in Washington whose personal information was compromised in the data breach disclosed by Carruth Compliance Consulting, Inc. in January 2025.

108. Excluded from the Class are the following: Defendants and Defendants' parents, subsidiaries, affiliates, officers, and directors, and any judge to whom this case is assigned, as well as his or her staff and immediate family.

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

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

111. Numerosity. While the exact number of Class Members is unknown to Plaintiffs at this time, on information and belief, the Class is likely to consist of at least tens of thousands of members—far too many to join in a single action.

112. Ascertainability. Class Members are readily identifiable from information in Defendants' possession, custody, or control.

113. Typicality. Plaintiffs' claims are typical of Class Members' claims, as each arise from the same Data Breach, the same alleged negligence of, breach and/or the same statutory violations by Defendants.

114. 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 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.

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

115. 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 Defendants 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 Defendants' conduct was negligent; and (c) Whether Plaintiffs and the Class are entitled to damages and/or injunctive relief.

116. 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 Defendants' privacy practices economically feasible in the absence of the class action procedure.

117. In the alternative, class certification is appropriate because Defendants have 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.

118. The aggregate amount in controversy of the claims of all Class Members, exclusive of interest and costs, does not exceed the sum or value of $5,000,000.

VII. CAUSES OF ACTION

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

119. Plaintiffs incorporate by reference all foregoing factual allegations.

120. Defendants 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

121. Defendants failed to inform Plaintiffs and the Class that their systems were inadequate to safeguard sensitive information, and that transferring Personal Information could lead to attackers gaining access to their sensitive information.

122. 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.

123. Defendants failed to implement and maintain adequate security practices and procedures to prevent the Data Breach.

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

125. 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.

126. Defendants' duty of care arose as a result of their knowledge that individuals trusted them to protect the confidential data that they provided to them. Only the Defendants were in a position to ensure that their own protocols were sufficient to protect against the harm to Plaintiffs and the Class from a data breach of their own systems.

127. Defendants also had a duty to use reasonable care in protecting confidential data because they committed to comply with industry standards for the protection of Personal Information and committed to the public to protect the privacy of information the employees provided to the Defendants.

128. Defendants knew, or should have known, of the vulnerabilities in their security practices and procedures, and the importance of adequate security to the employees and the owners of sensitive data.

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

129. Plaintiffs and the Class have suffered harm as a result of Defendants' 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.

SECOND CAUSE OF ACTION
VIOLATION OF THE WASHINGTON CONSUMER PROTECTION ACT, RCW 19.86
Claim of Relief for Plaintiffs and the Class and Against Defendant CCC

130. Plaintiffs incorporate by reference all foregoing factual allegations.

131. CCC is a "person" within the meaning of the Washington Consumer Protection Act, RCW 19.86.010(1), and it conducts "trade" and "commerce" within the meaning of RCW 19.86.010(2). Plaintiffs and Class Members are "persons" within the meaning of RCW 19.86.010(1).

132. CCC's failure to safeguard the Personal Information exposed in the Data Breach constitutes an unfair act that offends public policy.

133. CCC's failure to safeguard the Personal Information compromised in the Data Breach caused substantial injury to Plaintiffs and the Class. CCC's failure is not outweighed by any countervailing benefits to consumers or competitors, and it was not reasonably avoidable by consumers.

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

135. As a direct and proximate result of CCC's unfair acts or practices, Plaintiffs and the Class suffered injury-in-fact.

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

136. As a result of CCC's conduct, Plaintiffs the Class have suffered actual damages, including the lost value of their Personal Information; the lost value of their personal data and lost property in the form of their breached and compromised Personal Information (which is of great value to third parties); ongoing, imminent, and certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen Personal Information; the illegal sale of the compromised data on the dark web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

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

THIRD CAUSE OF ACTION
UNJUST ENRICHMENT
Claim of Relief for Plaintiffs and the Class and Against Defendants

138. Plaintiffs incorporate by reference all foregoing factual allegations.

139. Plaintiffs and Class Members conferred a monetary benefit to Defendants by providing Defendants with their valuable PI and putting money into retirement accounts. In so conferring this benefit, Plaintiff and Class Members understood that part of the benefit derived by Defendants from the PI would be applied to data security efforts to safeguard the PI.

140. Defendants knew that Plaintiffs and Class Members conferred a monetary benefit to Defendants by entering into a professional or business relationship. Defendants acknowledged and retained this benefit when they accepted the terms of this relationship with Plaintiffs and Class Members.

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

141. Instead of providing a reasonable level of data security which would have prevented the Data Breach, Defendants chose to use less costly ineffective data security measures. Plaintiffs and Class Members suffered as a direct and proximate result of Defendant's ineffective security measures.

142. Defendants should not be permitted to retain any monetary benefit as a result of their failure to implement necessary security measures to protect the Personal Information of Plaintiffs and Class Members.

143. Defendants gained access to Plaintiffs' and Class Members' Personal Information through inequitable means because Defendants failed to disclose that they used inadequate security measures.

144. Plaintiffs and Class Members were unaware of the inadequate security measures and would not have provided their Personal Information to Defendants had they known of the inadequate security measures.

145. To the extent that this cause of action is pleaded in the alternative to the others, Plaintiffs and Class Members have no adequate remedy at law.

146. As a direct and proximate result of Defendants' 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 Personal Information is used; (iii) the compromise and/or theft of their Personal Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Personal 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 tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Personal Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants

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

fail to undertake appropriate and adequate measures to protect the Personal Information of Plaintiffs and Class Members; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Personal Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

147. As a direct and proximate result of Defendants' conduct, 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.

FOURTH CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
Claim of Relief for Plaintiffs and the Class and Against Defendants

148. Plaintiffs incorporate by reference all foregoing factual allegations.

149. Plaintiffs and the Class Members, who are employees of SPS, delivered their PI to Defendants as part of the process of receiving employee benefits.

150. Upon providing their Personal Information in exchange for receiving employee benefits, Plaintiffs and Class Members entered into implied contracts with Defendants under which Defendants agreed to safeguard and protect such information and to timely and accurately notify Plaintiffs and Class Members if and when their data had been breached and compromised. Each such contractual relationship imposed on Defendants an implied covenant of good faith and fair dealing by which Defendants were required to perform their obligations and manage Plaintiffs' and Class Members' Personal Information in a manner which comported with the reasonable expectations of privacy and protection attendant to entrusting such data to Defendants.

151. In providing their Personal Information, Plaintiffs and Class Members entered into an implied contract with Defendants whereby Defendants, in receiving such data, became obligated to reasonably safeguard Plaintiffs' and the other Class Members' Personal Information.

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

152. In delivering their Personal Information to Defendants, Plaintiffs and Class Members intended and understood that Defendants would adequately safeguard that data.

153. Plaintiffs and the Class Members would not have entrusted their Personal Information to Defendants in the absence of such an implied contract.

154. Defendants accepted possession of Plaintiffs' and Class Members' personal data for the purpose of providing employee benefit services to Plaintiffs and Class Members.

155. Had Defendants disclosed to Plaintiffs and Class Members that Defendants did not have adequate computer systems and security practices to secure their Personal Information, Plaintiffs and Class Members would not have provided their Personal Information to Defendants.

156. Defendants recognized that Personal Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiffs and Class Members.

157. Plaintiffs and the Class fully performed their obligations under the implied contract with Defendants.

158. Defendants breached the implied contract with Plaintiffs and Class Members by failing to take reasonable measures to safeguard their data.

159. As a direct and proximate result of the breach of the contractual duties, Plaintiffs and Class Members have suffered actual, concrete, and imminent injuries. The injuries suffered by Plaintiffs and the Class Members include: (a) invasion of privacy; (b) the compromise, disclosure, theft, and unauthorized use of Plaintiffs' and Class Members' Personal Information; (c) economic costs associated with the time spent to detect and prevent identity theft, including loss of productivity; (d) monetary costs associated with the detection and prevention of identity theft; (e) economic costs, including time and money, related to incidents of actual identity theft; (f) the emotional distress, fear, anxiety, nuisance and annoyance of dealing related to the theft and compromise of their Personal Information; (g) the diminution in the value of the services bargained for as Plaintiffs and Class Members were deprived of the data protection and security

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

that Defendants promised when Plaintiffs and the Class Members entrusted Defendants with their Personal Information; and (h) the continued and substantial risk to Plaintiffs' and Class Members' Personal Information, which remains in the Defendants' possession with inadequate measures to protect such Personal Information.

VIII. PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of the Class, request that the Court enter judgment against Defendants 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 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 Defendants from engaging in the wrongful and unlawful acts described herein;

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

iii. Requiring Defendants to delete, destroy, and purge the Personal Information of Plaintiffs and Class Members unless Defendants 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 Defendants 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 Defendants from maintaining the Personal Information of Plaintiffs and Class Members on a cloud-based database;

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

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

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

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

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

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

xi. Requiring Defendants 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 Defendants 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 Defendants to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding

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

subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting Personal Information;

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

xv. Requiring Defendants to meaningfully educate Plaintiffs and 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 Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' 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 Defendants' 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;

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

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

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

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

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

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

DATED this 20th day of March 2025.

Respectfully Submitted,

By: */s/ Timothy W. Emery*

Timothy W. Emery, WSBA No. 34078
Patrick B. Reddy, WSBA No. 34092
Brook E. Garberding, WSBA No. 37140
Paul Cipriani, WSBA No. 59991
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
Email: brook@emeryreddy.com
Email: paul@emeryreddy.com

M. Anderson Berry, WSBA No. 63160
Gregory Haroutunian (*pro hac vice forthcoming)*
CLAYEO C. ARNOLD
A PROFESSIONAL CORPORATION
865 Howe Avenue
Sacramento, CA 95825
Phone: (916) 239-4778
Fax: (916) 924-1829
Email: aberry@justice4you.com
Email: gharoutunian@justice4you.com

Attorneys for Plaintiffs