E-FILED
06-16-2025, 14:43
Scott G. Weber, Clerk
Clark County

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

JAMES REESE, ON BEHALF OF HIMSELF and all others similarly situated, Plaintiff, v. CLARK COUNTY, WASHINGTON, Defendant.	No. 25-2-02214-06 **CLASS ACTION COMPLAINT**

ORIGINAL COMPLAINT—CLASS ACTION

Plaintiff James Reese ("Plaintiff"), through his attorneys, individually and on behalf of all others similarly situated, sues Clark County, Washington, ("Clark" or "Defendant"), to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations upon information and belief, except as to his own actions, the investigation of his counsel, and the facts that are a matter of public record.

I. INTRODUCTION

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

1. This class action arises out of the recent data security incident and data breach that was perpetrated against Defendant, (the "Data Breach"), which held in its possession certain sensitive personally identifiable information ("PII") and protected health information ("PHI") (collectively, the "Private Information"), of Plaintiff and other current and former residents of Defendant, the putative class members ("Class"). This Data Breach occurred between October 16, 2023, and October 21, 2023.

2. Clark County, Washington is among the fastest-growing counties in Washington, experiencing rapid increases in population, employment and housing.[1]

3. The Private Information compromised in the Data Breach included certain Private Information of Defendant's current and former residents, including Plaintiff. According to the notice of data event that Defendant Clark posted on its website states that this Private Information included but is not limited to "individual's names, Social Security numbers, government-issued identification numbers, dates of birth, financial account information, payment card information, and medical or health insurance information."[2]

4. As of the filing of Plaintiff's original Complaint, Defendant's data breach does not appear on the HHS list of cases currently under investigation.[3]

5. The Private Information was acquired by cyber-criminals who perpetrated the attack and remains in the hands of those cyber-criminals.

6. The Data Breach resulted from Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect individuals' Private Information with which they were entrusted.

---

[1] Clark County, Washington, "*About Clark County"* https://clark.wa.gov/county-manager/about-clark-county (last visited June 13, 2025).

[2] Clark County, Washington, "*Notice of data event" https://clark.wa.gov/communications/news-updates* (last visited June 13, 2025).

[3] *See* U.S. Department of Health and Human Services, Cases Currently Under Investigation, *available at* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited June 4, 2025).

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

7. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that they collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information was subjected to unauthorized access by an unknown third party and precisely what specific type of information was accessed.

8. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

9. Defendant, through its employees, disregarded the rights of Plaintiff and Class Members (defined below) by, among other things, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions.

10. Defendant also failed to disclose that it did not have adequately robust computer systems and security practices to safeguard Plaintiff' and Class Members' Private Information and failed to take standard and reasonably available steps to prevent the Data Breach.

11. In addition, Defendant's employees failed to properly monitor the computer network and systems that housed the Private Information. Had Defendant's employees (presumably in the IT department) properly monitored its property, it would have discovered the intrusion sooner.

12. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained is now in the hands of data thieves.

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

13. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes. These crimes include opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, filing false medical claims using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

14. Because of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft.

15. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

16. Plaintiff and Class Members may also incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

17. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of himself, and all similarly situated individuals whose Private Information was accessed during the Data Breach.

18. Plaintiff seek remedies including, but not limited to, compensatory damages, punitive damages, nominal damages, restitution, injunctive and declaratory relief, reasonable attorneys' fees and costs, and all other remedies this Court deems just and proper.

19. Accordingly, Plaintiff sues Defendant seeking redress for its unlawful conduct and asserting claims for: (i) negligence, (ii) breach of implied contract, and (iii) unjust enrichment.

II. PARTIES

20. Plaintiff James Reese is and at all times mentioned herein was an individual citizen of Washington, residing in the city of Battle Ground.

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

21. Plaintiff provided Defendant with his sensitive Private Information as a condition of being a resident of Defendant and to obtain services from Defendant.

22. Plaintiff received notice of the Data Breach around May 29, 2025, informing him that his sensitive information was part of Defendant's Data Breach. ***See*** **Exhibit A.**

23. Defendant can be served through its registered agent and/or Clark County Clerk, Scott G. Weber, located at the Clark County Courthouse, 1200 Franklin Street, Vancouver, Washington 98660.

III. JURISDICTION AND VENUE

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

25. This Court has personal jurisdiction over Defendant because Defendant is a political subdivision of the State of Washington and resides for purposes of venue and jurisdiction in Clark County, Washington.

26. Venue is proper in this Court pursuant to RCW 4.12.020(3) and RCW 4.92.010 because a substantial part of the events or omissions giving rise to Plaintiff's and Class Members' claims occurred in this county and because Defendant resides in this county.

27. 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) Defendant is a county that regularly transacts business, and is headquartered, within Washington; (c) the alleged conduct of Defendant occurred within Washington; (d) the injuries to Plaintiff and the Class occurred within Washington; and (e) 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 Defendant 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)

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

pursuant to 28 U.S.C. § 1332(d)(2), the amount in controversy does not exceed the sum or value of $5,000,000, exclusive of interest and costs.

IV. FACTUAL ALLEGATIONS

A. Defendant's Business

28. Clark County is a county in the southwestern corner of Washington State, just across the Columbia River from Portland, Oregon. It's the fifth-most populous county in Washington, with a population of 503,311 as of the 2020 census. Vancouver is the county seat and largest city.[4]

29. Plaintiff and Class Members are current and former residents (collectively "residents") of Defendant.

30. In the ordinary course of business, Defendant's residents are encouraged and/or are mandated to provide the Defendant's (and Plaintiff did provide) Defendant with sensitive, personal, and private information, such as his or her:

a. name;

b. date of birth;

c. Social Security numbers;

d. medical information;

e. government-issued identification numbers;

f. financial account information;

g. payment card information

h. health insurance information.

31. Defendant stored this Private Information in its information technology computer systems and servers.

---

[4] Oregon Secretary of State, *"Clark County History and Records" https://sos.oregon.gov/archives/records/provisional-guide/Pages/record-inventory-clark.aspx#:~:text=Clark%20County%20was%20created%20as,near%20the%20fort%20in%201825.* (last accessed on June 5, 2025).

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

32. All of Defendant's employees, staff, entities, sites, and locations may share residents' information with each other for various purposes, as should be disclosed in a HIPAA compliant privacy notice ("Privacy Policy") that Defendant maintains.

33. Upon information and belief, Defendant's HIPAA Privacy Policy is provided to every resident prior to receiving services, and upon request.

34. Defendant agreed to and undertook legal duties to maintain the personal information entrusted to it by Plaintiff and Class Members safely, confidentially, and in compliance with all applicable contractual obligations, laws, regulations, including but not limited to HIPAA, and common law.

35. The residents' information held by Defendant in its computer systems and networks included the Private Information of Plaintiff and Class Members.

36. Defendant had an obligation created by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act"), HIPAA (45 C.F.R. § 160.102), industry standards, state law, and representations made to Plaintiff and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

37. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known it was responsible for protecting Plaintiff's and Class Members' Private Information from disclosure.

B. The Data Breach

38. A Data Breach typically occurs when unauthorized individuals, akin to cyber criminals, intend to and successfully do act to access and steal Private Information that has not been adequately secured by public entities like Defendant.

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

39. On May 29, 2025, Defendant mailed Plaintiff and Class Members a Notice[5] that stated in part:

> **What happened?** On October 21, 2023, Clark County detected suspicious activity on our computer network and determined that some systems were encrypted by malware. Upon identifying the activity, Clark County took quick steps to bring the network offline, ensure the security of our systems, and launch an investigation into the nature and scope of the event. The investigation determined that an unknown actor gained access to Clark County systems between October 16, 2023, and October 21, 2023, and accessed and/or stole data stored on certain Clark County
> …
>
> **What Information Was Involved?** Based on the review, the information related to you that may be involved in this event includes your name and: date of birth and Social Security number. Please note, there is currently no evidence of actual or attempted misuse of your information in connection with this event.

40. The U.S. Department of Health and Human Services requires, "[i]f a breach of unsecured protected health information affects *500 or more individuals*, a covered entity must notify the Secretary of the breach without unreasonable delay and *in no case later than 60 calendar days* from the discovery of the breach."[6] Further, if "the number of individuals affected by a breach is uncertain at the time of submission, the covered entity should provide an estimate," and later provide an addendum or correction to HHS.[7]

41. As of the filing of Plaintiff's original Complaint, Defendant's data breach does not appear on the HHS list of cases currently under investigation.[8]

42. Plaintiff's notice letter was dated May 29, 2025 —more than seven months after the Data Breach.

---

[5] *See* Behavioral Health Resources, Public Notice of Incident available at: http://www.bhr.org/wp-content/uploads/2025/04/BHR-Updated-Website-Notice.pdf (last visited at April 25, 2025).

[6] U.S. Department of Health and Human Services, *Submitting Notice of a Breach to the Secretary* (Feb. 27, 2023) https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html (last viewed June 45, 2025).

[7] *Id.*

[8] *See* U.S. Department of Health and Human Services, Cases Currently Under Investigation, *available at* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (*last visited* June 4, 2025).

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

43. Defendant had obligations created by HIPAA, contract, industry standards, state law, common law, and representations made to Plaintiff and Class Members, to keep Plaintiff's and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

44. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

45. Defendant's data security obligations were particularly important given the substantial increase in Data Breaches targeting personal identifying information preceding the date of the breach.

46. In 2023, a record 3,205 data breaches occurred, resulting in around 353,027,892 individuals' information being compromised, a 78% increase from 2022.[9] Of the 2023 recorded data breaches, 809 of them, or 25% were in the medical or healthcare industry.[10]The 809 reported breaches reported in 2023 exposed nearly 56 million sensitive records, compared to only 343 breach that exposed just over 28 million sensitive records in 2022. [11]

47. Data breaches such as the one experienced by Defendant 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.

48. In fact, according to the cybersecurity firm Mimecase, 90% of health care organization experienced cyberattacks in the past year.[12]

---

[9] *See* Identity Theft Resource Center, *2023 Data Breach Report* (January2024), *available at* https://www.idtheftcenter.org/publication/2023-data-breach-report/ (last visited June 5, 2025).

[10] *Id.*

[11] *Id.* at 11, Fig. 3.

[12] Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack, Security Magazine* (Nov. 23, 2020), *available at* https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last visited June 5, 2025).

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

49. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public, including Defendant.

C. Data Breaches are Preventable

50. Defendant failed to use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

51. Defendant could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting its equipment and computer files containing Private Information.

52. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[13]

53. To prevent and detect cyber-attacks and/or ransomware attacks, Defendant 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.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- 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.

[13] How to Protect Your Networks from RANSOMWARE, at 3, available at: https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited June 5, 2025).

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

- 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 write 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 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 logical separation of networks and data for different organizational units.[14]

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

Secure Internet-Facing Assets

- Apply latest security updates

[14] *Id.* at 3-4.

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

- 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

- 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]

[15] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at:* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last viewed June 5, 2025).

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

55. Given that Defendant was storing the Private Information of its current and former residents Defendant could and should have implemented all the above measures to prevent and detect cyberattacks.

56. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and data thieves acquiring and accessing the Private Information of, upon information and belief, at least thousands to tens of thousands of individuals, including that of Plaintiff and Class Members.

D. Defendant Acquires, Collects & Stores Members' Private Information

57. Defendant acquires, collects, and stores a massive amount of Private Information on its current and former residents

58. As a condition of becoming a resident of Defendant, Defendant requires all residents to entrust it with highly sensitive personal information of various types.

59. By obtaining, collecting, and using Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from disclosure.

60. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and would not have entrusted it to Defendant absent a promise to safeguard that information.

61. Upon information and belief, while collecting Private Information from residents, including Plaintiff, Defendant promised to provide confidentiality and adequate security for their data through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

62. Plaintiff and the Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

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

E. Value Of Private Information

63. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[16] 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."[17]

64. Washington similarly defines identity theft as "knowingly obtain[ing], possess[ing], use[ing] or transfer[ing] a means of identification or financial information of another person, living or dead, with the intent to commit, or to aid or abet, any crime "

65. The PII 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.[18]

66. For example, Personal Information can be sold at a price ranging from $40 to $200.[19] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[20]

67. Theft of PHI is gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get

---

[16] 17 C.F.R. § 248.201 (2013).

[17] *Id.*

[18] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last viewed June 5, 2025).

[19] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last viewed June 5, 2025).

[20] *In the Dark*, VPN Overview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last viewed June 5, 2025).

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

other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[21]

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

69. 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 also between when Private Information 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 the harm resulting from data breaches cannot necessarily rule out all future harm.[22]

70. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

71. Defendant Fails to Comply with FTC Guidelines

72. The FTC has promulgated many guides for businesses which show how important it is to implement reasonable data security practices. According to the FTC, the need for data security should shape all business decision-making.

73. 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 Private Information that they keep; properly

---

[21] Medical I.D. Theft, E-Fraud Prevention, available at https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20your,credit%20report%20may%20be%20affected. (last visited June 5, 2025).

[22] *Report to Congressional Requesters, GAO, at 29 (June 2007), available at: https://www.gao.gov/assets/gao-07-737.pdf (last visited* June 5, 2025).

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

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.[23] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor incoming traffic for activity suggesting 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.[24]

74. The FTC further recommends that companies not maintain PII 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.

75. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient data, by 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 also clarify the measures businesses must take to meet their data security obligations.

76. These FTC enforcement actions include actions against defendants that failed to properly implement basic data security practices.

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

---

[23] Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (2016), *available at* www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited June 5, 2025).

[24] *Id.*

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

78. Defendant was always fully aware of its obligation to protect the Private Information of its residents. Defendant was also aware of the significant repercussions that would result from its failure to do so.

F. Defendant Fails to Comply with Industry Standards

79. As shown above, experts studying cyber security routinely identify entities that maintain PII and PHI data as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

80. Several best practices have been identified that at a minimum should be implemented by public entities like Defendant, including, but not limited to, educating all employees; using strong passwords; creating multi-layer security, including firewalls, antivirus, and anti- malware software; encryption, making data unreadable without a key; using multi-factor authentication; protecting backup data; and limiting which employees can access sensitive data.

81. Other best cybersecurity practices that are standard for public entities 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 protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

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

83. These foregoing frameworks are existing and applicable industry standards, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

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

G. Defendant's Conduct Violates HIPAA and Reveals Its Insufficient Data Security

84. HIPAA requires covered entities such as Defendant to protect against reasonably anticipated threats to the security of sensitive health information.

85. Covered entities must implement safeguards to ensure the confidentiality, integrity and availability of PHI. Safeguards must include physical, technical, and administrative components.

86. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PHI like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include: 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. §164.312(a)(1); 45 C.F.R. § 164.308(A)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D); and 45 C.F.R. § 164.530(b).

87. A Data Breach such as the one Defendant experienced is considered a breach under the HIPAA rules because there is an access of PHI not permitted under the HIPAA Privacy Rule. *See* 45 C.F.R. 164.402 (Defining "Breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under [the HIPAA Privacy Rule] which compromises the security or privacy of the protected health information.")

88. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate it failed to meet standards mandated by HIPAA regulations.

V. DEFENDANT'S BREACH

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

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

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

b. Failing to adequately protect residents' Private Information;

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

d. Failing to ensure that vendors with access to Defendant's protected health data employed reasonable security procedures;

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

f. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

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

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

i. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(3);

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

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

l. Filing to render the electronic PHI they maintained unusable, unreadable, or indecipherable to unauthorized individuals, as they had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 C.F.R. § 164.304, definition of "encryption")

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

m. Failing to put into place proper procedures, software settings, and data security software protections to adequately protect against a blunt force intrusion;

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

o. Failing to adhere to industry standards for cybersecurity; and

p. Failing to provide notice once the scope of the breach was determined.

90. As the result of computer systems needing security upgrading, inadequate procedures for handling emails containing ransomware or other malignant computer code, and inadequately trained employees who opened files containing the ransomware virus, Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information.

91. As the result of computer systems needing security upgrading, Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information.

92. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft.

A. Because of Defendant's Failure to Safeguard Private Information, Plaintiff and the Class Members Have and Will Experience Substantial Harm in the Form of Risk of Continued Identity Theft.

93. Plaintiff and members of the proposed Class have suffered injury from the misuse of their Private Information that can be directly traced to Defendant.

94. The ramifications of Defendant's failure to keep Plaintiff's and the Class's Private Information secure are severe. Identity theft occurs when someone uses another's personal information such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes. According to experts, one out of four data breach notification recipients become a victim of identity fraud.

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

95. Because of Defendant's failures to prevent—and to timely detect—the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their Private Information is used;

b. The diminution in value of their Private Information;

c. The compromise and continuing publication of their Private Information;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies; Unauthorized use of stolen Private Information; and

g. The continued risk to their Private Information, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the Private Information in its possession.

96. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.

97. The value of Plaintiff's and the proposed Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals often post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

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

98. It can take victims years to spot identity or PII theft, giving criminals plenty of time to abuse that information for money.

99. One such example of criminals using PII for profit is the development of "Fullz" packages.

100. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

101. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and other members of the proposed Class's stolen PII is being misused, and that such misuse is traceable to the Data Breach.

102. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims, and the numbers are only rising.[25]

103. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

---

[25] *See* https://www.ic3.gov/AnnualReport/Reports/2019_ic3Report.pdf (last visited June 13, 2025).

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

104. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims must spend a considerable time repairing the damage caused by the theft of their Private Information. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

105. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen Private Information. To protect himself, Plaintiff and the Class will need to remain vigilant against unauthorized data use for years or even decades to come.

106. The FTC has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."[26]

107. The FTC has also issued many guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making. According to the FTC, data security requires:

a. encrypting information stored on computer networks;

b. retaining payment card information only as long as necessary;

c. properly disposing of personal information that is no longer needed;

d. limiting administrative access to business systems;

e. using industry-tested and accepted methods for securing data;

f. monitoring activity on networks to uncover unapproved activity;

g. verifying that privacy and security features function properly;

[26] Statement of FTC Commissioner Pamela Jones Harbour-Remarks Before FTC Exploring Privacy Roundtable, (Dec. 7, 2009).(last visited June 5, 2025).

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

h. testing for common vulnerabilities; and

i. updating and patching third-party software.

108. According to the FTC, unauthorized PII disclosures ravage consumers' finances, credit history and reputation, and can take time, money and patience to resolve the fallout.[27] The FTC treats 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(a) of the FTC Act.

109. Defendant's failure to properly notify Plaintiff and Class Members of the Data Breach exacerbated Plaintiff's and Class Members' injury by depriving them of the earliest ability to take appropriate measures to protect their Private Information and take other necessary steps to mitigate the harm caused by the Data Breach.

110. Plaintiff and Class Members now face an increased risk of fraud and identity theft.

B. Data Breaches Put Consumers At an Increased Risk of Fraud and Identity Theft

111. Data Breaches such as the one experienced by Defendant's residents are especially problematic because of the disruption they cause to the daily lives of victims affected by the attack.

112. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[28]

113. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the

---

[27] *See* Taking Charge, What to Do If Your Identity is Stolen, FTC, at 3 (2012), *available at* https://www.ojp.gov/ncjrs/virtual-library/abstracts/taking-charge-what-do-if-your-identity-stolen (last visited June 5, 2025).

[28] U.S. Government Accountability Office, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), *available at* https://www.gao.gov/new.items/d07737.pdf (last visited June 5, 2025) ("GAO Report").

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

credit bureaus to place a fraud alert (possibly an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[29]

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

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

116. Theft of Private Information is gravely serious. PII/PHI is a valuable property right.[30]

117. Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

118. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII on the black market for the purpose of

---

[29] Federal Trade Commission, *What To Do Right Away* (2024), *available at* https://www.identitytheft.gov/Steps (last visited June 5, 2025).

[30] *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).

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

target marketing their products and services to the physical maladies of the data breach victims himself.

119. It must also be noted there may be a substantial time lag—measured in years—between when harm occurs versus when it is discovered, and between when Private Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which studied data breaches:

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

See GAO Report, at p. 29.

120. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for years.

121. There is a strong probability that all the stolen information has been dumped on the black market or will be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

122. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[31] PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

---

[31] Ashiq Ja, *Hackers Selling [healthcare] Data in the Black Market*, InfoSec (July 27, 2015), *available at* https://resources.infosecinstitute.com/topic/hackers-selling-[healthcare]-data-in-the-black-market/ (last visited June 5, 2025).

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

123. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for more credit lines.[32] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[33] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

124. It is also hard to change or cancel a stolen Social Security number.

125. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[34]

126. Healthcare data, as one would expect, demands a much higher price on the black market. The National Association of Healthcare Access Management reports,"[p]ersonal medical data is said to be more than ten times as valuable as credit card information."[35]

---

[32] Social Security Administration, *Identity Theft and Your Social Security Number* (2018), *available at* https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited June 5, 2025).

[33] *Id* at 4.

[34] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (February 9, 2015), *available at* http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited June 5, 2025).

[35] Laurie Zabel, *The Value of Personal Medical Information: Protecting Against Data Breaches*, NAHAM Connections, *available at* https://www.naham.org/page/ConnectionsThe-Value-of-Personal-Medical-Information (last visited June 5, 2025).

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

127. Medical information is especially valuable to identity thieves. According to account monitoring company LogDog, coveted Social Security numbers were selling on the dark web for just $1 in 2016—the same as a Facebook account. That pales in comparison with the asking price for medical data, which was selling for $300 and up.[36]

128. In recent years, the corporations that maintain medical and financial data in their network systems have experienced disproportionally higher numbers of data theft events than other industries. Defendant therefore knew or should have known this and strengthened its data systems accordingly. Defendant were put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

VI. PLAINTIFF'S EXPERIENCE

129. Plaintiff James Reese is and at all times mentioned herein was an individual citizen of Washington, residing in the city of Battle Ground.

130. Plaintiff provided Defendant with his sensitive Private Information as a condition of being a resident of Defendant.

131. Plaintiff is careful about sharing his sensitive Private Information. Plaintiff has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

132. Plaintiff stores any documents containing his sensitive Private Information in a safe and secure location or destroys the documents.

133. Moreover, Plaintiff diligently chooses unique usernames and passwords for his sensitive online accounts.

134. Had Plaintiff been aware that Defendant's computer systems were not secure, he would not have entrusted his personal data to Defendant.

---

[36] Paul Ducklin, *FBI "ransomware warning" for healthcare is a warning for everyone!*, Sophos (Oct. 29, 2020) *available at* https://news.sophos.com/en-us/2020/10/29/fbi-ransomware-warning-for-healthcare-is-a-warning-for- everyone/ (last visited June 5, 2025).

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

135. Because of the Data Breach, Defendant advised Plaintiff to take certain steps to protect his Private Information and otherwise mitigate his damages.

136. Because of the Data Breach, Plaintiff spent time dealing with the consequences of his Private Information being exfiltrated by cybercriminals, which includes time spent verifying the legitimacy of the Notice of Data Breach and self-monitoring his accounts to track any fraudulent activity that has occurred and the time it has taken or will take to rectify any fraudulent activity.

137. This time has and will be lost forever because it cannot be recaptured. This time was spent because Defendant's direct instructions by way of the Data Breach notice where Defendant recommended that Plaintiff mitigate his damages by, among other things, monitoring his accounts for fraudulent activity.

138. Even with the best response, the harm caused to Plaintiff cannot be undone.

139. Plaintiff suffered actual injury in the form of damage and diminution to the value of Plaintiff's Private Information—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and because of the Data Breach.

140. Plaintiff suffered lost time, annoyance, interference, and inconvenience because of the Data Breach and has constant anxiety and increased concerns for the loss of his privacy.

141. Plaintiff has suffered imminent and impending injury arising from the exacerbated risk of fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of criminals.

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

VII. PLAINTIFF'S AND CLASS MEMBERS' DAMAGES

143. To date, Defendant has done little to provide Plaintiff and Class Members with relief for the damages they have suffered because of the Data Breach, including, but not limited to, the costs and loss of time they incurred because of the Data Breach. Defendant has only

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

offered inadequate identity monitoring services, despite Plaintiff and Class Members being at risk of identity theft and fraud for the remainder of their lifetimes.

144. The credit monitoring offered to persons whose Private Information was compromised is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud. What's more, Defendant places the burden on Plaintiff and Class Members by requiring them to expend time signing up for that service rather than automatically enrolling all victims of this Data Breach.

145. Defendant's credit monitoring advice to Plaintiff and Class Members places the burden on Plaintiff and Class Members, rather than on Defendant, to investigate and protect himself from Defendant's tortious acts resulting in the Data Breach.

146. Plaintiff and Class Members have been damaged by the compromise and exfiltration of their Private Information in the Data Breach, and by the severe disruption to their lives as a direct and foreseeable consequence of this Data Breach.

147. Plaintiff's Private Information was compromised and exfiltrated by cyber-criminals as a direct and proximate result of the Defendant's failure to use reasonable and adequate measures in protecting the data it collected and maintained.

148. Plaintiff and Class Members were damaged in that their Private Information is now, and for the foreseeable future, in the hands of cyber criminals.

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

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

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

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

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

153. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

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

155. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

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

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Placing "freezes" and "alerts" with credit reporting agencies;

g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

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

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

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

j. Paying late fees and declined payment fees imposed because of failed automatic payments that were tied to compromised cards that had to be cancelled; and

k. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

157. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by implementing security measures and safeguards, including, but not limited to, making sure that the storage of data or documents containing personal and financial information is inaccessible online and that access to such data is password protected.

158. Further, because of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information —which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

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

VIII. CLASS REPRESENTATION ALLEGATIONS

160. Under Rule 23(B)(2), 23(B)(3), and 23(C)(4) Of the Washington Superior Court Rules of Civil Procedure, Plaintiff brings this case as a class action against Defendant on behalf of the Class preliminarily defined as follows:

All persons whose Private Information was compromised because of the October 2023, Data Breach (the "Class").

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

161. Excluded from the Class are Defendant's officers and directors, and any entity in which Defendant have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are Members of the judiciary to whom this case is assigned, their families and Members of their staff.

162. Plaintiff reserves the right to amend or modify the class definitions with greater specificity or division after having an opportunity to conduct discovery.

163. This action satisfies the numerosity, commonality, typicality, and adequacy of requirements under Rule 23(B)(2), 23(B)(3), and 23(C)(4) of the Washington Superior Court Rules of Civil Procedure.

164. Numerosity. In accordance with R. CIV. P. 23(A)(1), the Members of the Class are so numerous that joinder of all of them is impracticable. Although the precise number of individuals is currently unknown to Plaintiff and exclusively in the possession of Defendant, upon information and belief, thousands of individuals were impacted. The Class is apparently identifiable within Defendant records and Defendant has already identified these individuals (as evidenced by sending them breach notification letters).

165. Commonality. In satisfaction of R. CIV. P. 23(A)(2) and (B)(3) There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;
b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

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

d. Whether Defendant's data security systems prior to and during the Data Breach adhered to industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendant breached their duty to Class Members to safeguard their Private Information;

g. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

h. Whether Plaintiff and Class Members suffered legally cognizable damages from Defendant's misconduct;

i. Whether Defendant's conduct was negligent;

j. Whether Defendant's conduct was per se negligent;

k. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

l. Whether Defendant was unjustly enriched;

m. Whether Defendant failed to provide notice of the Data Breach promptly; and

n. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

166. Typicality. Pursuant to R. CIV. P. 23(A)(3) Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class member, was compromised in the Data Breach. Plaintiff's claims are typical of those of the other Class Members because, among other things, all Class Members were injured through the common misconduct of Defendant. Plaintiff is advancing the same claims and legal theories on behalf of himself and all other Class Members, and no defenses are unique to Plaintiff. Plaintiff's claims and those of Class Members arise from the same operative facts and are based on the same legal theories.

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

167. Adequacy. As R. CIV. P. 23(A)(4) requires Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

168. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

169. Superiority and Manageability. Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

170. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since Defendant would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff were exposed is representative of that experienced by the Class and will establish the right of each

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

Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

171. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

172. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

173. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

174. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate.

175. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such issues include, but are not limited to:

a. Whether Defendant failed to timely notify the public of the Data Breach;
b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;
c. Whether Defendant's security measures to protect their data systems were reasonable considering best practices recommended by data security experts;
d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;
e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and

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

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

176. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

IX. CAUSES OF ACTION

FIRST COUNT
NEGLIGENCE
(On Behalf of Plaintiff and All Class Members)

177. Plaintiff re-alleges and incorporates the above allegations from paragraph 1 to paragraph 176 as if fully set forth herein.

178. Defendant required Plaintiff and Class Members to submit non-public personal information to as a condition of their residency and to obtain services from Defendant.

179. By collecting and storing this data in Defendant's computer property, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and Plaintiff's and Class Members' Private Information held within it—to prevent disclosure of the private information, and to safeguard the private information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period and to give prompt notice to those affected in the case of a Data Breach.

180. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

181. Defendant's duty of care to use reasonable security measures arose because of the special relationship that existed between Defendant and its residents including Plaintiff and

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

Class Members, which is recognized by laws and regulations, including, but not limited to, HIPAA, as well as common law. Defendant could ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

182. Defendant owed these duties to Plaintiff and members of the Class because they are Members of a well-defined, foreseeable, and probable class of individuals who Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols.

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

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

185. Defendant's duty to use reasonable care in protecting confidential data arose not only because of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

186. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

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

c. Failing to periodically ensure that its email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to detect timely that Class Members' Private Information had been compromised;

f. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

g. Failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

187. It was foreseeable that Defendant's failure to use reasonable and adequate measures to protect Plaintiff and Class Members' Private Information would result in injury to Plaintiff and Class Members. Further, the Data Breach was reasonably foreseeable given the known high frequency of cyberattacks and data breaches targeting protected health information.

188. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

189. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered because of the Data Breach.

190. Defendant's negligent conduct is ongoing, in that they still hold the Private Information of Plaintiff and Class Members in an unsafe and unsecure manner.

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

SECOND COUNT
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and All Class Members)

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

192. Plaintiff re-alleges and incorporates the above allegations from paragraph 1 through 176 as if fully set forth herein.

193. When Plaintiff and Class Members provided their Private Information to Defendant as a condition of being a resident of Defendant, they entered implied contracts with Defendant under which Defendant agreed to reasonably protect such information.

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

195. In entering such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, and adhered to industry standards.

196. Plaintiff and Class Members paid money to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

197. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that they adopted reasonable data security measures. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

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

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

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

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

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

THIRD COUNT
UNJUST ENRICHMENT
(On Behalf of Plaintiff and All Class Members)

202. Plaintiff re-alleges and incorporates the above allegations from paragraph 1 through 176 as if fully set forth herein.

203. Defendant became guardians of Plaintiff's and Class Members' Private Information, creating a special relationship between Defendant and Plaintiff and Class Members.

204. As such, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff's and Class Members' Private Information; (2) to timely notify Plaintiff and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

205. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of Defendant's relationship with its residents, in particular, to keep secure their Private Information.

206. Defendant breached its fiduciary duties by, inter alia, failing to comply with the guidelines outlined under HIPAA and the FTC act for safeguarding and storing it. This failure resulted in the Data Breach that ultimately came to pass.

207. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach.

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

208. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to:

a. actual identity theft;

b. the compromise, publication, and/or theft of their Private Information;

c. out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information;

d. lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft;

e. the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession;

f. future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the rest of the lives of Plaintiff and Class Members; and

g. the diminished value of Defendant's services they received.

209. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

210. Plaintiff and the Class seek compensatory damages for breach of fiduciary duty, which entails the amount of the difference between the price they paid for defendant's services as promised and the diminished value of its services and the costs of future monitoring of their credit history for identity theft and fraud, and/or other damages, plus prejudgment interest and costs.

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

X. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Class described above seek the following relief:

a. For an Order certifying this action as a class action, defining the Class as requested herein, appointing Plaintiff and his counsel to represent the Class, and finding that Plaintiff are proper representatives of the Class requested herein;

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

c. For equitable relief compelling Defendant to use appropriate methods and policies related to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

d. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained because of Defendant's wrongful conduct;

e. Ordering Defendant to pay for not less than ten years of credit monitoring services for Plaintiff and the Class;

f. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g. For an award of punitive damages, as allowable by law;

h. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i. Pre- and post-judgment interest on any amounts awarded; and

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

j. Any other relief that this court may deem just and proper.

DATED this 13th day of June, 2025.

/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

Leigh S. Montgomery*
Texas Bar No. 24052214
lmontgomery@eksm.com
EKSM, LLP
4200 Montrose Blvd., Suite 200
Houston, Texas 77006
Phone: (888) 350-3931
Fax: (888) 276-3455
Service Only: service@eksm.com

**Pro Hac Vice* forthcoming

Attorneys for Plaintiff and Putative Class

EXHIBIT A

P.O. Box 1907
Suwanee, GA 30024

46 117586 **********AUTO**3-DIGIT 9860
James Reese
[redacted]

Enrollment Code: Y3A3P49MEJ

To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://app.idx.us/account-creation/protect

May 29, 2025

Notice of Security Incident

Dear James Reese:

Clark County, Washington, writes to inform you of an event that may impact some of your information. This notice includes an overview of the event, our response, and resources available to help you further protect your information, should you feel it necessary to do so.

What Happened?

On October 21, 2023, Clark County detected suspicious activity on our computer network and determined that some systems were encrypted by malware. Upon identifying the activity, Clark County took quick steps to bring the network offline, ensure the security of our systems, and launch an investigation into the nature and scope of the event. The investigation determined that an unknown actor gained access to Clark County systems between October 16, 2023, and October 21, 2023, and accessed and/or stole data stored on certain Clark County systems.

As part of the investigation, Clark County initiated a thorough and comprehensive review of the data that may have been accessed or stolen to determine what data is involved, to whom it relates, and contact information for those individuals. Through that review, Clark County determined that some of your information may be involved.

***What Information* Was Involved?**

Based on the review, the information related to you that may be involved in this event includes your name and: date of birth and Social Security number. Please note, there is currently no evidence of actual or attempted misuse of your information in connection with this event.

What We Are Doing.

Clark County takes this event and the security of the information in our care very seriously. Upon detecting the event, we moved quickly to respond, securely restore our systems, assess the security of our network, and investigate the event. Clark County also reported the event to law enforcement and is notifying state regulators, as required. As part of our ongoing commitment to information security, Clark County reviewed our policies, procedures, security tools, and employee training programs to reduce the risk of a similar event occurring in the future.

Clark County is also offering 12 months of complementary credit monitoring through IDX. You must enroll in these services yourself as Clark County is unable to do so on your behalf. Enrollment instructions can be found in the enclosed *Steps You Can Take to Help Protect Your Information.* The deadline to enroll is August 29, 2025.