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

Attorney for Plaintiffs and the Proposed Class

IN THE UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

RICHARD McMILLEN, individually and on behalf of all others similarly situated, Plaintiff, v. HOUSER LLP, Defendant.	Case No.: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Richard McMillen ("Plaintiff"), individually and on behalf of all others similarly situated, brings this class action against Defendant Houser LLP ("Defendant" or "Houser"), and alleges as follows:

I. JURISDICTION AND VENUE

1. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d) because (1) the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, (2) the action is a class

action, (3) there are members of the proposed Class who are diverse from Defendant, and (4) there are more than 100 proposed Class members.

2. This Court has general personal jurisdiction over Defendant because Defendant is a resident and citizen of this district, Defendant conducts substantial business in this district, and the events giving rise to Plaintiff's claims arise out of Defendant's contacts with this district.

3. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(1) & (2) because Defendant is a resident and citizen of this district and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this district.

II. PARTIES

4. Plaintiff Richard McMillen is a resident and citizen of Florida.

5. Defendant Houser LLP is a California stock limited liability partnership with its principal place of business at 9970 Research Drive, Irvine, CA 92618.

6. Upon information and belief, Houser LLP has at least one member, Eric D. Houser, A Law Corporation, who is a resident and citizen of California, residing in North Tustin, California. Eric Houser is listed as the managing partner on the Houser website.[1]

[1] https://houser-law.com/business/eric-houser/ (last visited March 4, 2024)

III. FACTUAL ALLEGATIONS

HOUSER LLP

7. Houser LLP is a law firm serving Fortune 500 companies and businesses of all size with eleven offices nationwide.

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

9. Plaintiff and Class members are customers of Defendant's clients.

10. Plaintiff and Class members provided certain Personally Identifying Information ("PII") to clients of Defendant, which clients then provided the information to Defendant.

11. As a sophisticated legal services provider with an acute interest in maintaining the confidentiality of the PII entrusted to it, Defendant is well-aware of the numerous data breaches that have occurred throughout the United States and its responsibility for safeguarding PII in its possession. Defendant represents to consumers and the public that it "takes the confidentiality, privacy, and security of information in our care seriously."[2]

[2] See Notice of Data Breach Notification Letter sent to Plaintiff, dated February 28, 2024, attached hereto as Exhibit A.

The Data Breach

12. On May 9, 2023, Houser discovered that certain files on their computer systems had been encrypted.[3]

13. Houser launched an investigation, with the assistance of third-party forensic investigators, to determine the nature and scope of the data breach.[4]

14. Through its investigation, Houser determined that there was unauthorized access to its computer network between May 7, 2023 and May 9, 2023, during which time certain files were copied and taken from Houser's network.[5]

15. After the files were copied and taken from Houser's network, the unauthorized criminal actors encrypted files on the network through the use of malicious software that the unauthorized persons had successfully deployed within Houser's network.

16. The encrypted files were discovered by Houser on May 9, 2023.[6]

17. Upon information and belief, the cybercriminal demanded that Houser pay a ransom in exchange for providing a decryption key for the encrypted files.

[3] *Id.*
[4] *Id.*
[5] *Id.*
[6] *Id.*

18. Upon information and belief, Houser paid the ransom in June 2023, at which time the cybercriminals claimed that they had deleted the files that were taken out of Houser's network.

19. However, assurances from cybercriminals that they deleted stolen, sensitive PII are worthless, as it involves trusting the very criminal actors who perpetrated the cyberattack in the first instance.

20. In a ransomware attack the attackers use software to encrypt data on a compromised network, rendering it unusable and demanding payment to restore control over the network.[7] 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."

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

[7] *Ransomware FAQs*, available at https://www.cisa.gov/stopransomware/ransomware-faqs

[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

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]

22. The files that were taken out of Houser's network by the cybercriminals including confidential PII belonging to Plaintiff and the putative Class Members here.

23. The compromised data includes Plaintiff's name and Social Security number, and affected persons' names, "Social Security number, driver's license number, individual tax identification number, financial account information, and medical information."[13]

[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/

[10] 2020 Ransomware Marketplace Report, available at https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report

[11] *Id*.

[12] *Id*.

[13] file:///C:/Users/dliet/Downloads/Houser%20LLP%20-%20Notice%20of%20Data%20Event%20-%20ME%20(1).pdf (last accessed March 4, 2024)

24. According to a notice of data breach filed with the Attorney General of Maine, the Data Breach has affected 326,386 individuals, including Plaintiff ("Data Breach").[14]

25. Defendant began notifying affected persons on February 28, 2024.[15]

26. Defendant's Data Breach notice letter also offered free credit monitoring services to Plaintiff, and similar monitoring was offered to those potentially impacted by the breach.

27. Houser also offered guidance to Plaintiff and potentially affected individuals on how better to protect themselves against identity theft and fraud, demonstrating that despite the alleged deletion of the stolen data by the cyberthieves, Houser itself believes that there is still a threat to Plaintiff and other affected persons of identity theft or fraud.

28. In correspondence to the Maine Attorney General, Houser identified multiple post-breach security changes, including changes to endpoint detection software, implementation of multi-factor authentication for Outlook 365, net extender VPNB and remote desktop connection, and ransomware detection software.

29. Defendant did not state why it was unable to prevent the Data Breach or which security feature failed. However, the post-incident data security changes

[14] https://apps.web.maine.gov/online/aeviewer/ME/40/f0c4fd5b-bb10-48f3-82f5-d46753d726a4.shtml (last accessed March 4, 2024)

[15] *Id.*

demonstrate that this data breach most likely occurred as a result of inadequate or out-of-date endpoint detection software, failure to employ multi-factor authentication on Outlook 365, and failure to employ ransomware detection software.

30. Defendant did not contact affected persons about the breach discovered May 9, 2023 until over ninth months had passed after discovering the breach.

31. Defendant failed to prevent the data breach because it did not adhere to commonly accepted security standards and failed to detect that its databases were subject to a security breach for approximately two days (from May 7, 2023 until May 9, 2023).

Injuries to Plaintiff and the Class

32. Shortly after February 28, 2024, Plaintiff received a breach notification from Defendant indicating that his Personally Identifiable Information ("PII") was compromised during the Data Breach.[16] According to the notification letter, the Data Breach exposed Plaintiff's name and Social Security number.

33. Plaintiff is very concerned about the theft of his PII and has and will continue to spend substantial amounts of time and energy monitoring his credit status. Had Plaintiff known that Defendant or anyone in Defendant's position would not implement reasonable data security necessary to protect his PII, he would not have entrusted it, directly or indirectly, to Defendant.

[16] *See* Exhibit A.

34. As a direct and proximate result of Defendant's actions and omissions in failing to protect Plaintiff's PII and PHI, Plaintiff and the Class have been damaged.

35. Plaintiff and the Class have been placed at a substantial risk of harm in the form of fraud or identity theft and have incurred and will likely incur additional damages, including spending substantial amounts of time monitoring accounts and records, in order to prevent and mitigate credit fraud, identity theft, and financial fraud.

36. In addition to the irreparable damage that may result from the theft of PII, identity theft victims must spend numerous hours and their own money repairing the impacts caused by this breach. Plaintiff and the Class will spend substantial time and expense (a) monitoring their accounts to identify fraudulent or suspicious charges; (b) cancelling and reissuing cards; (c) purchasing credit monitoring and identity theft prevention services; (d) attempting to withdraw funds linked to compromised, frozen accounts; (e) removing withdrawal and purchase limits on compromised accounts; (f) communicating with financial institutions to dispute fraudulent charges; (g) resetting automatic billing instructions and changing passwords; (h) freezing and unfreezing credit bureau account information; (i) cancelling and re-setting automatic payments as necessary; and (j) paying late fees and declined payment penalties as a result of failed automatic payments.

37. Additionally, Plaintiff and the Class have suffered or are at increased risk of suffering from, *inter alia*, the loss of the opportunity to control how their PII is used,

the diminution in the value and/or use of their PII entrusted to Defendant by Defendant's clients, and loss of privacy.

The Value of PII and PHI

38. People place a high value not only on their PII, but also on the privacy of that data. This is because identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.[17]

39. People are particularly concerned with protecting the privacy of their financial account information and social security numbers, which are the "secret sauce" that is "as good as your DNA to hackers."[18] There are long-term consequences to data breach victims whose social security numbers are taken and used by hackers. Even if they know their social security numbers have been accessed, Plaintiff and Class members cannot obtain new numbers unless they become a victim of social security number misuse. Even then, the Social Security Administration has warned that "a new number probably won't solve all [] problems … and won't guarantee … a fresh start."[19]

[17] Identity Theft Resource Center, *Identity Theft: The Aftermath 2017*, https://www.ftc.gov/system/files/documents/public_comments/2017/10/00004-141444.pdf.

[18] Cameron Huddleston, *How to Protect Your Kids From the Anthem Data Breach*, Kiplinger, (Feb. 10, 2015), https://www.kiplinger.com/article/credit/T048-C011-S001-how-to-protect-your-kids-from-the-anthem-data-brea.html.

[19] Social Security Admin., *Identity Theft and Your Social Security Number*, at 6-7, https://www.ssa.gov/pubs/EN-05-10064.pdf.

Industry Standards for Data Security

40. Defendant is, or reasonably should have been, aware of the importance of safeguarding PII, as well as of the foreseeable consequences of its systems being breached.

41. Security standards commonly accepted among businesses that store PII and PHI using the internet include, without limitation:

a. Employing multi-factor authentication for email accounts;

b. Maintaining a secure firewall configuration;

c. Monitoring for suspicious or irregular traffic to servers;

d. Monitoring for suspicious credentials used to access servers;

e. Monitoring for suspicious or irregular activity by known users;

f. Monitoring for suspicious or unknown users;

g. Monitoring for suspicious or irregular server requests;

h. Monitoring for server requests for PII;

i. Monitoring for server requests from VPNs; and

j. Monitoring for server requests from Tor exit nodes.

42. The U.S. Federal Trade Commission ("FTC") publishes guides for businesses for cybersecurity[20] and protection of PII and PHI[21] which includes basic security standards applicable to all types of businesses.

43. The FTC recommends that businesses:

a. Identify all connections to the computers where you store sensitive information.

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

[20] Start with Security: A Guide for Business, FTC (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[21] Protecting Personal Information: A Guide for Business, FTC (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting personalinformation.pdf.

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks.

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

44. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, 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, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[22]

45. Because Defendant was entrusted with consumers' PII, it had, and has, a duty to consumers to keep their PII secure.

46. Consumers, such as Plaintiff and the Class, reasonably expect that when they provide PII to companies or when those companies forward their PII to companies such as Defendant, that their PII will be safeguarded.

[22] Federal Trade Commission, *Privacy and Security Enforcement: Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement.

47. Nonetheless, Defendant failed to prevent the Data Breach by (upon information and belief) failing to utilize adequate or updated endpoint detection software, failing to use multi-factor authentication for its Outlook 365 accounts, failure to employ VPN connections, failure to properly configure remote access to block malicious activity, and failure to employ anti-ransomware software.

48. Had Defendant properly maintained and adequately protected its systems, it could have prevented the Data Breach.

49. Plaintiff and Class members are at a heightened risk of identity theft for years to come.

50. The unencrypted PII of Class members will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted PII may fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class members. As a result of the Data Breach, unauthorized individuals can now easily access the PII of Plaintiff and Class members.

51. 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.

52. 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 calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victim.

53. One such example of criminals piecing together bits and pieces of compromised Personal Information for profit is the development of "Fullz" packages.[23] With "Fullz" packages, cyber-criminals can cross-reference two sources of Personal 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 dossiers on individuals.

[23] "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-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/ (last visited on May 26, 2023).

54. The development of "Fullz" packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and Class members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still 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.

55. The existence and prevalence of "Fullz" packages means that the PII stolen from the data breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiff and the other Class members.

56. Thus, even if certain information (such as emails or telephone numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

57. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

58. PII is a valuable property right.[24] Its value is axiomatic, considering the value of big data in corporate America and the consequences of cyber thefts include

[24] *See, e.g.,* Randall T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("Personal Information") Equals the "Value" of Financial Assets, 15 Rich.

heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

59. An active and robust legitimate marketplace for PII exists. In 2022, the data brokering industry was worth roughly $268 billion.[25] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[26,27] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[28]

60. Users of the personal data collection app Streamlytics can earn up to $200 a month by selling their personal information to marketing companies who use it to build consumer demographics profiles.[29]

61. Consumers also recognize the value of their PII and offer it in exchange for goods and services or use it to verify their identity and to gain access to financial products. The value of PII can be derived not by a price at which consumers themselves actually seek to sell it, but rather in the economic benefit consumers derive from being

---

J.L. & Tech. 11, at *3-4 (2009) ("Personal 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).

[25] https://www.maximizemarketresearch.com/market-report/global-data-broker-market/55670/

[26] https://datacoup.com/

[27] https://digi.me/what-is-digime/

[28] Nielsen Computer & Mobile Panel, *Frequently Asked Questions, available at* https://computermobilepanel.nielsen.com/ui/US/en/faqen.html

[29] How To Sell Your Own Data And Why You May Want to, available at https://www.mic.com/impact/selling-personal-data-streamlytics

able to use it and control the use of it. For example, Plaintiff and Class members were only able to obtain services from Defendant or its clients after providing it with their PII and their ability to use their PII is encumbered when their identity or credit profile is infected by misuse or fraud. For example, a consumer with false or conflicting information on their credit report may be denied credit or be forced to pay a higher interest rate.

62. As a result of the Data Breach, Plaintiff's and Class members' {II, 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 Plaintiff or Class members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

63. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change, e.g., names and Social Security numbers.

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

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

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[30]

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

IV. CLASS ACTION ALLEGATIONS

67. Plaintiff, individually and on behalf of all others, brings this class action pursuant to Fed. R. Civ. P. 23.

68. The proposed Class is defined as follows:

> ***Nationwide Class***: *All persons whose PII and PHI was maintained on Defendant's servers and was compromised in the Data Breach.*

[30] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last visited Oct. 17, 2022).

69. *Numerosity*: The proposed Class is so numerous that joinder of all members is impracticable. Although the precise number is not yet known to Plaintiff, Defendant has reported that the number of persons affected by the Data Breach is 326,386. The Class members can be readily identified through Defendant's records.

70. *Commonality*: Questions of law or fact common to the Class include, without limitation:

a. Whether Defendant owed a duty or duties to Plaintiff and the Class to exercise due care in collecting, storing, safeguarding, and obtaining their PII;

b. Whether Defendant breached that duty or those duties;

c. Whether Defendant failed to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records to protect against known and anticipated threats to security;

d. Whether the security provided by Defendant was satisfactory to protect customer information as compared to industry standards;

e. Whether Defendant misrepresented or failed to provide adequate information to customers regarding the type of security practices used;

f. Whether Defendant knew or should have known that it did not employ reasonable measures to keep Plaintiff's and the Class's PII secure and prevent loss or misuse of that PII;

g. Whether Defendant acted negligently in connection with the monitoring and protecting of Plaintiff's and Class's PII;

h. Whether Defendant's conduct was intentional, willful, or negligent;

i. Whether Defendant violated any and all statutes and/or common law listed herein;

j. Whether the Class suffered damages as a result of Defendant's conduct, omissions, or misrepresentations; and

k. Whether the Class is entitled to injunctive, declarative, and monetary relief as a result of Defendant's conduct.

71. *Typicality*: The claims or defenses of Plaintiff are typical of the claims or defenses of the Class. Class members were injured and suffered damages in substantially the same manner as Plaintiff, Class members have the same claims against Defendant relating to the same course of conduct, and Class members are entitled to relief under the same legal theories asserted by Plaintiff.

72. *Adequacy*: Plaintiff will fairly and adequately protect the interests of the proposed Class and has no interests antagonistic to those of the proposed Class. Plaintiff

has retained counsel experienced in the prosecution of complex class actions including, but not limited to, data breaches.

73. *Predominance*: Questions of law or fact common to proposed Class members predominate over any questions affecting only individual members. Common questions such as whether Defendant owed a duty to Plaintiff and the Class and whether Defendant breached its duties predominate over individual questions such as measurement of economic damages.

74. *Superiority*: A class action is superior to other available methods for the fair and efficient adjudication of these claims because individual joinder of the claims of the Class is impracticable. Many members of the Class are without the financial resources necessary to pursue this matter. Even if some members of the Class could afford to litigate their claims separately, such a result would be unduly burdensome to the courts in which the individualized cases would proceed. Individual litigation increases the time and expense of resolving a common dispute concerning Defendant's actions toward an entire group of individuals. Class action procedures allow for far fewer management difficulties in matters of this type and provide the unique benefits of unitary adjudication, economies of scale, and comprehensive supervision over the entire controversy by a single judge in a single court.

75. *Manageability*: Plaintiff is unaware of any difficulties that are likely to be encountered in the management of this action that would preclude its maintenance as a class action.

76. The Class may be certified pursuant to Rule 23(b)(2) because Defendant has acted on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

77. The Class may also be certified pursuant to Rule 23(b)(3) because questions of law and fact common to the Class will predominate over questions affecting individual members, and a class action is superior to other methods for fairly and efficiently adjudicating the controversy and causes of action described in this Complaint.

78. Particular issues under Rule 23(c)(4) are appropriate for certification because such claims present particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein.

V. CAUSES OF ACTION

COUNT I
NEGLIGENCE
(on behalf of the Nationwide Class)

79. Plaintiff hereby incorporates by reference all preceding paragraphs as though fully set forth herein.

80. Defendant owed a duty of care to Plaintiff and Class members to use reasonable means to secure and safeguard the entrusted PII, to prevent its unauthorized

access and disclosure, to guard it from theft, and to detect any attempted or actual breach of its systems. These common law duties existed because Plaintiff and Class members were the foreseeable and probable victims of any inadequate security practices. In fact, not only was it foreseeable that Plaintiff and Class members would be harmed by the failure to protect their PII because hackers routinely attempt to steal such information and use it for nefarious purposes, but Defendant knew that it was more likely than not Plaintiff and Class members would be harmed by such exposure of their PII.

81. Defendant owed a duty to prevent the reasonably foreseeable cyberattack that occurred here, and to prevent the access to and theft of Plaintiff and Class Members' confidential PII.

82. Defendant's duties to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act ("FTC 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 PII and PHI. Various FTC publications and data security breach orders further form the basis of Defendant's duties. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

83. Defendant's violations of Section 5 of the FTC Act constitute evidence of negligence.

84. Defendant breached the aforementioned duties when it failed to use security practices that would protect the PII provided to it by Plaintiff and Class members, thus resulting in unauthorized third-party access to the Plaintiff's and Class members' PII.

85. Defendant further breached the aforementioned duties by failing to design, adopt, implement, control, manage, monitor, update, and audit its processes, controls, policies, procedures, and protocols to comply with the applicable laws and safeguard and protect Plaintiff's and Class members' PII and PHI within its possession, custody, and control.

86. As a direct and proximate cause of failing to use appropriate security practices, Plaintiff's and Class members' PII was disseminated and made available to unauthorized third parties.

87. Defendant admitted that Plaintiff's and Class members' PII was wrongfully disclosed as a result of the breach.

88. The breach caused direct and substantial damages to Plaintiff and Class members, as well as the possibility of future and imminent harm through the dissemination of their PII and the greatly enhanced risk of fraud or identity theft.

89. By engaging in the forgoing acts and omissions, Defendant committed the common law tort of negligence. For all the reasons stated above, Defendant's conduct was negligent and departed from reasonable standards of care including by, but not

limited to: failing to adequately protect the PII; failing to conduct regular security audits; and failing to provide adequate and appropriate supervision of persons having access to Plaintiff's and Class members' PII.

90. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and the Class, their PII would not have been compromised.

91. Neither Plaintiff nor the Class contributed to the breach or subsequent misuse of their PII as described in this Complaint. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and the Class have been put at an increased risk of fraud or identity theft, and Defendant has an obligation to mitigate damages by providing adequate credit and identity monitoring services. Defendant is liable to Plaintiff and the Class for the reasonable costs of future credit and identity monitoring services for a reasonable period of time, substantially in excess of one year. Defendant is also liable to Plaintiff and the Class to the extent that they have directly sustained damages as a result of identity theft or other unauthorized use of their PII, including the amount of time Plaintiff and the Class have spent and will continue to spend as a result of Defendant's negligence. Defendant is also liable to Plaintiff and the Class to the extent their PII has been diminished in value because Plaintiff and the Class no longer control their PII and to whom it is disseminated.

COUNT II
INVASION OF PRIVACY
(on behalf of the Nationwide Class)

92. Plaintiff hereby incorporates by reference all preceding paragraphs as though fully set forth herein.

93. Plaintiff and Class members have objective reasonable expectations of solitude and seclusion in their personal and private information and the confidentiality of the content of personal information and non-public medical information.

94. Defendant invaded Plaintiff's and the Class's right to privacy by allowing the unauthorized access to their PII and by failing to maintain the confidentiality of Plaintiff's and the Class's PII, as set forth above.

95. The intrusion was offensive and objectionable to Plaintiff, the Class, and to a reasonable person of ordinary sensibilities in that Plaintiff's and the Class's PII was disclosed without prior written authorization from Plaintiff and the Class.

96. The intrusion was into a place or thing which was private and is entitled to be private, in that Plaintiff and the Class provided and disclosed their PII to Defendant privately with an intention that the PII would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class were reasonable to believe that such information would be kept private and would not be disclosed without their written authorization.

97. As a direct and proximate result of Defendant's above acts, Plaintiff's and the Class's PII was viewed, distributed, and used by persons without prior written authorization and Plaintiff and the Class suffered damages as described herein.

98. Defendant is guilty of oppression, fraud, or malice by permitting the unauthorized disclosure of Plaintiff's and the Class's PII with a willful and conscious disregard of their right to privacy.

99. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause Plaintiff and the Class great and irreparable injury in that the PII maintained by Defendant can be viewed, printed, distributed, and used by unauthorized persons. Plaintiff and the Class have no adequate remedy at law for the injuries in that a judgment for the monetary damages will not end the invasion of privacy for Plaintiff and the Class, and Defendant may freely treat Plaintiff's and the Class's PII with sub-standard and insufficient protections.

COUNT III
BREACH OF QUASI-CONTRACT/UNJUST ENRICHMENT
(on behalf of the Nationwide Class)

100. Plaintiff hereby incorporates by reference all preceding paragraphs as though fully set forth herein.

101. Plaintiff and the Class have an interest, both equitable and legal, in their PII that was conferred upon, collected by, and maintained by Defendant and that was ultimately compromised in the data breach.

102. Defendant, by way of its acts and omissions, knowingly and deliberately enriched itself by saving the costs it reasonably should have expended on security measures to secure Plaintiff's and the Class's PII.

103. Defendant also understood and appreciated that the PII pertaining to Plaintiff and the Class was private and confidential and its value depended upon Defendant maintaining the privacy and confidentiality of that PII.

104. Instead of providing for a reasonable level of security that would have prevented the breach—as is common practice among companies entrusted with such PII—Defendant instead consciously and opportunistically calculated to increase its own profits at the expense of Plaintiff and the Class. Nevertheless, Defendant continued to obtain the benefits conferred on it by Plaintiff and the Class. The benefits conferred upon, received, and enjoyed by Defendant were not conferred officiously or gratuitously, and it would be inequitable and unjust for Defendant to retain these benefits.

105. Plaintiff and the Class, on the other hand, suffered as a direct and proximate result. As a result of Defendant's decision to profit rather than provide requisite security, and the resulting breach disclosing Plaintiff's and the Class's PII, Plaintiff and the Class suffered and continue to suffer considerable injuries in the forms of, *inter alia,* attempted identity theft, time and expenses mitigating harms, diminished value of PII, loss of privacy, and increased risk of harm.

106. Thus, Defendant engaged in opportunistic conduct in spite of its duties to Plaintiff and the Class, wherein it profited from interference with Plaintiff's and the Class's legally protected interests. As such, it would be inequitable, unconscionable, and unlawful to permit Defendant to retain the benefits it derived as a consequence of its conduct.

107. Accordingly, Plaintiff, on behalf of himself and the Class, respectfully request that this Court award relief in the form of restitution or disgorgement in the amount of the benefit conferred on Defendant as a result of its wrongful conduct, including specifically, the amounts that Defendant should have spent to provide reasonable and adequate data security to protect Plaintiff's and the Class's PII, and/or compensatory damages.

VI. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, prays for a judgment against Defendant as follows:

a. For an order certifying the proposed Class, appointing Plaintiff as Representative of the proposed Class, and appointing the law firms representing Plaintiff as counsel for the Class;

b. For compensatory and punitive and treble damages in an amount to be determined at trial;

c. Payment of costs and expenses of suit herein incurred;

d. Both pre-and post-judgment interest on any amounts awarded;

e. Payment of reasonable attorneys' fees and expert fees;

f. Such other and further relief as the Court may deem proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands trial by jury,

Dated: March 4, 2024

Respectfully submitted,

/s/ John J. Nelson

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

Counsel for Plaintiff and Proposed Class

ClassAction.org
