UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF OHIO
WESTERN DIVISION

IN RE MARSHALL & MELHORN, LLC DATA BREACH LITIGATION	**Case No. 3:23-CV-01181** **Judge James R. Knepp, II**
This Document Relates to: All Actions	**CONSOLIDATED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Mark Hendrix and Kaitlyn Thiel, bring this Class Action Complaint ("Complaint") against Defendant Marshall & Melhorn, LLC ("Defendant"), an Ohio corporation, individually and on behalf of all others similarly situated ("Class Members"), and allege, upon personal knowledge as to their own actions and their counsel's investigations, and upon information and belief as to all other matters as follows:

INTRODUCTION

1. Defendant experienced a cyberattack in September 2021 (the "Data Breach"). Plaintiffs bring this class action against Defendant on behalf of themselves and approximately 27,000 Class Members for Defendant's failure to properly secure and safeguard personally identifiable information ("PII") and protected health information ("PHI") that was stolen during the Data Breach, including: full names, addresses, Social Security numbers, financial account information, driver's licenses and state identification information, passport information, medical information, and health insurance information (collectively, "Private Information").

2. Defendant maintained Plaintiffs' and Class Members' Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer system and network in a condition vulnerable to cyberattacks. Upon information and belief, the

mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

3. The Private Information that was stolen is one-stop shopping for identity thieves to wreak complete havoc on their victims' lives. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, e.g., opening new financial accounts in Class Members' names or accessing existing accounts, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest. Given the sensitivity and static nature of the Private Information involved (such as names, Social Security numbers, and medical information), Plaintiffs and Class Members will be forced to live in fear the rest of their lives.

4. Despite the substantial risk of harm that Plaintiffs and Class Members now face, Defendant waited nearly two years before informing them that their Private Information was compromised in the Data Breach.

5. The substantial risk of harm from the Data Breach has caused Plaintiffs and Class Members to incur losses of time, out of pocket expenses (e.g., credit monitoring services), and to suffer fear, stress, and anxiety. As a result of having their Private Information acquired by cybercriminals, Plaintiffs and Class Members have also suffered invasions of privacy, and many, including Plaintiff Hendrix, have suffered instances of actual theft, fraud, and other misuse of Private Information.

6. Plaintiffs bring claims against Defendant for: (i) negligence, (ii) negligence *per se*, (iii) breach of implied contract, (iv) breach of fiduciary duty, and (v) unjust enrichment.

7. Plaintiffs seek remedies on behalf of themselves and the Class Members, including, but not limited to, nominal, compensatory, and punitive damages, as well as injunctive and declaratory relief regarding the need for continued credit monitoring and the continued inadequacy of Defendant's data security policies, procedures, and protections.

THE PARTIES

8. Plaintiff Mark Hendrix is, and at all times mentioned herein was, an individual citizen of the State of Ohio. Plaintiff Hendrix was notified of the Data Breach and his Private Information being compromised upon receiving a data breach notice letter dated on or around May 19, 2023.

9. Plaintiff Kaitlyn Thiel is, and at all times mentioned herein was, an individual citizen of the State of Ohio. Plaintiff Thiel was notified of the Data Breach and her Private Information being compromised upon receiving a data breach notice letter dated on or around May 19, 2023.

10. Defendant is a domestic limited liability company organized in Ohio and headquartered at 4 Seagate #8, Toledo, Ohio 43604 with its principal place of business in Toledo, Ohio. Upon information and belief, all of Defendant's members are residents of the State of Ohio.

11. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiffs. Plaintiffs will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

12. All of Plaintiffs' claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

JURISDICTION & VENUE

13. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendant to establish minimal diversity.[1]

14. The Northern District of Ohio has personal jurisdiction over Defendant because Defendant and/or its parents or affiliates are headquartered in this Ohio, Defendant conducts substantial business in Ohio, Defendant caused injury to Plaintiffs in the State of Ohio, and, upon information and belief, Defendant's members are residents of the State of Ohio.

15. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

FACTUAL ALLEGATIONS

Defendant's Business

16. Defendant is a law firm with offices in Toledo, Findlay, and Perrysburg, Ohio.[2] It employs approximately 40 professionals who "represent businesses of all types and sizes—from Fortune 500 companies and multi-national corporations, to small businesses …."[3]

17. On information and belief, in the ordinary course of rendering its services to its

[1] Defendant reported to the Attorney General of Indiana that 647 Indiana residents were affected by the Data Breach: See https://www.in.gov/attorneygeneral/consumer-protection-division/id-theft-prevention/files/UPDATED_Data-Breach-Year-to-Date-Report-2023.pdf at page 10, line 355.

[2] https://www.marshall-melhorn.com/Our-Firm (last visited: August 15, 2023).

[3] https://www.marshall-melhorn.com/Professionals/Search?search= (last visited: August 15, 2023); https://www.marshall-melhorn.com/Services/86708/Litigation (last visited: August 18, 2023).

clients, Defendant requires its clients to turn over their Private Information, or that of their customers' and patients' Private Information.

18. Because of the highly sensitive and personal nature of the information Defendant acquires and stores, Defendant, knew or should have known about the importance of keeping Private Information confidential. As a law firm, Defendant is also aware that it has a duty to protect the Private Information in its possession, and to provide prompt notification if this information is acquired by a third party without authorization.

19. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and would not have entrusted Defendant or Defendant's clients with their information had they known that Defendant would fail to safeguard this information from foreseeable threats.

The Data Breach

20. On September 14, 2022, Defendant experienced a computer outage on its network.[4]

21. Between August 2021 and September 14, 2021, a third party gained unauthorized access to Defendant's computer systems. [5]

22. On May 19, 2023, Defendant notified its business clients and others who were affected by the Data Breach, including approximately 27,271 individuals.

23. The Private Information in the Data Breach, included individuals' full names, addresses, Social Security numbers, financial account information, driver's licenses and state identification information, and passport information. The Data Breach also compromised files containing the medical information and health insurance information of approximately 9,412

[4] *Id.*

[5] https://www.bleepingcomputer.com/news/security/engineering-firm-parker-discloses-data-breach-after-ransomware-attack/amp/ (last visited May 19, 2022).

individuals.[6]

24. Plaintiffs and Class Members provided their Private Information, directly or indirectly, to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access. Plaintiffs and Class Members also understood that if their Private Information was stolen, they would be notified within a reasonable amount of time.

25. Inexplicably, Defendant did not begin mailing notifications to victims of the Data Breach until June 7, 2023.

26. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class Members, including Social Security numbers, 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 Plaintiffs and Class Members as a result of a breach. Defendant's negligence in safeguarding the Private Information of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to companies like Defendant to protect and secure the sensitive data they possess.

27. 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. Indeed, "[m]ore than a quarter of law firms in a 2022 American Bar Association survey said they experienced a data breach, up 2% from the previous year." [7]

28. Therefore, the increase in such attacks and the attendant risk of future attacks were

[6] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Aug. 18, 2023).

widely known to the public and to anyone in Defendant's industry, including Defendant.

Defendant's Breach of Its Data Security Obligations to Plaintiffs and Class Members

29. Defendant could have prevented this Data Breach by properly securing and encrypting the files containing the Private Information of Plaintiffs and Class Members. Alternatively, Defendant should have destroyed data that it no longer needed. For example, Defendant maintained Plaintiffs Thiel's Social Security Number in unencrypted files at the time of the Data Breach even though she had not worked for Defendant for more than two years.

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

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

b. Failing to adequately protect customers' Private Information;

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

d. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;

e. Failing to train its employees in the proper handling of emails containing Private Information and maintain adequate email security practices;

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

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

h. Waiting almost two years to notify Plaintiffs and Class Members that their Private Information was compromised in the Data Breach.

31. Defendant negligently and unlawfully failed to safeguard Plaintiffs' and Class

Members' Private Information by allowing cyberthieves to access Defendant's computer network and systems which contained unsecured and unencrypted Private Information.

Defendant Fails to Comply with FTC Guidelines

32. 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.

33. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[8] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[9]

34. 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

---

[8] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited May 23, 2021).

[9] *Id.*

reasonable security measures.

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

36. Defendant failed to properly implement basic data security practices.

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

38. Defendant was at all times fully aware of its obligation to protect the Private Information obtained from its customers. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Fails to Comply with Industry Standards

39. As shown above, experts studying cyber security routinely identify entities operating in the legal space as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

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

limiting which employees can access sensitive data.

41. Other best cybersecurity practices that are standard in the legal industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

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

43. These foregoing frameworks are existing and applicable industry standards in the legal industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the data breach.

Plaintiffs and Class Members Face a Substantial Risk of Harm

44. Victims of all data breaches are exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, 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 otherwise harass or track the victim.

45. 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 individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

46. Here, the cybercriminals targeted and successfully exfiltrated Social Security numbers, which are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult, if not impossible, for an individual to change. Identity thieves use Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. Identity thieves also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

47. 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 Social Security number and assuming your identity can cause

a lot of problems.[10]

48. It is incredibly difficult 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.

49. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The 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."[11]

50. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, only 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, including Social Security number and name, is impossible to "close" and difficult, if not impossible, to change.

51. Criminals are also able to piece together bits and pieces of compromised Private Information for develop what are called "Fullz" packages.[12]

---

[10] *Identity Theft and Your Social Security Number*, Social Security Administration, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Jan. 13, 2021).

[11] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last accessed Jan. 17, 2022).

[12] "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.

52. With "Fullz" packages, 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 dossiers on individuals.

53. The development of "Fullz" packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' 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.

54. The existence and prevalence of "Fullz" packages means that the Private Information stolen from the data breach can easily be linked to the unregulated data of Plaintiffs and the other Class Members. Cybercriminals can then use this information to misrepresent their identity to gain access to financial and other accounts by providing verifying information compiled from unique sources.

55. Thus, even if certain information was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

56. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to

---

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 August 7, 2023).

identity thieves and other criminals (like illegal and scam telemarketers).

57. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[13]

58. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[14]

59. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[15]

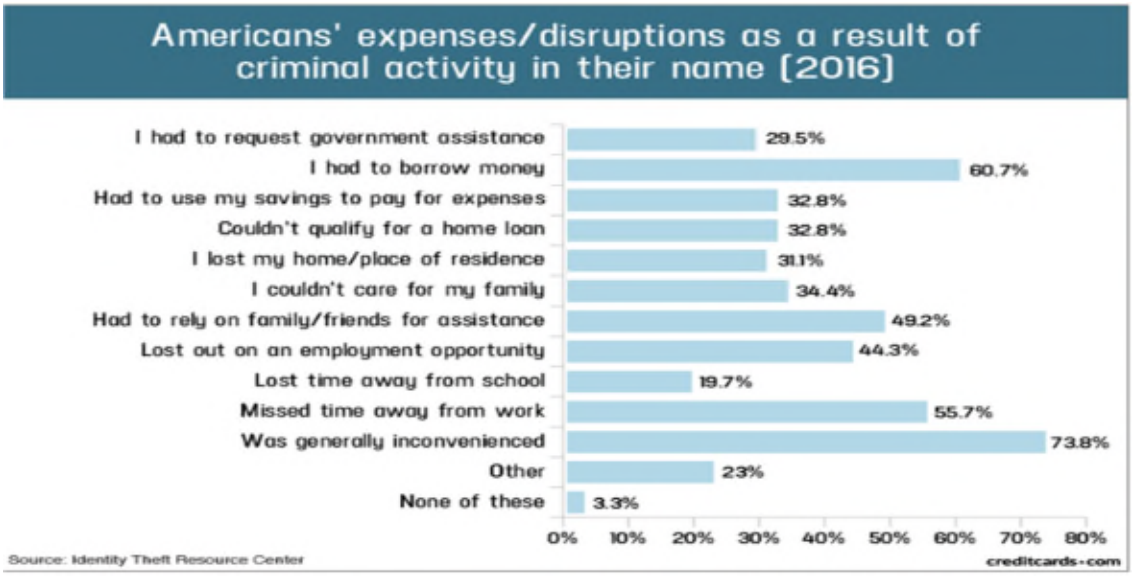
---

[13] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited May 23, 2021).

[14] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007). Available at https://www.gao.gov/new.items/d07737.pdf.

[15] *See* Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (Oct. 23, 2020)

https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php. (last visited May 27, 2021).



60. It must also be noted there may be a substantial time lag – measured in years – between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

61. According to the U.S. Government Accountability Office, 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.

See GAO Report, at p. 29.

62. Plaintiffs and Class Members must vigilantly monitor their financial and other accounts for many years to come. Yet, to date, Defendant has only offered Plaintiffs and Class Members temporary, non-automatic credit monitoring despite Plaintiffs and Class Members being forced to face a lifetime of risk of their financial information being compromised as a result of their sensitive, Private Information being exfiltrated in the Data Breach. Defendant's offer of temporary credit monitoring indicates that even Defendant understands that Plaintiffs and Class

Members now face a present and increased risk of harm due to their Private Information being exfiltrated from Defendant's systems by criminal threat actors.

The Value of Private Information

63. Private Information is an extremely valuable property right.[16]

64. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that 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.

65. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[17] Other studies show that 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.

66. Static information that does not change like names, Social Security numbers, and health information, is particularly valuable. Martin Walter, senior director at cybersecurity firm

---

[16] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[17] *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/.

[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 accessed Jan. 17, 2022).

[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 accessed Jan. 17, 2022).

RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[20]

67. An active and robust legitimate marketplace for Private Information also exists. In 2021, the data brokering industry was worth roughly $200 billion.[21] 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.[22,23] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[24] 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.[25]

68. Consumers also recognize the value of their personal information and offer it in exchange for goods and services. The value of Private Information 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 able to use it and control the use of it. For example, Plaintiffs and Class Members were only to obtain services from Defendant or Defendant's clients after providing their Private Information. A consumer's ability to use their Private Information is encumbered when their identity or credit profile is infected by misuse or fraud. For example, a consumer with

---

[20] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[21] https://www.latimes.com/business/story/2019-11-05/column-data-brokers

[22] https://datacoup.com/

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

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

[25] How To Sell Your Own Data And Why You May Want to, available at https://www.mic.com/impact/selling-personal-data-streamlytics (last accessed August 7, 2023).

false or conflicting information on their credit report may be denied credit. In this sense, among others, the theft of Private Information in the Data Breach led to a diminution in value of the Private Information.

69. 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.

Plaintiffs' and Class Members' Damages

70. Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach. All Plaintiffs and Class Members have suffered losses of time, invasions of privacy, and the diminished value of their Private Information.

71. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been forced to spend time dealing with the effects of the Data Breach. For example, the notification letters to Plaintiffs and Class Members stated, "We encourage you to remain vigilant against identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors." Plaintiffs and Class Members will also spend significant time:

a. Reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. Contacting financial institutions and closing or modifying financial accounts; and,

f. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

72. Plaintiffs and Class Members have incurred or will incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

73. Plaintiffs and Class Members all suffered injury from the loss of the benefit of their bargain. Specifically, Plaintiffs and Class Members provided their Private Information to Defendant or Defendant's clients with the understanding that their Private Information would be reasonably safeguarded from foreseeable threats, and that they would be notified within a reasonable amount of time if their Private Information was obtained by a third-party without authorization. Yet, this information was maintained in a negligent or reckless manner, and Defendant then waited almost two years to notify Plaintiffs and Class Members that their Private Information was compromised.

74. Plaintiffs and Class Members have also suffered fear, stress, and anxiety that is proportional to the risk of harm they face and the invasions of privacy that they have suffered.

75. Moreover, Plaintiffs and Class Members have a continuing interest in ensuring that their Private 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 password protected.

Plaintiff Mark Hendrix's Experience

76. Plaintiff Hendrix greatly values his privacy and is very careful with his Private Information. Plaintiff Hendrix stores any documents containing Private Information in a safe and secure location or destroys such documents when they are no longer needed. Plaintiffs Hendrix has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Moreover, Plaintiff Hendrix diligently chooses unique usernames and passwords for his various online accounts. When Plaintiff Hendrix does entrust a third-party with his Private Information, it is only because he understands such information will be reasonably safeguarded from foreseeable threats, and that he will be timely notified if his data is exposed.

77. Upon information and belief, Plaintiff Hendrix provided his sensitive Private Information to his current and former employer and/or healthcare network who was one of Defendant's clients and did so with the understanding that his Private Information would be safeguarded from foreseeable threats.

78. Plaintiff Hendrix received a letter dated June 7, 2023 from Defendant notifying him of the Data Breach. The letter advised that unauthorized third parties accessed and acquired files containing Private Information that were stored on Defendant's computer systems. The letter further advised Plaintiff Hendrix that his name and Social Security number were identified in files that may have been "accessed and/or acquired by an unauthorized actor."

79. As a result of the Data Breach, Plaintiff Hendrix will face a substantial risk of imminent harm for the rest of his life. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Hendrix faces, the letter offered Plaintiff Hendrix a 12-month subscription to credit monitoring services. The letter further instructed Plaintiff Hendrix "to remain vigilant against identity theft and fraud . . . ."

80. As a result of the Data Breach, Plaintiff Hendrix has spent approximately 20 hours researching the Data Breach, verifying the legitimacy of the notice letter, signing up for the credit monitoring service, reviewing his bank accounts, monitoring his credit report, changing her passwords and payment account numbers, contacting his bank to address fraudulent charges and replace his debit card, and other necessary mitigation efforts. This is valuable time Plaintiff Hendrix spent at Defendant's direction and that he otherwise would have spent on other activities, including but not limited to work and/or recreation. These losses of time will continue into the future for years to come.

81. Plaintiff Hendrix has also suffered several instances of fraud since the Data Breach. Between the date of the Data Breach and the filing of this Consolidated Complaint, Plaintiff Hendrix has had money stolen out of his checking account on more than five occasions. Although the money is eventually reimbursed, every time this happens, Plaintiff Hendrix is without access to his funds for days at a time. Moreover, each time money is stolen, Plaintiff Hendrix's debit card must be cancelled and reissued. The first time, Plaintiff Hendrix's bank replaced his debit card for free. However, the last four times, Plaintiff Hendrix has been charged a $5 fee to replace his card (total of $20). Upon information and belief, threat actors are able to use the information stolen in the Data Breach, combined with other publicly available information, to bypass bank security protocols and access Plaintiff Hendrix's funds.

82. The Data Breach also caused Plaintiff Hendrix to suffer a loss of privacy.

83. Plaintiff Hendrix anticipates spending additional considerable time and money on an ongoing basis to try to mitigate and address the present and impending injuries caused by the Data Breach.

84. The substantial risk of harm and loss of privacy from the Data Breach has caused

Plaintiff Hendrix to suffer fear, anxiety, stress, inconvenience, and nuisance.

85. The Data Breach caused Plaintiff Hendrix to suffer a diminution in the value of his Private Information.

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

Plaintiff Kaitlyn Thiel's Experience

87. Plaintiff Thiel greatly values her privacy and is very careful with her Private Information. Plaintiff Thiel stores any documents containing Private Information in a safe and secure location or destroys such documents when they are no longer needed. Plaintiff Thiel has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Moreover, Plaintiff Thiel diligently chooses unique usernames and passwords for her various online accounts. When Plaintiff Thiel does entrust a third-party with her Private Information, it is only because she understands such information will be reasonably safeguarded from foreseeable threats, and that she will be timely notified if her data is exposed.

88. For example, Plaintiff Thiel provided her sensitive Private Information to Defendant as a condition of her employment at Defendant and did so with the understanding that Defendant would safeguard it from unauthorized disclosure. Plaintiff Thiel first became an employee of Defendant's in or around 2017. Upon information and belief, Defendant used her Private Information when providing her with employment.

89. Plaintiff Thiel received a letter dated June 7, 2023 from Defendant notifying her of the Data Breach. The letter advised that unauthorized third parties accessed Defendant's network. The letter further advised that Plaintiff Thiel's Private Information—including her name and

Social Security number—was compromised in the Data Breach.

90. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Thiel faces, the letter offered Plaintiff Thiel a subscription to credit monitoring services for a period of no longer than 24 months. The letter further instructed Plaintiff Thiel to "remain vigilant by reviewing your account statements and credit reports closely." The letter additionally encouraged Plaintiff Thiel to consider implementing the protective measures detailed in the "Steps You Can Take to Protect Your Personal Information" section of the letter.

91. As a result of the Data Breach, Plaintiff Thiel has spent approximately 20 hours on activities including, but not limited to: signing up for credit monitoring and identity theft insurance, contacting credit bureaus to place freezes on her accounts, securing her online accounts, contacting banks to secure her financial accounts, contacting third parties to resolve the fraud and identity theft that she experienced, closing accounts that were compromised by identity thieves, and other necessary mitigation efforts. This is valuable time Plaintiff Thiel spent at Defendant's direction and that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

92. As a result of the Data Breach, Plaintiff Thiel suffered actual injury in the form of experiencing fraudulent charges to her Chase account in or about February 2023.

93. As a result of the Data Breach, Plaintiff Thiel suffered actual injury in the form of having a Chase credit card fraudulently opened under her name in or about February 2023.

94. As a result of the Data Breach, Plaintiff Thiel suffered actual injury in the form of having another Chase credit card fraudulently opened under her name in or about July 2023.

95. As a result of the Data Breach, Plaintiff Thiel suffered actual injury in the form of a fraudulent investment account at Ally Bank being opened under her name in or about February

2023.

96. As a result of the Data Breach, Plaintiff Thiel suffered actual injury in the form of an identity thief accessing her account at Huntington, a car loan service company.

97. As a result of the Data Breach, Plaintiff Thiel suffered actual injury in the form of her PII being disseminated on the dark web, according to Norton.

98. As a result of the Data Breach, Plaintiff Thiel suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails.

99. As a result of the Data Breach, Plaintiff Thiel suffered actual injury in the form of out-of-pocket expenses spent in response to the Data Breach, including a $25/month subscription to LifeLock for credit and identity theft monitoring services since in or about February 2023.

100. The Data Breach also caused Plaintiff Thiel to suffer a loss of privacy.

101. As a result of the Data Breach, Plaintiff Thiel will face a substantial risk of imminent harm for the rest of her life.

102. Plaintiff Thiel anticipates spending additional considerable time and money on an ongoing basis to try to mitigate and address the present and impending injuries caused by the Data Breach.

103. The substantial risk of harm and loss of privacy from the Data Breach has caused Plaintiff Thiel to suffer fear, anxiety, annoyance, inconvenience, and nuisance.

104. The Data Breach caused Plaintiff Thiel to suffer a diminution in the value of her Private Information.

105. Plaintiff Thiel has a continuing interest in ensuring that her Private Information, which upon information and belief, remains in Defendant’s possession, is protected and safeguarded from future breaches.

106. As a result of the Data Breach, Plaintiff has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff's Private Information being placed in the hands of cyber criminals; (c) damages to and diminution in value of Plaintiff's Private Information that was entrusted to Defendant with the understanding that Defendant would safeguard this information against disclosure; (d) loss of the benefit of the bargain she made with Defendant by overpaying for services that were intended to be accompanied by adequate data security but were not; (e) loss of time and effort that Plaintiff Thiel has had to expend in an attempt to ameliorate, mitigate, and address the consequences of the Data Breach, with such steps being taken at the direction of Defendant; and (f) continued risk to Plaintiff's Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

CLASS ACTION ALLEGATIONS

107. Plaintiffs bring this nationwide class action on behalf of themselves and all others similarly situated under Rules 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

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

> **All persons Defendant identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach.**

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

110. Plaintiffs reserve the right to amend or modify the Class definition and/or create additional subclasses as this case progresses.

111. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, the Class consists of more than 27,000 current and former clients and/or employees of Defendant whose sensitive data was compromised in Data Breach.

112. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;

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

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

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

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

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

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

h. Whether Defendant should have discovered the Data Breach sooner;

i. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

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

l. Whether Defendant breached a fiduciary duty to Plaintiffs and Class Members;

m. Whether Defendant violated the consumer protection statute invoked below;

n. Whether Defendant breach implied or express contracts with Plaintiffs and Class Members;

o. Whether Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiffs and Class Members;

p. Whether Defendant failed to provide notice of the Data Breach in a timely manner, and;

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

113. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' information, like that of every other Class Member, was compromised in the Data Breach.

114. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs' Counsel are competent and experienced in litigating data privacy class actions.

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

116. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

117. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

COUNT I
NEGLIGENCE
(On behalf of Plaintiffs and the Class)

118. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

119. As a condition of receiving employment or the services of Defendant or its clients, Plaintiffs and the Class were obligated to provide Defendant with their Private Information.

120. Plaintiffs and the Class entrusted their Private Information to Defendant on the premise and with the understanding that Defendant would exercise reasonable care in the protection of their Private Information.

121. 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.

122. 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.

123. Defendant 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. This duty includes, among other things, configuring, maintaining, and testing Defendant's security protocols to ensure that the Private Information of Plaintiffs and the Class in Defendant's possession was adequately secured and protected.

124. Defendant also had a duty to exercise appropriate clearinghouse practices to remove job applicants' Private Information it was no longer required to retain pursuant to regulations.

125. Defendant had a duty to properly train employees to recognize phishing attempts and other common data security risks.

126. 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 Nationwide Class.

127. Defendant's duty to use reasonable security measures arose as a result of the foreseeable harm that would occur due to its failure to exercise reasonable care.

128. Defendant was subject to an independent duty untethered to any contract between Defendant and Plaintiffs or the Class.

129. 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.

130. 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 Nationwide Class, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information.

131. Defendant's own conduct created a foreseeable risk of harm to Plaintiffs and the Nationwide Class. Defendant's misconduct included, but was not limited to, its failure to encrypt the data stored on its system or to implement other reasonable industry standard measures to safeguard Private Information.

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

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

134. 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 Information by third parties.

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

136. 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.

137. 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.

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

139. Defendant breached its duty to adequately train employees to recognize and avoid phishing attempts and other basic cybersecurity risks.

140. 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.

141. Defendant breached its duty to safeguard Plaintiffs' and Class Members' Private Information by failing to retain such information in an encrypted form.

142. Defendant breached its duty to safeguard Plaintiffs' and Class Members' Private Information by retaining the information for many years regardless of whether it was necessary to do so.

143. 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.

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

145. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of

productivity addressing and attempting to mitigate the present and continuing consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remain 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 of Plaintiffs and the Class; and (viii) present and continuing costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Nationwide Class.

146. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Nationwide 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.

147. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiffs and the Nationwide 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.

148. 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
NEGLIGENCE *PER SE*
(On behalf of Plaintiffs and the Class)

149. Plaintiffs repeat and re-allege each and every allegation contained the Complaint as if fully set forth herein.

150. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant's, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

151. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored, and the foreseeable consequences of the Data Breach for companies of Defendant's magnitude, including, specifically, the immense damages that would result to Plaintiffs and Members of the Class due to the valuable nature of the Private Information at issue in this case—including Social Security numbers.

152. Defendant's violations of Section 5 of the FTC Act constitute negligence *per se*.

153. Plaintiffs and members of the Class are within the class of persons that the FTC Act was intended to protect.

154. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and members of the Class.

155. As a direct and proximate result of Defendant's negligence per se, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their 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 of its current and former employees and customers in its continued possession; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

156. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and Class Members 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.

COUNT III
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiffs and the Class)

157. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

158. Defendant required Plaintiffs and Class Members to provide their Private Information as a condition of receiving its services or employment. In so doing, Plaintiffs and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and the Nationwide Class if their data had been breached and compromised or stolen.

159. Plaintiffs and the Class fully performed their obligations under the implied contracts with Defendant.

160. Defendant breached the implied contracts it made with Plaintiffs and the Class by (i) failing to implement technical, administrative, and physical security measures to protect the Private Information from unauthorized access or disclosure and improper (such as encryption of Social Security numbers) despite such measures being readily available, (ii) failing to limit access to the Private Information to Defendant's employees who needed such information to perform a specific job, (iii) failing to store the Private Information only on servers kept in a secure, restricted access area, and (iv) otherwise failing to safeguard the Private Information.

161. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and

economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

162. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT IV
BREACH OF FIDUCIARY DUTY
(On behalf of Plaintiffs and the Class)

163. Plaintiffs repeat and re-allege each and every allegation contained the Complaint as if fully set forth herein.

164. Plaintiff Hendrix and Defendant established a special relationship by virtue of Defendant accepting his Private Information in the ordinary course of providing its services to his employer and/or healthcare network. By accepting and storing Plaintiff Hendrix's Private Information in the course of providing legal services and the scope of that relationship, Defendant accepted the duty to safeguard his Private Information.

165. Plaintiff Thiel and Defendant established a special relationship by virtue of (1) Defendant accepting her Private Information and (2) Defendant maintaining her Private Information for at least three years after her employment ended with Defendant. By accepting and continuing to store Plaintiff Thiel's Private Information after her employment ended, Defendant accepted the duty as a fiduciary to safeguard her Private Information.

166. In light of the special relationship between Defendant and Plaintiffs and Class Members, whereby Defendant became guardians of Plaintiffs' and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its customers, including Plaintiffs and Class Members, as follows: (1) for the safeguarding of Plaintiffs' and Class Members' Private Information; (2) to timely notify Plaintiffs and Class Members of a data breach and disclosure; and (3) to maintain complete and accurate records of what customer information (and where) Defendant did and does store.

167. Defendant had a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of this relationship, in particular, to keep secure the Private Information of its customers.

168. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period of time.

169. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiffs' and Class Members' Private Information.

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

171. Defendant breached its fiduciary duties to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' Private Information.

172. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class Members have suffered and will 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 its 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 Plaintiff and Class Members; and (vii) the diminished value of Defendant's services they received.

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

COUNT V
UNJUST ENRICHMENT
(On behalf of Plaintiffs and the Class)

174. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

175. This claim is brought in the alternative to any claim for breach of contractual obligations.

176. Defendant benefited from receiving Plaintiffs' and Class Members' Private Information by its ability to retain and use that information for its own benefit. Defendant understood this benefit.

177. Defendant also understood and appreciated that Plaintiffs' and Class Members' Private Information was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that information.

178. Defendant was also enriched by the fees it was paid for its services which, in part, should have been used for adequate data security.

179. Plaintiffs and Class Members were required to provide Defendant or Defendant's clients with their Private Information. In exchange, Plaintiffs and Class Members should have received adequate protection and data security for such Private Information held by Defendant.

180. Defendant knew Plaintiffs and Class Members conferred a benefit, which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

181. Defendant failed to provide reasonable security, safeguards, and protections to the Private Information of Plaintiffs and Class Members.

182. Under the principles of equity and good conscience, Defendant should not be permitted to retain money or the value of benefits belonging to Plaintiffs and Class members, because Defendant failed to implement appropriate data management and security measures mandated by industry standard.

183. Defendant wrongfully accepted and retained these benefits to the detriment of Plaintiffs and Class Members.

184. Defendant's enrichment at the expense of Plaintiffs and Class Members is and was unjust.

185. As a result of Defendant's wrongful conduct, as alleged above, Plaintiffs and Class Members are entitled to restitution and disgorgement of all profits, benefits, and other compensation obtained by Defendant, plus attorneys' fees, costs, and interest thereon.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs Mark Hendrix and Kaitlyn Thiel pray for judgment as follows:

a) For an Order certifying this action as a Class action and appointing Plaintiffs as Class Representatives and their counsel as Class Counsel;

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

c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII and PHI compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e) Ordering Defendant to pay for lifetime credit monitoring services for Plaintiffs and the Class;

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

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

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

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

j) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury on all claims so triable.

Dated: August 21, 2023

Respectfully Submitted,

/s/ Phil Krzeski
Philip J. Krzeski (0095713)
Bryan L. Bleichner (*pro hac vice* forthcoming)
CHESTNUT CAMBRONNE PA
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Phone: (612) 339-7300
Fax: (612) 336-2940
bbliechner@chestnutcambronne.com
pkrzeski@chestnutcambronne.com

Terence R. Coates (0085579)
Dylan J. Gould (0097954)
MARKOVITS, STOCK & DEMARCO, LLC
119 East Court Street, Suite 530
Cincinnati, OH 45202
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
dgould@msdlegal.com

Gary M. Klinger (*admitted*)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606

Telephone: (202) 429-2290
gklinger@milberg.com

Attorneys for Plaintiffs and the Proposed Class

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on August 21, 2023, the foregoing was filed electronically. Notice of this filing will be sent to all parties by operation of the Court's electronic filing system. Parties may access this filing through the Court's system.

/s/ Phil Krzeski
Philip J. Krzeski (00095713)

ClassAction.org
