UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN

Kati Komorosky individually and on behalf of all others similarly situated, Plaintiff, v. McLaren Health Care Corporation, Defendant.	Case No.: _____ **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Kati Komorosky ("Plaintiff") brings this Class Action Complaint ("Complaint") against McLaren Health Care Corporation ("McLaren" or "Defendant"), as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to her own actions and her counsels' investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This class action arises out of the recent ransomware attack and data breach ("Data Breach") resulting from Defendant's failure to implement reasonable and industry standard data security practices.

2. Defendant detected suspicious activity in its IT systems in late August, and later confirmed that its network was subject to a ransomware attack that may affect up to 2.5 million patients (the "Data Breach"). [1]

[1] https://www.hipaajournal.com/mclaren-health-care-ransomware-attack-may-

3. In late September, the ALPHV/BlackCat ransomware group claimed responsibility for the attack and added McLaren Health Care to its dark web data leak site. ALPHV is a spin-off of the now-defunct Conti ransomware group and has a history of attacking healthcare organizations. The group claims to have exfiltrated more than 6 terabytes of data in the attack and says the stolen data includes the sensitive information of 2.5 million patients ("Private Information" or "PHI and PII"). While McLaren Health Care says all its systems are back online, ALPHV claims to still have access to McLaren Health Care's systems through an active backdoor. [2]

4. By obtaining, collecting, using, and deriving a benefit from the Private Information of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

5. This Complaint is brought against Defendant because of its failure to properly safeguard the Private Information entrusted to it, and to remedy the harms suffered by plaintiff and those similarly situated caused by this failure.

6. Despite its duties to Plaintiff and Class Members to secure and safeguard the PII entrusted to it, Defendant stored this Private Information on a

affect-up-to-2-5-million-patients/ (last visited October 5, 2023).

[2] *Id.*

database that was negligently and/or recklessly configured. Defendant failed to adequately protect Plaintiff's and Class Members' Private Information and failed to encrypt or redact this highly sensitive information. This unencrypted, unredacted Private Information was compromised due to Defendant's negligence.

7. Defendant maintained the Private Information in a negligent manner. Foreseeably, cybercriminals exploited these vulnerabilities, accessed and exfiltrated Plaintiff's and Class Members' Private Information.

8. Hackers targeted and obtained Plaintiff's and Class Members' Private Information because of its value in exploiting and stealing the identities of Plaintiff and Class Members.

9. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

10. As a result of the Data Breach, Plaintiff and Class Members suffered ascertainable losses, including but not limited to, a loss of privacy, the loss of the benefit of their bargain, out-of-pocket monetary losses and expenses, the value of their time reasonably incurred to remedy or mitigate the effects of the attack, the diminished value of their Private Information, and the substantial and imminent risk of identity theft. Given the theft of information that is largely static—like Social Security numbers—this risk will remain with Plaintiff and Class Members for the rest of their lives.

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

PARTIES

12. Plaintiff, Kati Komorosky, is a natural person and citizen of Michigan, where she intends to remain. Upon information and belief, Plaintiff's PII and/or PHI was compromised in the Data Breach.

13. Defendant, McLaren Health Care Corporation, is a non-profit corporation organized under the state laws of Michigan with its principal place of business located in Grand Blanc, Michigan.

JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

15. This Court has personal jurisdiction over Defendant because its principal place of business is in this District, it regularly conducts business in

Michigan, and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

16. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant's principal place of business is in this District.

FACTUAL ALLEGATIONS

Background

17. In late August, Defendant detected suspicious activity on its IT System. Upon investigation, Defendant confirmed it was subject to a ransomware attack by the ALPHV/Blackcat ransomware group.

18. The attacker accessed and acquired files in Defendant's computer systems containing unencrypted Private Information of Plaintiff and Class Members.

19. Upon information and belief, the Private including Plaintiffs' names, Social Security number, and protected health information.

20. In the ordinary course of serving its patients, Defendant stores, maintains, and uses Plaintiff's and Class Members' Private Information. The information held by Defendant in its computer systems included the unencrypted Private Information of Plaintiff and Class Members.

21. Defendant agreed to and undertook legal duties to maintain the Private Information of Plaintiff and Class Members safely, confidentially, and in compliance with all applicable laws.

22. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

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

24. Upon information and belief, Defendant made promises and representations to its customers, including Plaintiff and Class Members, that the Private Information collected from them and entrusted would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

25. Plaintiff and Class Members directly or indirectly entrusted Defendant with sensitive and confidential information, including their Private Information which includes information that is static, meaning it does not change, and can be used to commit myriad financial crimes.

26. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties.

27. Defendant had obligations created by FTC Act, the Gramm-Leach-Bliley Act, contract, industry standards, and representations made to Plaintiff and

Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

28. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class Members' Private Information. Without the required submission of Private Information, Defendant could not perform the services they provide.

29. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible to protect Plaintiff's and Class Members' Private Information from unauthorized disclosure, and that such an attempt to obtain said information was foreseeable.

30. Because Defendant failed to properly protect and safeguard Plaintiff's and Class Members' PII, an unauthorized third party was able to access Defendant's database, and then access and exfiltrate Plaintiff's and Class Members' Private Information stored on Defendant's database.

31. Plaintiff further believes his Private Information, and that of Class Members, was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

32. Plaintiff and Class Members are current and former patients of Defendant.

33. Upon information and belief, in the course of collecting Private Information from patients, including Plaintiff, Defendant promised to provide confidentiality and adequate security for patient data through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

34. In the course of their patient-physician relationship, patients, including Plaintiff and Class Members, provided Defendant with at least their Private Information.

35. Plaintiff and Class Members, as former and current patients of Defendant, relied on these promises and on this sophisticated business entity to keep their sensitive Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Patients, in general, demand security to safeguard their Private Information, especially when PHI and other sensitive Private Information is involved.

The Data Breach

36. In late August, McLaren "detected 'suspicious activity' on its computer network, immediately launched an investigation into the source of the disruption,

and retained outside global cybersecurity specialists to assist[.]"[3]

37. As a result of its investigation, Defendant "determined that [McLaren] did experienced a ransomware event."[4]

38. On or about September 29, 2023, Alphv cybercrime gang, also known as BlackCat, took credit for the ransomware attack and further claimed "to have stolen 6 terabytes of data on 2.5 million patients[.]"[5]

39. A ransomware attack, like that experienced by Defendant is a type of cyberattack that is frequently used to target companies due to the sensitive patient data they maintain.[6] 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]

40. 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

---

[3] https://www.databreachtoday.com/group-claims-stole-25-million-patients-data-in-attack-a-23212 (last accessed Oct. 5, 2023).

[4] *Id.*

[5] *Id.*

[6] *Ransomware warning: Now attacks are stealing data as well as encrypting it*, available at https://www.zdnet.com/article/ransomware-warning-now-attacks-are-stealing-data-as-well-as-encrypting-it/

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

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."

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

---

[8] *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/

[9] *2020 Ransomware Marketplace Report, available at https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report*

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

[11] *Id.*

[12] *Id.*

42. Upon information and belief, the cyberattack was targeted at Defendant, due to its status as a healthcare entity that collects, creates, and maintains Private Information on its computer networks and/or systems.

43. Uon information and belief, Plaintiff's and Class Members' Private Information was compromised and acquired in the Data Breach.

44. The files containing Plaintiff's and Class Members' Private Information, that were targeted and stolen from Defendant, included their PII and/or PHI.

45. Because of this targeted cyberattack, data thieves were able to gain access to and obtain data from Defendant that included the Private Information of Plaintiff and Class Members.

46. As evidenced by the Data Breach's occurrence, the Private Information contained in Defendant's network was not encrypted. Had the information been properly encrypted, the data thieves would have exfiltrated only unintelligible data.

47. Plaintiff further believes that her Private Information and that of Class Members was or soon will be published to the dark web, where it will be available to purchase, because that is the *modus operandi* of cybercriminals.

48. Defendant had obligations created by the FTC Act, HIPAA, contract, state and federal law, common law, and industry standards to keep Plaintiff's and

Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

Plaintiff Kati Komorosky's Experience

49. Plaintiff is Defendant's patient and has sought medical care from Defendant in several instances.

50. Plaintiff is very careful about sharing her Private Information. Plaintiff has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff stores any documents containing her sensitive PII in a safe and secure location or destroys the documents. Moreover, Plaintiff diligently chooses unique usernames and passwords for her various online accounts.

51. Plaintiff only allowed Defendant to maintain, store, and use her Private Information because she believed that Defendant would use basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendant at the time of the Data Breach.

52. Plaintiff suffered injury from a loss of privacy the moment that her Private Information was accessed and exfiltrated by a third party without authorization.

53. Plaintiff has also suffered injury in the form of damages to and diminution in the value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendant.

54. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of criminals.

55. This risk from the Data Breach has caused Plaintiff to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

56. The substantial risk of imminent harm and loss of privacy have caused Plaintiff to suffer stress, fear, and anxiety.

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

Value of Private Information

58. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person

without authority."[13] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[14]

59. The Private Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[15] Experian reports that a stolen credit or debit card

[13] 17 C.F.R. § 248.201 (2013)

[14] *Id.*

[15] *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 Mar. 25, 2023).

number can sell for $5 to $110 on the dark web.[16] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[17]

60. For example, Social Security numbers are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiff and some Class Members, 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.[18]

---

[16] *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 Mar. 25, 2023).

[17] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/ anonymous-browsing/in-the-dark/ (last accessed Mar. 25, 2023).

[18] Social Security Administration, *Identity Theft and Your Social Security Number, available at:* https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited May 17, 2023).

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

62. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link 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."[19]

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.

64. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to

[19] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at:* https://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited May 17, 2023).

credit card information, personally identifiable information … [is] worth more than 10x on the black market."[20]

65. Moreover, there may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[21]

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

---

[20] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/ article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Mar. 25, 2023).

[21] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last accessed Aug. 23, 2021).

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

68. Defendant were, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

69. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members.

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

71. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

72. Plaintiff and the Class Members relied on Defendant to implement and follow adequate data security policies and protocols, to keep their Private Information confidential and securely maintained, to use such Private Information

solely for business and health care purposes, and to prevent the unauthorized disclosures of the Private Information.

The Data Breach was Foreseeable and Preventable

73. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[22]

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

75. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed.[23] In 2022, there was a 41.5% increase in the number of victims impacted.[24] Of the 1,862 recorded data breaches in 2021, 330 of them, or 17.7% were in the medical or healthcare industry.

---

[22] *See* How to Protect Your Networks from RANSOMWARE, at 3, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last accessed May 17, 2023).

[23] See *Identity Theft Resource Center's 2021 Annual Data Breach Report Sets New Record for Number of Compromises*, https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/?utm_source=press+release&utm_medium=website&utm_campaign=2022+Annual+Data+Breach+Report.

[24] *Identity Theft Resource Center's 2022 Annual Data Breach Report Reveals Near-Record Number of Compromises*, https://www.idtheftcenter.org/post/2022-annual-data-breach-report-reveals-near-record-number-compromises/

The 330 reported breaches in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.

76. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack.[25]

77. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year. [26]

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

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

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks ....
- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender

[25] FBI, Secret Service Warn of Targeted, Law360 (Nov.18,2019), https://www.law360.com/articles/1220974/fbisecret-service-warn-of-targeted-ransomware.

appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net) ....

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it ....

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters-and keep them updated-to reduce malicious network traffic ....[27]

[27] *See* ST 19-001:Protecting Against Ransomware (original release date Apr. 11, 2019), *available at https://readiness255.rssing.com/chan-9268821/all_p83.html*

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

- **Secure internet-facing assets**
  - Apply latest security updates
  - Use threat and vulnerability management
  - Perform regular audit; remove privileged credentials;
- **Thoroughly investigate and remediate alerts**
  - Prioritize and treat commodity malware infections as potential full compromise;
- **Include IT Pros in security discussions**
  - Ensure collaboration among (security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;
- **Build credential hygiene**
  - Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;
- **Apply principle of least-privilege**
  - Monitor for adversarial activities
  - Hunt for brute force attempts
  - Monitor for cleanup of Event Logs
  - Analyze logon events;
- **Harden infrastructure**
  - Use Windows Defender Firewall
  - Enable tamper protection
  - Enable cloud-delivered protection

- Tum on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[28]

Defendant Acquires, Collects, And Stores Plaintiff's the Class's PII.

81. As a condition to open an account or otherwise obtain financial services from Defendant, Plaintiff and Class Members were required to give their sensitive and confidential PII to Defendant.

82. Defendant retains and stores this information and derives a substantial economic benefit from the Private Information that they collect. But for the collection of Plaintiff's and Class Members' Private Information, Defendant would be unable to perform its services.

83. By obtaining, collecting, and storing the Private Information of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that they were responsible for protecting the Private Information from disclosure.

84. As a custodian of Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiff and Class members, and of the foreseeable consequences if its data security

[28] *Human-operated ransomware attacks: A preventable disaster,* https://www.microsoft.com/ en-us/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster

systems were breached, including the significant costs imposed on Plaintiff and Class Members as a result of a breach.

Defendant Failed to Properly Protect Plaintiff's and Class Members' Private Information

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

86. Defendant's negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to companies like Defendant to protect and secure sensitive data they possess.

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

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

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Configure firewalls to block access to known malicious IP addresses.

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[29]

Defendant Failed to Comply with FTC Guidelines

[29] *See* How to Protect Your Networks from RANSOMWARE, at 3, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Aug. 23, 2021).

89. 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.

90. 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 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.[30]

91. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

[30] 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.

92. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect personally identifiable 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 ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions clarify the measures businesses take to meet their data security obligations.

93. Defendant failed to properly implement basic data security practices, such as making a database storing Private Information available to the public without the use of a password or multifactor authentication.

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

95. Defendant were always fully aware of their obligation to protect the PII of Plaintiff and Class members. Defendant were also aware of the significant repercussions that would result from their failure to do so.

Defendant failed to Comply with Industry Standards

96. As shown above, experts studying cyber security routinely identify companies in the finance industry as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

97. Several best practices have been identified that at a minimum should be implemented by service providers like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and antimalware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

98. 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.

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

As a Result of Defendant's Failure to Safeguard Private Information, Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft and Have Experienced Substantial Harm.

100. Plaintiff and Class Members have suffered injury from the access to, and misuse of, their PII that can be directly traced to Defendant.

101. The ramifications of Defendant's failure to keep Plaintiff's and the Class's Private Information secure are severe.

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

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

b. The diminution in value of their Private Information;

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

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

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

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen Private Information; and

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

103. One such example of criminals using Private Information for profit, to the detriment of Plaintiff and the Class Members, is the development of "Fullz" packages.

104. 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. These dossiers are known as "Fullz" packages.

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

and other members of the proposed Class's stolen Private Information is being misused, and that such misuse is fairly traceable to the Data Breach.

106. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.[31]

107. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." Defendant did not rapidly report to Plaintiff and the Class that their Private Information had been stolen, and in fact did not notify Plaintiff for five months.[32]

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

109. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by the theft of their Private Information. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor

[31] Available at 2019_IC3Report.pdf (last accessed Apr. 4, 2023).

[32] *Id.*

their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

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

111. According to the FTC, unauthorized Private Information disclosures are extremely damaging to consumers' finances, credit history and reputation, and can take time, money and patience to resolve the fallout. [33] The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act.

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

Plaintiff's and Class Members' Damages

[33] *See* Taking Charge, What to Do If Your Identity is Stolen, FTC, at 3 (2012), https://www.ojp.gov/ncjrs/virtual-library/abstracts/taking-charge-what-do-if-your-identity-stolen (last visited October 10, 2022).

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

114. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

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

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

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

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

119. Defendant's delay in noticing affected persons of the theft of their Private Information prevented early mitigation efforts and compounded the harm.

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

a. Reviewing and monitoring financial and other 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 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, bank accounts, and credit reports for unauthorized activity for years to come.

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

CLASS ALLEGATIONS

122. Plaintiff brings this nationwide class action on behalf of herself and on behalf of others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

123. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

> All persons whose Private Information was actually or potentially accessed or acquired by an unauthorized party as a result of the Data Breach (the "Class").

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

125. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

126. Numerosity, Fed R. Civ. P. 23(a)(1): Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are

certainly tens of thousands, and probably at least more than 2,500,000 individuals whose Private Information was improperly accessed in the Data Breach, and each Class is apparently identifiable within Defendant's records.

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

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

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

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

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

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

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

g. 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;

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

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

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

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

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

129. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant have acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

130. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. Plaintiff has also retained counsel

experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

131. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

132. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the

costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

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

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

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

136. Further, Defendant have acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding

declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

137. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

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

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

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

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

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

g. 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; and

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

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Putative Rule 23 Class)

138. Plaintiff and the Class repeat and re-allege each allegation as if fully set forth herein.

139. Plaintiff and the Class entrusted Defendant with their Private Information.

140. Plaintiff and the Class entrusted their Private Information to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their information for business purposes only, and/or not disclose their Private Information to unauthorized third parties.

141. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and the Class could and would suffer if the Private Information were wrongfully disclosed.

142. 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 Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

143. By accepting, storing, and maintaining Plaintiff's and Class Members' Private Information, Defendant undertook a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised,

lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the Private Information of Plaintiff and the Class Members in Defendant's possession was adequately secured and protected.

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

145. By accepting, storing, and maintaining Plaintiff's and Class Members' Private Information, Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the Private Information of Plaintiff and the Class.

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

147. Defendant were subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

148. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, due to the nature of Defendant's industry, and particularly in light of Defendant's inadequate security practices.

149. Plaintiff 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 Plaintiff and the Class, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendant's systems.

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

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

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

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

154. Defendant were in the best position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

155. Defendant had and continues to have a duty to adequately disclose that the Private Information of Plaintiff 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 Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Info by third parties.

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

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

158. Defendant, through their actions and/or omissions, unlawfully breached their duties to Plaintiff and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the Private Information of Plaintiff and the Class during the time the Private Information was within Defendant's possession or control.

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

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

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

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

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

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

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

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

167. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to, the following: (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 remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the Private Information of Plaintiff 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 Plaintiff and the Class.

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

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

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

COUNT II
NEGLIGENCE PER SE
(On behalf of Plaintiff and the Putative Rule 23 Class)

171. Plaintiff and the Class repeat and re-allege each allegation in the Complaint as if fully set forth herein.

172. 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, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

173. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

174. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

175. Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect.

176. 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 their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

177. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff 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 PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (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 PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiff 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 PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class.

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

179. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the PII in their continued possession.

180. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT III
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the Putative Rule 23 Class)

181. Plaintiff and the Class repeat and re-allege each allegation in the Complaint as if fully set forth herein.

182. Plaintiff and Class Members were required to provide Defendant with their Private Information as a condition of their employment.

183. By Plaintiff and Class Members providing their Private Information, and by Defendant accepting this Private Information, the parties mutually assented to implied contracts. These implied contracts included an implicit agreement and understanding that (1) Defendant would adequately safeguard Plaintiff's and Class Members' Private Information from foreseeable threats, (2) that Defendant would delete the information of Plaintiff and Class Members once it no longer had a legitimate need; and (3) that Defendant would provide Plaintiff and Class Members with notice within a reasonable amount of time after suffering a data breach.

184. On information and belief, at all relevant times Defendant promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiff and Class Members that it would only disclose Private Information under certain circumstances, none of which relate to the Data Breach.

185. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiff's and Class Members' Private Information would remain protected.

186. Defendant provided consideration by providing services, while Plaintiff and Class Members provided consideration by providing valuable property—i.e., their Private Information. Defendant benefitted from the receipt of this Private Information by increasing profit from additional business.

187. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

188. Defendant materially breached their implied contracts with Plaintiff and Class Members when it (1) placed their Private Information on an unsecured computer system that could (and later was) accessed by unauthorized and (2) waited an unreasonably long time to notify them of the Data Breach. It is common sense that Plaintiff and Class Members would not have provided Defendant with their Private Information had they known that Defendant would not implement basic data security measures or that it would wait several months to notify them of a data breach involving their Private Information.

189. Defendant's breaches of contract have caused Plaintiff and Class Members to suffer damages from the lost benefit of their bargain, out of pocket monetary losses and expenses, loss of time, and diminution of the value of their Private Information.

190. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff 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.

COUNT IV
UNJUST ENRICHMENT
(On behalf of Plaintiff and the Putative Rule 23 Class)

191. Plaintiff and the Class repeat and re-allege each allegation as if fully set forth herein.

192. Plaintiff and Class Members conferred a monetary benefit on Defendant, by providing Defendant with their valuable Private Information.

193. Defendant enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Private Information.

194. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid their data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

195. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

196. Defendant acquired the monetary benefit and PII through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

197. If Plaintiff and Class Members knew that Defendant had not secured their Private Information, they would not have agreed to provide their Private Information to Defendant.

198. Plaintiff and Class Members have no adequate remedy at law.

199. As a direct and proximate result of Defendant's conduct, Plaintiff 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 PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, 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 identity theft; (vi) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect Private Information in their continued possession and (vii) 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 Plaintiff and Class Members.

200. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them.

COUNT V
DECLARATORY AND INJUNCTIVE RELIEF
(On behalf of Plaintiff and the Putative Rule 23 Class)

201. Plaintiff and the Class repeat and re-allege each allegation as if fully set forth herein.

202. Plaintiff pursues this claim under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

203. Defendant owes a duty of care to Plaintiff and Class Members that require it to adequately secure Plaintiff's and Class Members' Private Information.

204. Defendant failed to fulfill their duty of care to safeguard Plaintiff's and Class Members' Private Information.

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

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

207. Plaintiff, therefore, seeks a declaration (1) that Defendant's existing data security measures do not comply with their contractual obligations and duties of care to provide adequate data security, and (2) that to comply with their contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to, the following:

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

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

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

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

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

f. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel and employees how to safely share and maintain highly sensitive personal information, including but not limited to, Plaintiff and Class Members' Personally Identifiable Information.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Class, and appointing Plaintiff and her Counsel to represent the Class;

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

C. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

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

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

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

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

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

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

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

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

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

x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personally identifiable information, as well as protecting the personally identifiable information of Plaintiff and Class Members;

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

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

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

xiv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personally identifiable information to third parties, as well as the steps affected individuals must take to protect themselves;

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

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

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

F. For prejudgment interest on all amounts awarded; and

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

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Respectfully submitted,

Date: October 9, 2023

/s/ Bryan L. Bleichner

Bryan L. Bleichner (MN BAR #0326689)
Philip J. Krzeski (OH BAR #0095713)
CHESTNUT CAMBRONNE PA
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Telephone: (612) 339-7300
Facsimile: (612) 336-2940
bbleichner@chestnutcambronne.com
pkrzeski@chestnutcambronne.com

Terry R. Coates (OH BAR #0085579)
MARKOVITS STOCK & DEMARCO, LLC
119 E. Court Street, Suite 530
Cincinnati, OH 45202
Telephone: (513) 651-3700
tcoates@msdlegal.com

Attorneys for Plaintiff and the Class