Exhibit A

Joseph M. Lyon (SBN 351117)
THE LYON FIRM
9210 Irvine Center Drive, Suite 200
Irvine, CA 92618
Telephone: (513) 381-2333
Facsimile: (513) 766-9011
Email: jlyon@thelyonfirm.com

John J. Nelson (SBN 317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
280 S. Beverly Drive
Beverly Hills, CA 90212
Telephone: (858) 209-6941
Email: jnelson@milberg.com

Attorneys for Plaintiffs and Putative Class

UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA

IN RE: HOUSER LLP DATA BREACH LITIGATION Defendant.	Case No. 8:24-cv-00468-WLH-ADS **CONSOLIDATED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

PLAINTIFFS' CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Richard McMillen, Mark Giannelli, Joseph Kausse, Scott Miller, Jennifer Rivera, and Karie Simmons ("Plaintiffs") bring this Class Action Complaint against Houser LLP ("Houser" or "Defendant"), individually and on behalf of all

others similarly situated ("Class Members"), and allege, upon personal knowledge as to their own actions and the investigation of counsel, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Plaintiffs bring this class action against Defendant for its failure to properly secure and safeguard personally identifiable information ("PII") including, but not limited to, full names, Social Security numbers, driver's license numbers, individual tax identification numbers, and financial account information (collectively "Private Information").

2. Defendant is a law firm that serves Fortune 500 companies and businesses of all sizes with eleven offices nationwide.[1]

3. Plaintiffs are individual consumers who bring this class action against Defendant for its failure to properly secure and safeguard the Private Information.

4. Plaintiffs are largely unaware of the specific nature and manner in which their Private Information came to be in the Defendant's possession.

5. However, upon information and belief, to provide its legal services, Defendant required that its corporate and finance clients provide the Private

[1] https://houser-law.com/ (last visited Aug. 8, 2024).

Information of Plaintiffs and Class Members, which Defendant stored and utilized on its computer network.

6. By obtaining, collecting, using, and deriving a benefit from the Private Information of Plaintiffs and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. By voluntarily undertaking the collection of this sensitive Private Information, Defendant assumed a duty to use due care to protect that information.

7. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class Members and the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of the Data Breach.

8. On May 9, 2023, Defendant discovered an unauthorized party gained access to its systems between May 7 and May 9, 2023, on which the highly sensitive personal information of Plaintiffs' and Class Members' was stored unencrypted and in an internet accessible environment (the "Data Breach").[2]

[2] Data Breach Notifications, Office of the Maine Attorney General, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/d9317b04-babe-4a70-b1aa-f013f50c28f2.shtml (last visited Aug. 8, 2024).

9. During the course of the Data Breach, the unauthorized third party was able to access Defendant's network, and then access and exfiltrate Plaintiffs' and Class Members' Private Information stored on Defendant's network. This Private Information was then likely listed for sale on the dark web as that is the *modus operandi* of cybercriminals who target personal information for its value in committing fraud and identity theft.

10. Upon information and belief, Defendant committed multiple acts of negligence that were a cause of the Data Breach, including but not limited to Defendant's: (i) failure to design, implement, and maintain reasonable data security systems and safeguards; (ii) failure to exercise reasonable care in the hiring, supervision, training, and monitoring of its employees and agents and vendors; (iii) failure to comply with industry standard data security practices; (iv) failure to comply with federal and state laws and regulations that govern data security and privacy practices that are intended to protect the type of Private Information at issue in this action; and/or (v) failure to design, implement and execute reasonable data retention and destruction policies.

11. Upon information and belief, despite its role in managing so much sensitive information, Houser failed to take basic security measures such as adequately encrypting its data or following industry security standards to destroy Private Information that was no longer necessary for the intended business purpose.

12. As a result of the Data Breach, Plaintiffs and roughly 326,000 Class Members suffered concrete harms in the forms of invasion of privacy, diminution of value of their Private Information, and an increased risk of identity theft and fraud, as well as at least one separate concrete harm in the form of out-of-pocket monetary losses and expenses, and/or the value of their time reasonable incurred to remedy or mitigate the effects of the attack. Moreover, given the theft of information that is largely static—i.e., Social Security numbers—the risk of identity theft and fraud will remain constant with Plaintiffs and Class Members for the foreseeable future. Plaintiffs and Class Members now face years of increased risk of identity theft and fraud, and the need to mitigate those risks through constant surveillance and monitoring of their financial and personal records.

13. Upon information and belief, Plaintiffs' and Class Members' Private Information remains in Defendant's possession. Plaintiffs and Class Members therefore have a continuing interest in ensuring that their information is and remains safe and should be provided injunctive and other equitable relief.

14. Plaintiffs, individually and on behalf of all others similarly situated, bring claims for (i) negligence; (ii) breach of contract to which Plaintiffs and Class Members were intended third party beneficiaries; (iii) violation of the California Consumer Privacy Act ("CCPA"); (iv) breach of the Washington Consumer Protection Act; and (v) declaratory and injunctive relief.

15. Plaintiffs seek actual, compensatory, consequential, and, alternatively, nominal damages, in an amount to be proven at trial. Plaintiffs also seek future compensatory damages to provide adequate credit and identity theft monitoring. Further, Plaintiffs seek declaratory and injunctive relief related to the ongoing future risk of identity theft requiring Defendant to delete, destroy, or purge all Private Information of Plaintiffs and Class Members for which Defendant has no reasonable justification for retaining on its network in order to prevent incidents like the Data Breach from reoccurring in the future.

PARTIES

16. Plaintiff Richard McMillen is an adult individual and, at all relevant times herein, a resident and citizen of Tampa, Florida where he intends to remain.

17. Plaintiff Mark Giannelli is an adult individual and, at all relevant times herein, a resident and citizen of Sumner, Maine where he intends to remain.

18. Plaintiff Joseph Kausse is an adult individual and, at all relevant times herein, a resident and citizen of Wichita, Kansas where he intends to remain.

19. Plaintiff Scott Miller is an adult individual and, at all relevant times herein, a resident and citizen of Los Angeles, California where he intends to remain.

20. Plaintiff Jennifer Rivera is an adult individual and, at all relevant times herein, a resident and citizen of Aurora, Illinois where she intends to remain.

21. Plaintiff Karie Simmons is an adult individual and, at all relevant times herein, a resident and citizen of King County, Washington where she intends to remain.

22. Defendant Houser LLP is a California limited liability partnership with its principal place of business at 9970 Research Drive, Irvine, California 92618. Upon information and belief, Defendants provide legal services to clients nationwide.

JURISDICTION AND VENUE

23. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The number of class members exceeds 100, many of whom have different citizenship from Defendant, including several Plaintiffs. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

24. This Court has personal jurisdiction over Defendant because it operates and is headquartered in this District and conducts substantial business in this District.

25. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Moreover, Defendant is based in this District, maintains Plaintiffs' and Class Members' Private Information in this District, and has caused harm to Plaintiffs and Class Members in this District.

FACTUAL ALLEGATIONS

Background

26. Houser LLP is a law firm serving Fortune 500 companies and businesses of sizes nationwide.

27. Houser provides legal services to commercial businesses and financial institutions.

28. Plaintiffs and Class Members are customers of Defendant's clients.

29. Plaintiffs and Class Members provided certain Private Information to clients of Defendant's, who in turn provided the information to Defendant.

30. In the ordinary course of its business practices, Defendant collects, stores, maintains, and uses Plaintiffs' and Class Members' Private Information.

31. As a sophisticated legal services provider with a heightened interest in maintaining the confidentiality of the Private Information entrusted to it, Defendant was or should have been aware of the numerous data breaches that have occurred throughout the United States and its responsibility to safeguard the Private Information in its possession. Indeed, Defendant represented to victims of the Data Breach that it "it takes the confidentiality, privacy, and security of information in

[its] care seriously."[3]

32. Plaintiffs and Class Members indirectly entrusted Defendant with sensitive and confidential information, including their Private Information which includes information that is static, meaning it does not change, and can be used to commit myriad financial crimes for the remainder of Plaintiffs' and Class Members' lives.

The Data Breach

33. On May 9, 2023, Defendant discovered that an unauthorized party gained access to Defendant's systems between May 7, 2023, and May 9, 2023.[4]

34. On or around February 28, 2024, Defendant notified Plaintiffs and Class Members of the Data Breach (the "Notice of Data Breach), stating:

> **What Happened?** On May 9, 2023, Houser discovered that certain files on their computer systems had been encrypted. We immediately launched an investigation, with the assistance of third-party forensic specialists, to determine the nature and scope of the activity. Our investigation determined that there was unauthorized access to our network between May 7, 2023, and May 9, 2023, during which time certain files were copied and taken from our network. However, in June 2023, the

[3] *See 2024-04-12 Houser Data Breach Notice to Consumers*, Office of the Vermont Atty. Gen., available at https://ago.vermont.gov/document/2024-04-12-houser-data-breach-notice-consumers.

[4] *Id.*

> unauthorized actor informed us that they deleted copies of any stolen data and would not distribute any stolen files.

35. Defendant's Notice of Data Breach admits that Plaintiffs and Class Members' Private Information was accessed, copied, and taken in the Data Breach without authorization. In other words, the data was exfiltrated and stolen by the cybercriminals.

36. Ransomware attacks, like that experienced by Defendant, are frequently leveraged by cybercriminals to extort a ransom from the entities from which they steal consumer data in exchange for a promise to delete that data. However, often times criminals will accept a ransom payment, falsify evidence of deletion, and then sell personal data on the dark web. For example, recently United Healthcare paid a $22 million dollar ransom in exchange for proof of deletion only to find that the patient data exfiltrated in the cyberattack was subsequently being sold on the dark web.[5]

37. According to an FBI publication, "[r]ansomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return. Ransomware

[5] *After paying a $22M ransom to delete it, data stolen in Change HealthCare breach resurfaces*, accessible at, https://www.comparitech.com/news/after-paying-a-22m-ransom-to-delete-it-data-stolen-in-change-healthcare-breach-resurfaces/ (last visited Aug. 7, 2024).

attacks can cause costly disruptions to operations and the loss of critical information and data."[6] This publication also explains that "[t]he FBI does not support paying a ransom in response to a ransomware attack. Paying a ransom doesn't guarantee you or your organization will get any data back. It also encourages perpetrators to target more victims and offers an incentive for others to get involved in this type of illegal activity."[7]

38. Companies should treat ransomware attacks as any other data breach incident because ransomware attacks don't just hold networks hostage, "ransomware groups sell stolen data in cybercriminal forums and dark web marketplaces for additional revenue."[8] As cybersecurity expert Emisoft warns, "[a]n absence of evidence of exfiltration should not be construed to be evidence of its absence […] the initial assumption should be that data may have been exfiltrated."

39. An increasingly prevalent form of ransomware attack is the "encryption+exfiltration" attack in which the attacker encrypts a network and

---

[6] https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware (last visited Aug. 7, 2024).

[7] *Id.*

[8] *Ransomware: The Data Exfiltration and Double Extortion Trends*, available at https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends (last visited Aug. 7, 2024).

exfiltrates the data contained within.[9] In 2020, over 50% of ransomware attackers exfiltrated data from a network before encrypting it.[10] Once the data is exfiltrated from a network, its confidential nature is destroyed and it should be "assume[d] it will be traded to other threat actors, sold, or held for a second/future extortion attempt."[11] And even where companies pay for the return of data attackers often leak or sell the data regardless because there is no way to verify copies of the data are destroyed.[12]

40. Despite learning of the Data Breach on May 9, 2023, Defendant waited until February 28, 2024, before informing Plaintiffs and Class Members that their Private Information was exfiltrated in the Data Breach, a delay of almost ten months.

41. Furthermore, Defendant's Notice of Data Breach directed Plaintiffs to be vigilant and to take certain steps to protect their Private Information and otherwise mitigate their damages.

---

[9] *The chance of data being stolen in a ransomware attack is greater than one in ten*, available at https://blog.emsisoft.com/en/36569/the-chance-of-data-being-stolen-in-a-ransomware-attack-is-greater-than-one-in-ten/ (last visited Aug. 7, 2024).

[10] 2020 Ransomware Marketplace Report, available at https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report (last visited Aug. 7, 2024).

[11] *Id.*

[12] *Id.*

42. Following this Notice of Data Breach, Plaintiffs heeded Defendant's warnings and spent time dealing with the consequences of the Data Breach, which included time spent verifying the legitimacy of the Notice, and self-monitoring their accounts and credit reports to ensure no fraudulent activity had occurred. This time has been lost forever and cannot be recaptured. Moreover, this time was spent at Defendant's direction by way of the Notice of Data Breach wherein Defendant advised Plaintiffs to mitigate their damages by, among other things, monitoring their accounts for fraudulent activity.

The Data Breach was Foreseeable

43. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class Members and the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

44. 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]

[13] *See* 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 Aug. 7, 2024).

45. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the legal industry preceding the date of the breach.

46. According to the 2017 ABA Legal Technology Survey, 22% of responding law firms were hacked or experienced data breaches in 2017,[14] and, according to the 2020 ABA Legal Technology Survey, 29% of responding law firms reported experiencing security breaches[15] affecting more than 46,000 Americans.[16] Indeed, since 2020, "more than 750,000 Americans had personal information comprised in law firm hacks."[17]

47. In light of the ever-increasing trend of cybersecurity incidents affecting law firms, Defendant knew or should have known that its electronic records would

---

[14] David G. Ries, *2017 Security*, ABA TECHREPORT 2017 (Dec. 1, 2017), https://www.americanbar.org/groups/law_practice/publications/techreport/2017/security/.

[15] John G. Loughnane, *2020 Cybersecurity*, ABA TECHREPORT (Oct. 19, 2020), https://www.americanbar.org/groups/law_practice/publications/techreport/2020/cybersecurity/.

[16] Dan Roe, *Cyberattacks 'Inevitable' for Law Firms*, Highlighting Need for Comprehensive Incident Response Plans, LAW.COM (Jan. 10, 2023), https://www.law.com/americanlawyer/2023/01/10/cyberattacks-inevitable-for-law-firms-highlighting-need-for-comprehensive-incident-response-plans/?slreturn=20230313110804.

[17] *Id.*

be targeted by cybercriminals.

48. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

Value of Private Information

49. The Private Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[18] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[19] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[20]

50. Based on the foregoing, the information compromised in the Data

---

[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 visited Aug 7, 2024).

[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 visited Aug 7, 2024).

[20] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Aug 7, 2024).

Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts.

51. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information…[is] worth more than 10x on the black market."[21]

Defendant Failed to Properly Protect Plaintiffs' and Class Members' Private Information.

52. Defendant could have prevented this Data Breach by properly securing and encrypting the systems containing the Private Information of Plaintiffs and Class Members. Alternatively, Defendant could have destroyed the data, especially for individuals with whom it had not had a relationship for a period of time, or a legitimate business purpose for retaining.

53. Defendant's negligence in safeguarding the Private Information of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts

[21] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Aug 7, 2024).

directed to companies like Defendant to protect and secure sensitive data they possess.

54. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiffs and Class Members from being compromised.

55. To prevent and detect unauthorized cyber-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.
- 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.
- 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.[22]

56. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, 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
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

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

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

Apply principle of least-privilege

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

57. Given that Defendant was storing the Private Information of Plaintiffs and Class Members, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks. Instead, upon information and belief, Defendant failed to implement at least one of the above-mentioned basic security measures, like password protection, encryption, or multifactor authentication.

Defendant Failed to Comply with FTC Guidelines

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

59. 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 patient information that they keep; properly dispose of personal information that is no longer

needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[23]

60. The FTC further recommends that companies not maintain Private Information 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.[24]

61. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions clarify the measures businesses take to meet their data security obligations.[25]

---

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

[24] *Id.*

[25] *Privacy and Security Enforcement*, Fed. Trade Comm'n, https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement (last visited Aug. 5, 2024).

62. Upon information and belief, among others, Defendant failed to properly implement basic data security practices, e.g., failing to properly dispose of data that Defendant no longer had a legitimate business purpose for retaining, or encrypting such information.

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

Defendant failed to Comply with Industry Standards

64. According to the FTC, unauthorized Private Information disclosures are extremely damaging to consumers' finances, credit history and reputation, and can take time, money and patience to resolve the fallout.[26] 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.

65. Several best practices have been identified that at a minimum should be implemented by service providers like Defendant, including but not limited to:

[26] *See* Taking Charge, What to Do If Your Identity is Stolen, FTC, at 3 (2012), https://www.ojp.gov/ncjrs/virtual-library/abstracts/taking-charge-what-do-if-your-identity-stolen (last visited Aug. 6, 2024).

educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and antimalware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

66. Upon information and belief, Defendant failed to meet the minimum standards of one or more 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.

67. The foregoing frameworks are existing and applicable industry standards in the legal industry, and upon information and belief Defendant failed to comply with one or more of these accepted standards, thereby opening the door to and causing the Data Breach.

68. Upon information and belief, Defendant failed to comply with one or more of the foregoing industry standards.

COMMON INJURIES IN FACT AND DAMAGES

69. The ramifications of Defendant's failure to keep Plaintiffs' and the

Class's Private Information secure are severe. As a result of the Data Breach, Plaintiffs and Class Members suffered the concrete injury of invasion of privacy and general damages the moment the information was disclosed and placed in the hands of the criminal actors. Moreover, Plaintiffs and Class Members' data was diminished in value.

70. Due to the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to Plaintiffs and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) loss of time incurred due to actual identity theft; (e) loss of time due to increased spam and targeted marketing emails; (f) diminution of value of their Private Information; and (g) the continued risk to their Private Information, which remains in Defendant's possession, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

The Risk of Identity Theft to Plaintiff and Class Members is Present and Ongoing

71. Plaintiffs also now face the imminent and substantial risk of identity

theft and fraud. According to experts, one out of four data breach notification recipients become a victim of identity fraud.[27]

72. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

73. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity – or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

74. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone

[27] *See* Serge Malenkovich, *One in Four That Receive Data Breach Letters Affected by Identity Theft*, Kaspersky.com (Mar. 1, 2013), https://usa.kaspersky.com/blog/data-breach-letters-affected-by-identity-theft/1262/.

calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on the victims.

75. The dark web is an unindexed layer of the internet that requires special software or authentication to access.[28] Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or 'surface' web, dark web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[29] This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

76. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs, and frequently, personal information like the PII at issue here.[30] The digital character of PII stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the internet

---

[28] Louis DeNicola, *What Is the Dark Web?*, Experian (May 12, 2021), https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.

[29] *Id.*

[30] *What is the Dark Web?*, Microsoft 365 (July 15, 2022), https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.

and the buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social Security numbers, dates of birth, and medical information.[31] As Microsoft warns "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others."[32]

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

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

[31] *Id.*; Louis DeNicola, *What Is the Dark Web?*, Experian (May 12, 2021), https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.

[32] *What is the Dark Web?*, Microsoft 365 (July 15, 2022), https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.

> Social Security number and assuming your identity can cause a lot of problems.[33]
>
> What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

78. Even then, 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."

79. 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

[33] Social Security Administration, *Identity Theft and Your Social Security Number*, available at https://www.ssa.gov/pubs/EN-05-10064.pdf.

being issued in the victim's name. And the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.

80. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC further 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."[34]

81. Examples of identity theft and fraud that Plaintiffs and Class Members face includes, but is not limited to, fraudulent loans opened in their names, medical services billed in their names, fraudulent tax returns, utility bills opened in their names, credit card fraud, and similar forms of identity theft.

82. Due to the risk of one's Social Security number being exposed, state legislatures have passed laws in recognition of the risk: "[t]he social security number

[34] *See generally Fighting Identity Theft With the Red Flags Rule: A How-To Guide for Business*, FED. TRADE. COMM., https://www.ftc.gov/business-guidance/resources/fighting-identity-theft-red-flags-rule-how-guide-business (last visited Aug. 5, 2024).

can be used as a tool to perpetuate fraud against a person and to acquire sensitive personal, financial, medical, and familial information, the release of which could cause great financial or personal harm to an individual. While the social security number was intended to be used solely for the administration of the federal Social Security System, over time this unique numeric identifier has been used extensively for identity verification purposes[.]"[35]

83. Moreover, "SSNs have been central to the American identity infrastructure for years, being used as a key identifier[.] . . . U.S. banking processes have also had SSNs baked into their identification process for years. In fact, SSNs have been the gold standard for identifying and verifying the credit history of prospective customers."[36]

84. "Despite the risk of fraud associated with the theft of Social Security numbers, just five of the nation's largest 25 banks have stopped using the numbers to verify a customer's identity after the initial account setup[.]"[37] Accordingly, since Social Security numbers are frequently used to verify an individual's identity after logging onto an account or attempting a transaction, "[h]aving access to your Social

---

[35] *See* N.C. Gen. Stat. § 132-1.10(1).

[36] *See* https://www.americanbanker.com/opinion/banks-need-to-stop-relying-on-social-security-numbers (last visited Aug. 7, 2024).

[37] *See* https://archive.nytimes.com/bucks.blogs.nytimes.com/2013/03/20/just-5-banks-prohibit-use-of-social-security-numbers/ (last visited Aug. 7, 2024).

Security number may be enough to help a thief steal money from your bank account"[38]

85. Another such example of criminals using Private Information for profit, to the detriment of Plaintiffs and the Class Members, is the development of "Fullz" packages.[39]

86. Cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete

[38] *See* https://www.credit.com/blog/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/ (last visited Aug. 7, 2024).

[39] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-forsale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-undergroundstolen-from-texas-life-insurance-finn/ (last visited Aug. 7, 2024).

dossiers on individuals. These dossiers are known as "Fullz" packages.

87. The development of "Fullz" packages means that stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' 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 Private Information 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 Plaintiffs and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs' and other members of the proposed Class's stolen Private Information is being misused, and that such misuse is fairly traceable to the Data Breach.

88. 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.[40]

89. Defendant's failure to properly notify Plaintiffs and Class Members of

[40] *See 2019 Internet Crime Report*, FBI (Feb. 11, 2020), https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120.

the Data Breach exacerbated Plaintiffs' and Class Members' injuries 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.

Loss of Time to Mitigate the Risk of Identity Theft and Fraud

90. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

91. Thus, due to the actual and imminent risk of identity theft, Plaintiffs and Class Members must, as Defendant's Notice instructs them, "remain vigilant against identity theft and fraud" and "review [their] account statements, and [] monitor [their] credit reports for suspicious activity."

92. 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.[41]

93. In order to mitigate the risk of identity theft and fraud, Plaintiffs and Class Members heeded Defendants advice and took a variety of steps that incurred costs in the form of time and/or money, including: (i) Placing "freezes" and "alerts" with reporting agencies; (ii) Closely reviewing and monitoring Social Security numbers, accounts, and credit reports for unauthorized activity for years to come; and (iii) credit monitoring fees, credit report fees, and/or credit freeze fees.

94. A number of Plaintiffs have each also suffered misuse of the stolen data in the form of an increase in spam or phishing calls and emails following the Data Breach. Spam calls, texts, and emails are often used to garner additional information from a victim of a data breach or to initiate phishing attacks to gain access to a broader swath pf the victim's data.

95. Plaintiffs' mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breach ("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."[42]

---

[41] *See 2019 Internet Crime Report*, FBI (Feb. 11, 2020), https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120.

[42] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting

Future Cost of Credit and Identity Monitoring is Reasonable and Necessary

96. To date, Defendant has done little to provide Plaintiffs and Class Members with relief for the damages they have suffered as a result of the Data Breach, including, but not limited to, the costs and loss of time they incurred because of the Data Breach. To be sure, Defendant has only offered 12 months of inadequate identity monitoring services to some, but not all Class Members, despite Plaintiffs and Class Members being at an imminent and substantial risk of identity theft and fraud for the remainder of their lifetimes.

97. Plaintiffs' mitigation efforts are also consistent with the steps that the FTC recommends that data breach victims to take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their reports.[43]

98. Given the type of targeted attack in this case and sophisticated criminal

---

Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf.

[43] *See* Federal Trade Commission, Identity Theft.gov, https://www.identitytheft.gov/Steps (last visited July 7, 2022).

activity, the type of Private Information, and the *modus operandi* of cybercriminals, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes – e.g., opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

99. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen Private Information. 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.[44]

[44] *Report to Congressional Requesters*, GAO, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf (last visited Aug. 7, 2024).

Diminution of Value of the Private Information

100. Private Information is a valuable property right.[45] 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.

101. Sensitive PII can sell for as much as $363 per record according to the Infosec Institute.[46]

102. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[47]

103. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn

---

[45] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf ("GAO Report").

[46] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("Private Information") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("Private Information, 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).

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

aggregates the information and provides it to marketers or app developers.[48,49]

104. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[50]

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

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

[48] https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited Aug. 7, 2024).
[49] https://datacoup.com/ (last visited Aug. 7, 2024).
[50] https://digi.me/what-is-digime/ (last visited Aug. 7, 2024).

PLAINTIFF SPECIFIC EXPERIENCES AND ALLEGATIONS

Plaintiff Richard McMillans Experience

107. At the time of the Data Breach, Defendant retained Plaintiff McMillan's Private Information in its system.

108. Plaintiff McMillan was sent a Notice Letter dated February 28, 2024, informing him that Defendant had experienced a Data Breach and that Plaintiff McMillan's Private Information, including his full name, and Social Security number were compromised in the Data Breach.

109. As a result of the Data Breach, Plaintiff McMillan spent time dealing with the consequences of the Data Breach, including verifying the legitimacy of the Notice of Data Breach and self-monitoring his financial accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured. Moreover, this time was spent at Defendant's direction by way of the Notice Letter where Defendant advised Plaintiff McMillan to remain vigilant for incidents of identity theft, and to mitigate his damages by, among other things, placing fraud alerts on his credit accounts and monitoring his accounts for fraudulent activity.

110. Plaintiff McMillan regularly takes steps to safeguard his own Private Information in his own control.

111. Plaintiff McMillan is a cautious person and is therefore very careful

about sharing his sensitive Private Information. As a result, he has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff McMillan stores any documents containing his Private Information in a safe and secure location or destroys the documents. Moreover, Plaintiff McMillan diligently chooses unique usernames and passwords for his various online accounts, changing and refreshing them as needed to ensure his information is as protected as it can be.

112. In the instant that his Private Information was accessed and obtained by a third party without his consent or authorization, Plaintiff McMillan suffered injury from a loss of privacy.

113. Plaintiff McMillan has also experienced an increase in the number of spam calls and emails since the Data Breach.

114. The Data Breach has caused Plaintiff McMillan to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of criminals and potentially sold on the Dark Web.

115. In fact, as a result of the Data Breach, Plaintiff McMillan has already suffered the misuse of his Private Information when he was informed that unauthorized individuals attempted to make two fraudulent transactions from his Wells Fargo account.

116. Since learning of those attempts, Plaintiff McMillan has received several alerts from Wells Fargo that a threat actor has repeeatedly attempted to access his account and Plaintiff McMillan has been forced to spend time monitoring this account and changing his passwords to prevent unauthorized access.

117. The loss of privacy and substantial present risk of additional imminent harm have caused Plaintiff McMillan to suffer stress, fear, and anxiety as Plaintiff McMillan is very concerned that his sensitive Private Information is now in the hands of data thieves and shall remain that way for the remainder of his lifetime and there is nothing Plaintiff McMillan can do to retrieve his stolen Private Information from the cyber-criminals.

118. Given the time Plaintiff McMillan has lost investigating this data breach, taking steps to understand its full scope, determining the appropriate remedial steps, contacting counsel, etc., coupled with Plaintiff McMillan's resultant and naturally foreseeable fears/concerns for the use of Plaintiff McMillan's valuable Private Information, the damages articulated more specifically above are far from the full extent of the harm thereto.

Plaintiff Mark Giannelli's Experience

119. At the time of the Data Breach, Defendant retained Plaintiff Giannelli's Private Information in its system.

120. Plaintiff is unaware of the basis or means of which Defendant came to

possess his Private Information and is unaware of any legitimate business reason for which Defendant continues to retain his Private Information.

121. Plaintiff Giannelli was sent a Notice Letter dated February 28, 2024, informing him that Houser had experienced a Data Breach and that Plaintiff's Private Information, including his full name and Social Security number were compromised in the Data Breach.

122. As a result of the Data Breach, Plaintiff Giannelli spent five hours dealing with the consequences of the Data Breach, including verifying the legitimacy of the Notice of Data Breach and self-monitoring his accounts and/or credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured. Moreover, this time was spent at Defendant's direction by way of the Notice Letter where Defendant advised Plaintiff Ginnelli to remain vigilant for incidents of identity theft, and to mitigate his damages by, among other things, placing fraud alerts on his credit accounts and monitoring his accounts for fraudulent activity.

123. Plaintiff Giannelli regularly takes steps to safeguard his own Private Information in his own control.

124. Plaintiff Giannelli is a cautious person and is therefore very careful about sharing his sensitive Private Information. As a result, he has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other

unsecured source. Plaintiff Giannelli stores any documents containing his Private Information in a safe and secure location or destroys the documents. Moreover, Plaintiff Giannelli diligently chooses unique usernames and passwords for his various online accounts, changing and refreshing them as needed to ensure his information is as protected as it can be.

125. In the instant that his Private Information was accessed and obtained by a third party without his consent or authorization, Plaintiff Giannelli suffered injury from a loss of privacy.

126. Plaintiff Giannelli has also experienced an increase in the number of spam calls and emails since the Data Breach.

127. The Data Breach has caused Plaintiff Giannelli to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of criminals and potentially sold on the Dark Web.

128. The loss of privacy and substantial present risk of additional imminent harm have caused Plaintiff Giannelli to suffer stress, fear, and anxiety as Plaintiff Giannelli is very concerned that his sensitive Private Information is now in the hands of data thieves and shall remain that way for the remainder of his lifetime and there is nothing Plaintiff Giannelli can do to retrieve his stolen Private Information from the cyber-criminals.

129. Given the time Plaintiff Giannelli has lost investigating this data breach, taking steps to understand its full scope, determining the appropriate remedial steps, contacting counsel, etc., coupled with Plaintiff Giannelli's resultant and naturally foreseeable fears/concerns for the use of Plaintiff Giannelli's valuable Private Information, the damages articulated more specifically above are far from the full extent of the harm thereto.

130. Plaintiff has also suffered injury in the form of damages to and diminution in the value of his Private Information.

131. Defendant acknowledges the risk posed to Plaintiff and his Private Information. Indeed, Defendant has offered a 12-month credit monitoring service to Plaintiff and Class Members.

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

Plaintiff Kausse's Experience

133. At the time of the Data Breach, Defendant retained Plaintiff Kausse's Private Information in its system.

134. Plaintiff Kausse was sent a Notice Letter dated February 28, 2024, informing him that Defendant had experienced a Data Breach and that Plaintiff's Private Information, including his full name, and Social Security number were

compromised in the Data Breach.

135. As a result of the Data Breach, Plaintiff Kausse spent time dealing with the consequences of the Data Breach, including verifying the legitimacy of the Notice of Data Breach and self-monitoring his accounts and/or credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured. Moreover, this time was spent at Defendant's direction by way of the Notice Letter where Defendant advised Plaintiff Kausse to remain vigilant for incidents of identity theft, and to mitigate his damages by, among other things, placing fraud alerts on his credit accounts and monitoring his accounts for fraudulent activity.

136. Plaintiff Kausse regularly takes steps to safeguard his own Private Information in his own control.

137. Plaintiff Kausse is a cautious person and is therefore very careful about sharing his sensitive Private Information. As a result, he has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Kausse stores any documents containing her Private Information in a safe and secure location or destroys the documents. Moreover, Plaintiff Kausse diligently chooses unique usernames and passwords for his various online accounts, changing and refreshing them as needed to ensure his information is as protected as it can be.

138. In the instant that his Private Information was accessed and obtained by a third party without his consent or authorization, Plaintiff Kausse suffered injury from a loss of privacy.

139. Plaintiff Kausse has also experienced an increase in the number of spam calls and emails since the Data Breach.

140. The Data Breach has caused Plaintiff Kausse to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of criminals and potentially sold on the Dark Web.

141. In fact, Plaintiff Kausse has already suffered fraud and identity theft in the form of subprime loan activity using his name. In addition, Plaintiff Kausse has suffered an increase in spam and phishing attempts via phone call, text message, and email.

142. The loss of privacy and substantial present risk of additional imminent harm have caused Plaintiff Kausse to suffer stress, fear, and anxiety as Plaintiff Kausse is very concerned that his sensitive Private Information is now in the hands of data thieves and shall remain that way for the remainder of his lifetime and there is nothing Plaintiff Kausse can do to retrieve his stolen Private Information from the cyber-criminals.

143. Given the time Plaintiff Kausse has lost investigating this data breach,

taking steps to understand its full scope, determining the appropriate remedial steps, contacting counsel, etc., coupled with Plaintiff Kausse's resultant and naturally foreseeable fears/concerns for the use of Plaintiff Kausse's valuable Private Information, the damages articulated more specifically above are far from the full extent of the harm thereto.

Plaintiff Miller's Experience

144. At the time of the Data Breach, Defendant retained Plaintiff Miller's Private Information in its system.

145. Plaintiff Miller was sent a Notice Letter dated February 28, 2024, informing him that Defendant had experienced a Data Breach and that Plaintiff's Private Information, including his full name, Social Security number, driver's license number, and financial account number were compromised in the Data Breach.

146. As a result of the Data Breach, Plaintiff Miller spent more than eight hours dealing with the consequences of the Data Breach, including verifying the legitimacy of the Notice of Data Breach and self-monitoring his accounts and/or credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured. Moreover, this time was spent at Defendant's direction by way of the Notice Letter where Defendant advised Plaintiff Miller to remain vigilant for incidents of identity theft, and to mitigate his damages by, among

other things, placing fraud alerts on his credit accounts and monitoring his accounts for fraudulent activity.

147. Plaintiff Miller regularly takes steps to safeguard his own Private Information in his own control.

148. Plaintiff Miller is a cautious person and is therefore very careful about sharing his sensitive Private Information. As a result, he has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Miller stores any documents containing his Private Information in a safe and secure location or destroys the documents. Moreover, Plaintiff Miller diligently chooses unique usernames and passwords for his various online accounts, changing and refreshing them as needed to ensure his information is as protected as it can be.

149. In the instant that his Private Information was accessed and obtained by a third party without his consent or authorization, Plaintiff Miller suffered injury from a loss of privacy.

150. Plaintiff Miller has also experienced an increase in the number of spam calls and emails since the Data Breach.

151. The Data Breach has caused Plaintiff Miller to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his Private Information being placed

in the hands of criminals and potentially sold on the Dark Web.

152. The loss of privacy and substantial present risk of additional imminent harm have caused Plaintiff Miller to suffer stress, fear, and anxiety as Plaintiff Miller is very concerned that his sensitive Private Information is now in the hands of data thieves and shall remain that way for the remainder of his lifetime and there is nothing Plaintiff Miller can do to retrieve his stolen Private Information from the cyber-criminals.

153. As a result of the Data Breach, Plaintiff Miller will continue to incur out-of-pocket expenses in the form of credit monitoring.

154. Given the time Plaintiff Miller has lost investigating this Data Breach, taking steps to understand its full scope, determining the appropriate remedial steps, contacting counsel, etc., coupled with Plaintiff Miller's resultant and naturally foreseeable fears/concerns for the use of Plaintiff Miller's valuable Private Information, the damages articulated more specifically above are far from the full extent of the harm thereto.

Plaintiff Rivera's Experience

155. At the time of the Data Breach, Defendant retained Plaintiff Rivera's Private Information in its system.

156. Plaintiff Rivera was sent a Notice Letter[51] dated February 28, 2024, informing her that Defendant had experienced a Data Breach and that Plaintiff Rivera's Private Information, including her full name, date of birth, and Social Security number were compromised in the Data Breach.

157. As a result of the Data Breach, Plaintiff Rivera has spent approximately 15 hours dealing with the consequences of the Data Breach, including verifying the legitimacy of the Notice Letter, contacting her bank, reviewing her credit monitoring notifications, and self-monitoring her accounts and/or credit reports to ensure no fraudulent activity has occurred. Plaintiff Rivera was forced to spend an hour of her time contacting her bank and to report a fraudulent transaction on her debit card. Additionally, Plaintiff Rivera spends approximately 10 minutes each day monitoring her financial accounts and reviewing the notifications she receives from her credit monitoring company. This time has been lost forever and cannot be recaptured. Moreover, this time was spent at Defendant's direction by way of the Notice Letter where Defendant advised Plaintiff Rivera to remain vigilant for incidents of identity theft, and to mitigate her damages by, among other things, placing fraud alerts on her credit accounts and monitoring her accounts for fraudulent activity.

158. Plaintiff Rivera regularly takes steps to safeguard her own Private

[51] The Notice Letter was addressed to the Plaintiff's maiden name, Jennifer C. Cooper.

Information in her own control.

159. Plaintiff Rivera is a cautious person and is therefore very careful about sharing her sensitive Private Information. As a result, she has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Rivera stores any documents containing her Private Information in a safe and secure location or destroys the documents. Moreover, Plaintiff Rivera diligently chooses unique usernames and passwords for her various online accounts, changing and refreshing them as needed to ensure her information is as protected as it can be.

160. In the instant that her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff Rivera suffered injury from a loss of privacy.

161. Plaintiff Rivera has also experienced an increase in the number of spam calls, emails, and text messages since the Data Breach.

162. The Data Breach has caused Plaintiff Rivera to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of criminals and potentially sold on the Dark Web.

163. In fact, Plaintiff Rivera was informed by her credit monitoring services that her Private Information was located on the Dark Web.

164. Plaintiff Rivera has already suffered fraud and identity theft in the form of an unauthorized transaction on her debit card.

165. In addition, Plaintiff Rivera has suffered an increase in spam and phishing attempts via phone calls, text messages, and emails. Plaintiff Rivera was forced to close her personal digital calendar due to the increase in unauthorized scheduled appointments.

166. The loss of privacy and substantial present risk of additional imminent harm have caused Plaintiff Rivera to suffer stress, fear, and anxiety as Plaintiff Rivera is very concerned that her sensitive Private Information is now in the hands of data thieves and shall remain that way for the remainder of her lifetime and there is nothing Plaintiff Rivera can do to retrieve her stolen Private Information from the cyber-criminals.

167. Given the time Plaintiff Rivera has lost investigating this data breach, taking steps to understand its full scope, determining the appropriate remedial steps, contacting counsel, etc., coupled with Plaintiff Rivera's resultant and naturally foreseeable fears/concerns for the use of Plaintiff Rivera's valuable Private Information, the damages articulated more specifically above are far from the full extent of the harm thereto.

Plaintiff Simmons' Experience

168. At the time of the Data Breach, Defendant retained Plaintiff Simmons'

Private Information in its system.

169. Plaintiff Simmons was sent a Notice Letter dated February 28, 2024, informing her that Defendant had experienced a Data Breach and that Plaintiff's Private Information, including her full name, and Social Security number were compromised in the Data Breach.

170. As a result of the Data Breach, Plaintiff Simmons spent time dealing with the consequences of the Data Breach, including verifying the legitimacy of the Notice of Data Breach and self-monitoring her accounts and/or credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured. Moreover, this time was spent at Defendant's direction by way of the Notice Letter where Defendant advised Plaintiff Simmons to remain vigilant for incidents of identity theft, and to mitigate her damages by, among other things, placing fraud alerts on her credit accounts and monitoring her accounts for fraudulent activity.

171. Plaintiff Simmons regularly takes steps to safeguard her own Private Information in her own control.

172. Plaintiff Simmons is a cautious person and is therefore very careful about sharing her sensitive Private Information. As a result, she has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Simmons stores any documents containing her Private

Information in a safe and secure location or destroys the documents. Moreover, Plaintiff Simmons diligently chooses unique usernames and passwords for her various online accounts, changing and refreshing them as needed to ensure her information is as protected as it can be.

173. In the instant that her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff Simmons suffered injury from a loss of privacy.

174. Plaintiff Simmons has also experienced an increase in the number of spam calls and emails since the Data Breach.

175. The Data Breach has caused Plaintiff Simmons to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of criminals and potentially sold on the Dark Web.

176. The loss of privacy and substantial present risk of additional imminent harm have caused Plaintiff Simmons to suffer stress, fear, and anxiety as Plaintiff Simmons is very concerned that her sensitive Private Information is now in the hands of data thieves and shall remain that way for the remainder of her lifetime and there is nothing Plaintiff Simmons can do to retrieve her stolen Private Information from the cyber-criminals.

177. Given the time Plaintiff Simmons has lost investigating this data

breach, taking steps to understand its full scope, determining the appropriate remedial steps, contacting counsel, etc., coupled with Plaintiff Simmons' resultant and naturally foreseeable fears/concerns for the use of Plaintiff Simmons' valuable Private Information, the damages articulated more specifically above are far from the full extent of the harm thereto.

CLASS ALLEGATIONS

178. Plaintiffs bring this nationwide class action individually and on behalf of others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

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

> All persons whose Private Information was actually or potentially accessed or acquired during the Data Breach event that is the subject of the Notice of Data Breach that Defendant published to Plaintiffs and other Class Members on or around February 28, 2024 (the "Class").

180. Plaintiffs seek certification of a California Subclass, defined as follows:

> All California residents whose Private Information was actually or potentially accessed or acquired during the Data Breach event that is the subject of the Notice of Data Breach that Defendant published to Plaintiffs and other Class Members on or around February 28, 2024 (the "California Subclass").

181. Additionally, Plaintiffs seek certification of a Washington State Subclass, defined as follows:

> All Washington State residents whose Private Information was actually or potentially accessed or acquired during the Data Breach event that is the subject of the Notice of Data Breach that Defendant published to Plaintiffs and other Class Members on or around February 28, 2024 (the "Washington Subclass").

182. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

183. Plaintiffs reserve the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

184. Numerosity, Fed R. Civ. P. 23(a)(1): Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are certainly tens of thousands, and possibly in excess of 369,000 individuals whose Private Information was improperly accessed in the Data Breach, and each Class is apparently identifiable within Defendant's records.

185. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only

individual Class Members. These include:

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

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

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

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

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

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

g. Whether Defendant violated the law by failing to remove, delete, or destroy highly sensitive personal information of consumers that is no longer being used for any valid business purpose;

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

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

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

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

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

186. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of those of other Class Members because all had their Private Information compromised as a result of the Data Breach, due to Defendant's misfeasance.

187. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct

with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

188. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that Plaintiffs have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiffs have suffered are typical of other Class Members. Plaintiffs have also retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

189. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): 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.

190. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they 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 Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each 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.

191. 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 demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

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

193. Unless a Class-wide injunction is issued, Defendant may continue in

their 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.

194. 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 under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

195. Likewise, particular issues under Rule 23(c)(4) 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 particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. Whether Defendant failed to comply with applicable laws, regulations, and industry standards relating to data security;

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

e. 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;

f. Whether Defendant failed to remove, delete, or destroy highly sensitive personal information of consumers that was never or is no longer being used for any valid business purpose; and

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

CAUSES OF ACTION
COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class)

196. Plaintiffs and the Class re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

197. Defendant knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized

parties.

198. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and the Class could and would suffer if the Private Information were wrongfully disclosed.

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

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

201. By accepting, storing, and maintaining Plaintiffs' and Class Members' Private Information, Defendant also had a duty to exercise appropriate clearinghouse practices to remove Private Information they were no longer required to retain pursuant to regulations.

202. By accepting, storing, and maintaining Plaintiffs' and Class Members'

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

203. 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.

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

205. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiffs and the Class. That special relationship arose because Defendant was entrusted with their confidential Private Information, a necessary part of Defendant's clients obtaining legal services from Defendant.

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

207. Plaintiffs and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have

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

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

209. Defendant knew or should have known that Plaintiff's and Class Members' Private Information was stored on its database and was or should have been aware of the extreme risks associated with failing to properly safeguard Plaintiff's and Class Members' Private Information.

210. Despite being aware of the likelihood that Defendant's databases were vulnerable, not secure, and likely to be attacked by cybercriminals, Defendant failed to correct, update, or upgrade its security protections, thus causing the Data Breach.

211. Plaintiffs and the Class had no ability to protect their Private Information that was in, and possibly remains in, Defendant's possession.

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

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

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

215. Defendant has admitted that the Private Information of Plaintiffs and Class Members was improperly accessed, exfiltrated, and encrypted by unauthorized third persons as a result of the Data Breach.

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

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

Defendant's possession or control.

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

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

220. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove Private Information which they were no longer required to retain pursuant to regulations.

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

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

223. Said differently, if Defendant had properly prevented a "technical security configuration," then the Data Breach would not have occurred, and Plaintiff's and Class Members' Private Information would have been appropriately safeguarded.

224. Plaintiffs and Class Members suffered an injury when their Private Information was accessed by unknown third parties.

225. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiffs and the Class and the harm, and the substantial risk of imminent harm, suffered by Plaintiffs and the Nationwide Class.

226. The Private Information of Plaintiffs and Class Members was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

227. As a direct and proximate result of Defendant's breaches of its duties, Plaintiffs and Class Members have suffered and will continue to suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which

remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in their continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; (vii) the cost of future credit monitoring; and (viii) the diminished value of Defendant's services they received.

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

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

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

COUNT II
THIRD-PARTY BENEFICIARY CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class)

231. Plaintiffs re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

232. Defendants entered into various contracts with their clients to perform legal services.

233. These contracts were made in part for the benefit of Plaintiffs and the Class, as Plaintiffs and Class Members were the intended third-party beneficiaries of the contracts entered into between Defendants and their clients. The contracts were made with the intent and expectation that Plaintiffs' and Class Members' Private Information would remain private and would be adequately protected from unauthorized disclosure.

234. By permitting unauthorized third parties to access and exfiltrate the Private Information of Plaintiffs and the Class, Defendant breached its contracts with their clients.

235. Defendant knew that if it were to breach these contracts with their clients, the clients' customers—Plaintiffs and Class Members—would be harmed.

236. Defendant and its clients intended that Defendant's performance under their contracts would necessarily and directly benefit Plaintiffs and the Class. Defendant would collect payment from its clients to perform legal services for the

benefit of Plaintiffs and Class Members.

237. Defendant breached these contracts with their clients by, among other things, failing to (i) use reasonable data security measures and (ii) implement adequate protocols and employee training sufficient to protect Plaintiffs' and Class Members' Private Information from unauthorized disclosure to third parties.

238. As foreseen, Plaintiffs and the Class were harmed by Defendant's breach of their contracts with their clients, as such breach is alleged herein, and are entitled to compensatory damages they have sustained as a direct and proximate result thereof.

239. Plaintiffs and the Class seek damages, injunctive relief, and other and further relief as the Court may deem just and proper.

COUNT III
CALIFORNIA CONSUMER PRIVACY ACT
Cal. Civ. Code § 1798.100, *et seq.*
(On Behalf of Plaintiff Miller & the California Subclass)

240. Plaintiff Miller, individually and on behalf of the California Subclass, re-alleges and incorporates by reference the paragraphs above as if fully set forth herein.

241. Plaintiff Miller brings this claim individually and on behalf of the California Subclass against Houser for violation of the California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100, *et seq.* ("CCPA").

242. Plaintiff Miller and California Subclass Members are consumers and California residents as defined by Cal. Civ. Code § 1798.140(i).

243. Houser is a "business" as defined by Civ. Code § 1798.140(b) because it is partnership that does business in the state of California and has annual revenues in excess of $25,000,000.

244. The CCPA provides that "personal information" includes "[a]n individual's first name or first initial and the individual's last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted . . . (i) Social Security number." Civ. Code §§ 1798.150(a)(1) and 1798.81.5(d)(1)(A).

245. Plaintiff Miller and Class Members' names in combination with Social Security numbers, and other sensitive Private Information compromised in the Data Breach constitutes "personal information" within the meaning of the CCPA.

246. Through the Data Breach, Plaintiff Miller and Class Members' Private Information was accessed without authorization, exfiltrated, and stolen by criminals in a nonencrypted and/or nonredacted format.

247. The Data Breach occurred as a result of Defendant's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

248. Defendant violated the § 1798.150 of the CCPA by failing to protect Plaintiff Miller's and California Subclass Members' nonencrypted Private Information from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

249. Defendant had a duty to implement and maintain reasonable security practices to protect Plaintiff Miller's and California Subclass Members' Private Information. As detailed herein, Defendant failed to do so.

250. As a direct and proximate result of Defendant's acts, the Private Information of Plaintiff Miller's and California Subclass Members' Private Information was subjected to unauthorized access and exfiltration, theft, or disclosure.

251. Plaintiff Miller and the California Subclass seek injunctive or other equitable relief to ensure that Defendant hereinafter adequately safeguards Private Information by implementing reasonable security procedures and practices. This relief is important because Defendant still holds Private Information related to Plaintiffs and the California Subclass. Plaintiffs and the California Subclass have an interest in ensuring that their Private Information is reasonably protected.

252. On August 6, 2024, Plaintiff Miller's counsel sent a CCPA notice letter to Defendant via certified mail. If Defendant does not cure the effects of the Data

Breach, which would require retrieving the Private Information or securing the Private Information from continuing and future use, within 30 days of delivery of such CCPA notice letter (which Plaintiffs believe any such cure is not possible under these facts and circumstances), Plaintiff shall seek actual damages and statutory damages of no less than $100 and up to $750 per customer record subject to the Data Breach on behalf of the California Subclass as authorized by the CCPA.

COUNT IV
VIOLATION OF THE WASHINGTON CONSUMER PROTECTION ACT RCW 19.86.010, *et seq.*,
(On Behalf of Plaintiff Simmons & the Washington Subclass)

253. Plaintiff Simmons and the Washington Subclass re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

254. The Washington State Consumer Protection Act, RCW 19.86.020 (the "WCPA") prohibits any "unfair or deceptive acts or practices" in the conduct of any trade or commerce as those terms are described by the WCPA and relevant case law.

255. Defendant is a "person" as described in RWC 19.86.010(1).

256. Defendant engages in "trade" and "commerce" as described in RWC 19.86.010(2) in that they engage in the sale of services and commerce directly and indirectly affecting the people of the State of Washington.

257. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach,

Defendant engaged in unlawful, unfair, and fraudulent practices within the meaning, and in violation of, the WCPA, in that Defendant's practices were injurious to the public interest because they injured other persons, had the capacity to injure other persons, and have the capacity to injure other persons.

258. Defendant's failure to safeguard the Private Information exposed in the Data Breach constitutes an unfair act that offends public policy.

259. Defendant's failure to safeguard the Private Information compromised in the Data Breach caused substantial injury to Plaintiff Simmons and the Washington Subclass Members. Defendant's failure is not outweighed by any countervailing benefits to consumers or competitors, and it was not reasonably avoidable by consumers.

260. Defendant's failure to safeguard the Private Information disclosed in the Data Breach, and its failure to provide timely and complete notice of the Data Breach to the victims, is unfair because these acts and practices are immoral, unethical, oppressive, and/or unscrupulous.

261. In the Course of conducting their business, Defendant committed "unfair or deceptive acts or practices" by, inter alia, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Subclass Members'

Private Information, and violating the common law alleged herein in the process. Plaintiff and Subclass Members reserve the right to allege other violations of law by Defendant constituting other unlawful business acts or practices. As described above, Defendant's wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

262. Defendant also violated the WCPA by failing to timely notify, and by concealing from Plaintiff and Subclass Members, information regarding the unauthorized release and disclosure of their Private Information. If Plaintiff and Subclass Members had been notified in an appropriate fashion, and had the information not been hidden from them, they could have taken precautions to safeguard and protect their Private Information and identities.

263. The gravity of Defendant's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

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

265. As a direct and proximate result of Defendant's above-described wrongful action, inaction, omissions, and want of ordinary care that directly and indirectly and proximately caused the Data Breach and their violations of the WCPA, Plaintiff and Subclass Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, inter alia, (1) an imminent, immediate and continuing increased risk of identity theft and fraud—risks justifying expenditures from protective and remedial services for which they are entitled to compensation; (2) invasion of privacy; (3) breach of confidentiality of their Private Information; (4) deprivation of the value of their Private Information, for which there is a well-established national and international market; and/or (5) the financial and temporal cost of monitoring credit, monitoring financial accounts, and mitigating damages.

266. Unless restrained or enjoined, Defendant will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiff, therefore, on behalf of the Washington Subclass, seeks restitution and an injunction prohibiting Defendant from continuing such wrongful conduct, requiring Defendant to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect the Private Information, and requiring Defendant to delete, destroy, or purge any Private Information belonging

to Plaintiff and Class Members that Defendant no longer has a legitimate business reason for retaining.

267. Plaintiff, individually and on behalf of the Washington Subclass, also seeks to recover actual damages sustained by each Subclass Member together with the costs of the suit, including reasonable attorney fees. In addition, Plaintiff, individually and on behalf of Subclass Members, requests that this Court use its discretion, pursuant to RCW 19.86.090, to increase the damages award for each Subclass Member by three times the actual damages sustained, not to exceed $25,000 per Subclass Member.

COUNT V
DECLARATORY AND INJUNCTIVE RELIEF
(On Behalf of Plaintiffs & the Nationwide Class)

268. Plaintiffs and the Class re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

269. Plaintiffs pursue this claim under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

270. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and granting further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

271. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard Plaintiffs' and Class Members' Private Information, and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from future data breaches that compromise their Private Information. Plaintiffs and the Class remain at imminent risk that further compromises of their Private Information will occur in the future.

272. The Court should also issue prospective injunctive relief requiring Defendant to employ adequate security practices consistent with law and industry standards to protect Private Information.

273. Further, the Court should issue injunctive relief requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information weighed against the privacy interests of Plaintiffs and Class Members.

274. Defendant still possesses the Private Information of Plaintiffs and the Class.

275. To Plaintiffs' knowledge, Defendant has made no announcement that it has changed its data retention practices relating to the Private Information.

276. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at Houser LLP. The risk of another such breach is real, immediate, and substantial.

277. As described above, actual harm has arisen in the wake of the Data Breach regarding Defendant's duties of care to provide security measures to Plaintiffs and Class Members. Further, Plaintiffs and Class members are at risk of additional or further harm due to the exposure of their Private Information and Defendant's failure to address the security failings that led to such exposure.

278. There is no reason to believe that Defendant's employee training and security measures are any more adequate now than they were before the breach to meet Defendant's legal duties.

279. The hardship to Plaintiffs and Class Members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another data breach occurs at Houser, Plaintiffs and Class Members will likely continue to be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

280. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Houser, thus eliminating the additional injuries that would result to Plaintiffs and Class Members.

281. Plaintiffs, therefore, seek a declaration (i) that Defendant's existing data security measures do not comply with its duties of care to provide adequate data security, and (ii) that to comply with its duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to, the following:

a. Ordering that Defendant engage internal security personnel to conduct testing, including audits on Defendant's systems, on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendant audit, test, and train its security personnel and employees regarding any new or modified data security policies and procedures;

d. Ordering that Defendant purge, delete, and destroy, in a reasonably secure manner, any Private Information not necessary for its provision

of services;

e. Ordering that Defendant conduct regular database scanning and security checks; and

f. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel and employees how to safely share and maintain highly sensitive personal information, including but not limited to, client personally identifiable information.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the Class, requests judgment against Defendant and that the Court grant the following:

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

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

C. For injunctive relief requested by Plaintiffs, including, but not limited to, injunctive and other equitable relief as is necessary to protect the

interests of Plaintiffs and Class Members, including but not limited to an order:

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

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

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

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

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

vi. requiring Defendant to engage independent third-party security

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

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

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

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

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

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities

with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

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

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

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

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their

confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

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

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

F. For prejudgment interest on all amounts awarded; and

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

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

Date: August 8, 2024

Respectfully Submitted,

/s/ *Joseph M. Lyon*

Joseph M. Lyon (CA Bar # 351117)
Kevin M. Cox*
THE LYON FIRM
9210 Irvine Center Drive, Suite 200
Irvine, CA 92618
Phone: (513) 381-2333
Fax: (513) 766-9011
jlyon@thelyonfirm.com
kcox@thelyonfirm.com

John J. Nelson (SBN 317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
280 S. Beverly Drive
Beverly Hills, CA 90212
Telephone: (858) 209-6941
Email: jnelson@milberg.com

M. Anderson Berry (SBN 262879)
aberry@justice4you.com
Gregory Haroutunian (SBN 330263)
gharoutunian@justice4you.com
Brandon P. Jack (SBN 325584)
bjack@justice4you.com
CLAYEO C. ARNOLD
A PROFESSIONAL CORPORATION
12100 Wilshire Boulevard, Suite 800
Los Angeles, CA 90025
Telephone: (747) 777-7748

Paul M. Demarco (SBN 112834)
pdemarco@msdlegal.com
MARKOVITS, STOCK & DEMARCO, LLC
119 East Court Street, Suite 530

Cincinnati, OH 45202
Telephone: (513) 651-3700
Facsimile: (513) 665-0219

Zachary O. Chambers*
zchambers@classlawdc.com
MIGLIACCIO & RATHOD LLP
412 H Street NE, no. 302,
Washington, DC, 20002
Office: (202) 470-3520

Robert Mackey (SBN 125961)
bobmackeyesq@aol.com
LAW OFFICES OF ROBERT MACKEY
660 Baker Street
Building A, Ste. 201
Costa Mesa, CA 92626

Counsel for Plaintiffs and Putative Class

* *Admitted Pro Hac Vice*