# Exhibit A

**THE UNITED STATES DISTRICT COURT**
**FOR THE NORTHERN DISTRICT OF ILLINOIS**

| | |
|---|---|
| **IN RE ARTHUR J. GALLAGHER DATA BREACH LITIGATION**<br><br>This Document Relates To: All Actions | Master File No.: 1:21-cv-04056<br><br>Consolidated with No. 1:21-cv-04415 and No. 1:21-cv-04554 |

# CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs John Parsons, Adrian Villalobos, Christopher Caswell, Robert Davie, Peter Horning, Julia Kroll, Amanda Marr, Brent McDonald, Jonathon Mitchell, Jason Myers, John Owens, Alan Wellikoff, Chandra Wilson, Arda Yeremian, and Tracey Bock ("Plaintiffs") bring this Class Action Complaint against Arthur J. Gallagher Co. ("AJG") and Gallagher Basset Services, Inc. ("GBS") (collectively, "Defendants"), individually and on behalf of all others similarly situated ("Class Members"), and allege, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

## I. INTRODUCTION

1. Plaintiffs bring this class action against Defendants for their failure to properly secure and safeguard personally identifiable information including names; Social Security numbers or tax identification numbers; driver's license, passport or other government identification numbers; dates of birth; usernames and passwords; employee identification numbers; financial account or credit card information; and/or electronic signatures (collectively, "personally identifiable information" or "PII") as well as medical treatment, claim, diagnosis, medication or other medical information; health insurance information; medical records or account numbers; and/or biometric information ("protected health information" or "PHI").

2. According to AJG's website, it has "has grown to be one of the leading insurance

brokerage, risk management, and HR & benefits consulting companies in the world. With significant reach internationally, our organization employs over 34,000 people and our global network provides services in more than 150 countries."[1]

3. AJG's website states that its global group of companies and partners includes GBS, a "Third-Party Administrator and claims manager [that] guide[s] [its] clients to improve their claims handling processes, guard the reputation and financial interests of our clients, and go beyond expectations to accelerate resolution."[2]

4. According to its website, GBS is "the premier multiline claims service provider."[3] GBS represents that it "guide[s] those suffering a loss to the best outcomes for their futures" and "guard[s] [its] clients' names and assets with unrivalled products and service."[4]

5. From June 3, 2020 to September 26, 2020, certain segments of AJG's network, including segments at GBS, were accessed by an unknown party during a ransomware event (the "Data Breach").

6. During the Data Breach, the attacker accessed records that contained the personal information of more than three million individuals.

7. On or around September 26, 2020, Defendants finally detected the months-long ransomware event underlying the Data Breach.

8. On or around June 30, 2021, more than nine months after reports began surfacing on the Internet about the Data Breach, Defendants finally began notifying some Class Members of the Data Breach.

9. On or around June 30, 2021, more than nine months after it detected the

[1] *See* https://www.ajg.com/us/about-us/ (last visited Oct. 27, 2021).
[2] *See* https://www.ajg.com/us/about-us/gallagher-companies/ (last visited Oct. 27, 2021).
[3] *See* https://www.gallagherbassett.com/ (last visited Oct. 27, 2021).
[4] *Id.*

ransomware event underlying the Data Breach, Defendants began notifying various states' Attorneys General of the Data Breach.

10. On June 30, 2021, Defendants reported to the Maine Attorney General that the Data Breach affected 7,376 individuals.

11. On July 16, 2021, Defendants reported to the Maine Attorney General that the Data Breach affected an additional 212,721 individuals.

12. On July 21, 2021, Defendants reported to the Maine Attorney General that the Data Breach affected an additional 722,325 individuals.

13. On August 4, 2021, Defendants reported to the Maine Attorney General that the Data Breach affected an additional 6,823 individuals.

14. On August 12, 2021, Defendants reported to the Maine Attorney General that the Data Breach affected an additional 584,048 individuals.

15. On August 17, 2021, Defendants reported to the Maine Attorney General that the Data Breach affected an additional 1,140,520 individuals.

16. On September 1, 2021, Defendants reported to the Maine Attorney General that the Data Breach affected an additional 111,317 individuals.

17. On September 8, 2021, Defendants reported to the Maine Attorney General that the Data Breach affected an additional 5,577 individuals.

18. On September 13, 2021, Defendants reported to the Maine Attorney General that the Data Breach affected an additional 104,526 individuals.

19. On September 29, 2021, Defendants reported to the Maine Attorney General that the Data Breach affected an additional 813,120 individuals.

20. By obtaining, collecting, using, and deriving a benefit from the PII and PHI of

Plaintiffs and Class Members, Defendants assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. Defendants admit that the unencrypted PII and PHI impacted during the Data Breach included names; Social Security numbers or tax identification numbers; driver's license, passport or other government identification numbers; dates of birth; usernames and passwords; employee identification numbers; financial account or credit card information; and/or electronic signatures as well as medical treatment, claim, diagnosis, medication or other medical information; health insurance information; medical records or account numbers; and/or biometric information.

21. The exposed PII and PHI of Plaintiffs and Class Members can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII and PHI to criminals. Plaintiffs and Class Members now face a lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers—the gold standard for identity thieves.

22. This PII and PHI was compromised due to Defendants' negligent and/or careless acts and omissions and the failure to protect the PII and PHI of Plaintiffs and Class Members. In addition to Defendants' failure to prevent the Data Breach, after discovering the breach, Defendants waited several months to report it to the states' Attorneys General and affected individuals. Defendants have also purposefully maintained secret the specific vulnerabilities and root causes of the breach and have not informed Plaintiffs and Class Members of that information.

23. As a result of this delayed response, Plaintiffs and Class Members had no idea their PII and PHI had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

24. Plaintiffs bring this action on behalf of all persons whose PII and PHI was

compromised as a result of Defendants' failure to: (i) adequately protect the PII and PHI of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendants' inadequate information security practices; and (iii) effectively secure hardware containing protected PII and PHI using reasonable and effective security procedures free of vulnerabilities and incidents. Defendants' conduct amounts to negligence and violates federal and state statutes.

25. Plaintiffs and Class Members have suffered injury as a result of Defendants' conduct. These injuries include: (i) lost or diminished value of PII and PHI; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; and (iv) the continued and substantially increased risk to their PII and PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII and PHI.

26. Defendants disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, and/or negligently failing to take and implement adequate and reasonable measures to ensure that the PII and PHI of Plaintiffs and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As the result, the PII and PHI of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

## II. PARTIES

27. Plaintiff Adrian Villalobos is a Citizen of California residing in Los Angeles County, California.

28. Plaintiff John Parsons is a Citizen of Louisiana residing in Lincoln Parish, Louisiana.

29. Plaintiff Christopher Caswell is a Citizen of Georgia residing in Fayette County, Georgia.

30. Plaintiff Robert Davie is a Citizen of California residing in San Bernardino County, California.

31. Plaintiff Peter Horning is a Citizen of Florida residing in Pinellas County, Florida.

32. Plaintiff Julia Kroll is a Citizen of Illinois residing in DuPage County, Illinois.

33. Plaintiff Amanda Marr is a Citizen of California residing in Riverside County, California.

34. Plaintiff Brent McDonald is a Citizen of California residing in San Diego County, California.

35. Plaintiff Jonathon Mitchell is a Citizen of New Hampshire residing in Rockingham County, New Hampshire.

36. Plaintiff Jason Myers is a citizen of California residing in Los Angeles County, California.

37. Plaintiff John Owens is a Citizen of Maryland residing in Maryland.

38. Plaintiff Alan Wellikoff is a Citizen of Maryland residing in Baltimore County, Maryland.

39. Plaintiff Chandra Wilson is a Citizen of Colorado residing in Arapahoe County,

Colorado.

40. Plaintiff Arda Yeremian is a Citizen of California residing in San Mateo County, California.

41. Plaintiff Tracey Bock is a Citizen of West Virginia residing in Wood County, West Virginia.

42. Defendant Arthur J. Gallagher & Co. is a corporation organized under the laws of Delaware, headquartered at 2850 Golf Road, Rolling Meadows, Illinois, with its principal place of business in Rolling Meadows, Illinois.

43. Defendant Gallagher Bassett Services, Inc. is a corporation organized under the laws of Delaware, headquartered at 2850 Golf Road, Rolling Meadows, Illinois, with its principal place of business in Rolling Meadows, Illinois.

44. 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.

45. All of Plaintiffs' claims stated herein are asserted against Defendants and any of their owners, predecessors, successors, subsidiaries, agents and/or assigns.

## III. JURISDICTION AND VENUE

46. 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 Defendants to establish minimal diversity.

47. The Northern District of Illinois has personal jurisdiction over Defendants named in this action because Defendants and/or their parents or affiliates are headquartered in this District and Defendants conduct substantial business in Illinois and this District through their headquarters, offices, parents, and affiliates.

48. Venue is proper in this District under 28 U.S.C. § 1391(b) because Defendants and/or their 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.

## IV. FACTUAL ALLEGATIONS

***Background***

49. Plaintiffs and Class Members directly or indirectly entrusted Defendants with sensitive and confidential information, including their PII and/or PHI, which includes information that is static, does not change, and can be used to commit myriad financial crimes.

50. Plaintiffs and Class Members relied on these sophisticated Defendants to keep their PII and PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members demand security to safeguard their PII and PHI.

51. Defendants had a duty to adopt reasonable measures to protect the PII and PHI of Plaintiffs and Class Members from involuntary disclosure to third parties.

52. Defendants' Privacy Policy, updated December 2019, applies to personal information collected directly from individuals or "via other insurers, consumer-reporting agencies, our affiliated companies, or other third parties in the course of conducting our business."[5]

53. The Privacy Policy represents that Defendants (i) "implement technical,

[5] *See* https://www.ajg.com/us/privacy-policy/ (last visited Oct. 27, 2021).

organizational, administrative and physical measures to help ensure a level of security appropriate to the risk to the personal information we collect, use, disclose and process" and (ii) "restrict access to your personal information to those who require access to such information for legitimate, relevant business purposes."[6]

54. Regarding the deletion of personal information Defendants no longer need, the Privacy Policy represents as follows:

> Once our relationship with you has come to an end, we will retain your personal information for a period of time that enables us to:
>
> - maintain business records for analysis and/or audit purposes;
> - comply with record retention requirements under the law;
> - defend or bring any existing or potential legal claims; and
> - deal with any complaints regarding the Services.
>
> We will delete your personal information when it is no longer required for these purposes. If there is any information that we are unable, for technical reasons, to delete entirely from our systems, we will put in place appropriate measures to prevent any further processing or use of the personal information.

***The Data Breach***

55. On or about August 17, 2021, Defendants sent Plaintiffs a Notice of Data Breach.[7] Defendants informed Plaintiffs (in substantially the same form) that:

> **What Happened?** On September 26, 2020, Gallagher detected a ransomware event impacting our internal systems. We promptly took all our systems offline, including those at Gallagher Bassett, as a precautionary measure, initiated response protocols, launched an investigation with the assistance of third-party cybersecurity and forensic specialists, implemented our business continuity plans to minimize disruption to our customers, and ensured the ongoing security of our systems. We worked with the cybersecurity and forensic specialists to determine what may have happened and what information may have been affected. Our investigation determined

[6] *Id.*

[7] *See, e.g.*, Exhibit 1 (Notice of Data Breach sent to Plaintiff Villalobos). All of the Plaintiffs received materially similar Notices of Data Breach.

> that an unknown party accessed or acquired data contained within certain segments of our network between June 3, 2020 and September 26, 2020. While the investigation was able to confirm that certain systems were accessed, it was unable to confirm what information within those systems was actually accessed. Therefore, in an abundance of caution, Gallagher conducted an extensive review of the entire contents of the impacted systems. On May 24, 2021, Gallagher's investigation confirmed that the impacted data included information relating to certain individuals. Gallagher continued to work through June 23, 2021 to notify our business partners and to obtain address information for impacted individuals to provide accurate notice to impacted parties.
>
> **What Information Was Involved?** Although we are unaware of any actual or attempted misuse of your information, we are providing you this notification in an abundance of caution because certain information relating to you was accessed or acquired during this event. The impacted information relating to you includes your name, medical diagnosis, medical treatment information, and medical claim information.
>
> **What Are We Doing.** The privacy and security of information are among one of our highest priorities and Gallagher has strict security measures in place to protect information in our care. Upon discovering this incident, we immediately took steps to protect the privacy and security of client, partner, and employee information. We also reviewed existing security policies and implemented additional measures and enhanced security tools to further protect information in our systems. We also implemented additional safeguards and are providing additional training to our employees on data privacy and security. We reported this incident to law enforcement and regulatory authorities, as required by law.
>
> In addition to providing notice of this event to you, we are also providing you access, at no cost, to identity and credit monitoring services for twenty-four (24) months through Kroll. Information and instructions on how to activate these complimentary services can be found in the "Steps You Can Take to Help Protect Your Information" attached to this letter.[8]

56. On or about June 30, 2021, Defendants notified various state Attorneys General of the Data Breach. Defendants also provided the Attorneys General with "sample" notices of the

[8] *Id.* at 1.

Data Breach.[9] Defendants advised that the information potentially impacted in the Data Breach included names; Social Security numbers or tax identification numbers; driver's license, passport or other government identification numbers; dates of birth; usernames and passwords; employee identification numbers; financial account or credit card information; and/or electronic signatures as well as medical treatment, claim, diagnosis, medication or other medical information; health insurance information; medical records or account numbers; and/or biometric information.[10]

57. Defendants admitted in the Notice of Data Breach, the reports to the Attorneys General, and the "sample" notices of the Data Breach, that unauthorized third persons accessed files that contained sensitive information about Plaintiffs and Class Members, including PII and/or PHI.

58. Defendants claim that "[u]pon discovery of the cyberattack, the Company took immediate action to secure our network and systems from further immediate harm."[11] However, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again have not been shared with regulators or Plaintiffs and Class Members, who retain a vested interest in ensuring that their information remains protected.

59. The unencrypted PII and PHI of Plaintiffs and Class Members will likely end up for sale on the dark web as that is the *modus operandi* of hackers. In addition, unencrypted PII and PHI may fall into the hands of companies that will use the detailed PII and PHI for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can easily access the PII and PHI of Plaintiffs and Class Members.

---

[9] *See* Exhibit 2 (sample notice filed with Maine Attorney General); Exhibit 3 (letter to Iowa Attorney General); Exhibit 4 (Notice of Data Event filed with Massachusetts Attorney General).
[10] Exhibit 4 at 4.
[11] Exhibit 1.

60. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information they were maintaining for Plaintiffs and Class Members, causing the exposure of PII and PHI for more than three million individuals.

61. 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."[12]

62. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

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

- 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.[13]

63. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendants 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 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

[13] *Id.* at 3–4.

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….[14]

64. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendants 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

[14] *See* CISA, *Security Tip (ST19-001) Protecting Against Ransomware* (Apr. 11, 2019) (rev. Sept. 2, 2021), https://us-cert.cisa.gov/ncas/tips/ST19-001.

**Apply principle of least-privilege**

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

**Harden infrastructure**

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[15]

65. Given that Defendants were storing the PII and PHI of more than three million individuals—and likely much more than that--Defendants could and should have implemented all of the above measures to prevent and detect ransomware attacks.

66. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the PII and PHI of more than 3 million individuals, including Plaintiffs and Class Members.

***Defendants Acquire, Collect, and Store the PII and PHI of Plaintiffs and Class Members.***

67. Defendants acquired, collected, and stored the PII and PHI of Plaintiffs and Class Members.

68. By obtaining, collecting, and storing the PII and PHI of Plaintiffs and Class Members, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting the PII and PHI from disclosure.

[15] *See* Microsoft 365 Defender Threat Intel. Team, *Human-operated ransomware attacks: A preventable disaster* (Mar. 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Aug. 23, 2021).

69. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII and PHI and relied on Defendants to keep their PII and PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

***Securing PII and PHI and Preventing Breaches***

70. Defendants could have prevented this Data Breach by properly securing and encrypting the systems containing the PII and PHI of Plaintiffs and Class Members. Alternatively, Defendants could have destroyed the data, especially for individuals with whom it had not had a relationship for a decade or more.

71. Defendants' negligence in safeguarding the PII and PHI of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to companies like Defendants to protect and secure sensitive data they possess.

72. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect the PII and PHI of Plaintiffs and Class Members from being compromised.

73. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[16] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[17]

[16] 17 C.F.R. § 248.201 (2013).
[17] *Id*.

74. The ramifications of Defendants' failure to keep secure the PII and PHI of Plaintiffs and Class Members are long lasting and severe. Once PII and PHI is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

***Value of Personal Identifiable Information***

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

76. Social Security numbers, for example, 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 for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get

[18] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Oct. 27, 2021).
[19] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed Oct. 27, 2021).
[20] *In the Dark*, VPNOverview (2019), https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed Oct. 27, 2021).

> 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.[21]

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

78. Even then, 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."[22]

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

80. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the

[21] Soc. Sec. Admin., *Identity Theft and Your Social Security Number* (July 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Oct. 27, 2021).
[22] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last accessed Oct. 27, 2021).

black market."[23]

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

82. The fraudulent activity resulting from the Data Breach may not come to light for years.

83. Theft of PHI is also gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."

84. Drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase PII and PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

85. According to account monitoring company LogDog, medical data sells for $50 and up on the Dark Web.[24]

86. Driver's license numbers are also incredibly valuable. "Hackers harvest license numbers because they're a very valuable piece of information. A driver's license can be a critical part of a fraudulent, synthetic identity – which go for about $1200 on the Dark Web. On its own,

---

[23] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Aug. 23, 2021).

[24] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content (last accessed July 20, 2021).

a forged license can sell for around $200."[25]

87. According to national credit bureau Experian:

> A driver's license is an identity thief's paradise. With that one card, someone knows your birthdate, address, and even your height, eye color, and signature. If someone gets your driver's license number, it is also concerning because it's connected to your vehicle registration and insurance policies, as well as records on file with the Department of Motor Vehicles, place of employment (that keep a copy of your driver's license on file), doctor's office, government agencies, and other entities. Having access to that one number can provide an identity thief with several pieces of information they want to know about you. Next to your Social Security number, your driver's license number is one of the most important pieces of information to keep safe from thieves.[26]

88. According to cybersecurity specialty publication CPO Magazine, "[t]o those unfamiliar with the world of fraud, driver's license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation."[27] However, this is not the case. As cybersecurity experts point out:

> "It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks."[28]

89. Victims of driver's license number theft also often suffer unemployment benefit fraud, as described in a recent New York Times article.[29]

---

[25] Lee Matthews, *Hackers Stole Customers' License Numbers From Geico In Months-Long Breach*, Forbes (Apr. 20, 2021, 11:57 A.M.), https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3e4755c38658 (last accessed July 20, 2021).

[26] Sue Poremba, *What Should I Do If My Driver's License Number is Stolen?* (Oct. 24, 2018), https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/ (last accessed July 20, 2021).

[27] Scott Ikeda, *Geico Data Breach Leaks Driver's License Numbers, Advises Customers to Watch Out for Fraudulent Unemployment Claims, CPO Magazine* (Apr. 23, 2021), https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/ (last accessed July 20, 2021).

[28] *Id.*

[29] Ron Lieber, *How Identity Thieves Took My Wife for a Ride,* NY Times (Apr. 27, 2021), https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html (last accessed July 20, 2021).

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

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

91. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the PII and PHI of Plaintiffs and Class Members, including Social Security numbers, and of the foreseeable consequences that would occur if Defendants' 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.

92. Plaintiffs 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 PII and PHI.

93. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants' network, amounting to potentially millions of individuals' detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

94. To date, Defendants have offered Plaintiffs and Class Members only two years of identity and credit monitoring services through Kroll. The offered service is inadequate to protect Plaintiffs and Class Members from the threats they face for years to come, particularly in light of

[30] U.S. Gov't Accountability Off., GAO-07-737, *Report to Congressional Requesters* at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf (last accessed Aug. 23, 2021).

the PII and PHI at issue here. Moreover, Defendants put the burden squarely on Plaintiffs and Class Members to enroll in the inadequate monitoring services.

95. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the PII and PHI of Plaintiffs and Class Members.

***Plaintiff John Parsons' Experience***

96. From January 1996 through April 1999, Plaintiff Parsons worked for Defendant Arthur J. Gallagher in Louisiana.

97. In connection with his employment with Defendant Gallagher, Plaintiff Parsons entrusted his PII and PHI to Defendant.

98. At the time of the Data Breach (June 3, 2020 to September 26, 2020), Defendant retained Plaintiff's name and social security number in its system.

99. Plaintiff McDonald received Defendant's Notice of Data Breach, dated July 12, 2021 on or about July 18, 2021. The notice stated that Plaintiff Parsons's name and social security number were among the information accessed or acquired during the Data Breach.

100. As a result of the Data Breach notice, Plaintiff Parsons spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

101. Additionally, Plaintiff Parsons is very careful about sharing his sensitive PII. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

102. Plaintiff Parsons stores any documents containing his sensitive PII in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

103. Plaintiff Parsons suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that Plaintiff Parsons entrusted to Defendant, which was compromised in and as a result of the Data Breach.

104. Plaintiff Parsons suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

105. Plaintiff Parsons has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII and PHI being placed in the hands of unauthorized third parties and possibly criminals.

106. Plaintiff Parsons has also experienced a substantial increase in suspicious telephone calls, emails, and text messages which he believes is related to his PII and PHI being placed in the hands of unauthorized third parties and possibly criminals in the Data Breach.

107. Plaintiff Parsons has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remain backed up in Defendant's possession, is protected and safeguarded from future breaches.

***Plaintiff Adrian Villalobos' Experience***

108. From approximately September 2015 to approximately August 2019, Plaintiff Villalobos worked for Prolacta Bioscience in Duarte, California.

109. In connection with his employment with Prolacta Bioscience, Plaintiff Villalobos entrusted his PII and/or PHI to Defendants, possibly through a third-party that provided human resources services to Prolacta.

110. At the time of the Data Breach (June 3, 2020 to September 26, 2020), Defendants retained Plaintiff Villalobos' name, medical diagnosis, medical treatment information, and medical claim information in its system.

111. Plaintiff Villalobos received Defendants' Notice of Data Breach, dated August 17, 2021, on August 20, 2021. The notice stated that Plaintiff Villalobos' name, medical diagnosis, medical treatment information, and medical claim information were among the information accessed or acquired during the Data Breach.

112. As a result of the Data Breach notice, Plaintiff Villalobos spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

113. Additionally, Plaintiff Villalobos is very careful about sharing his sensitive PII and PHI. He has never knowingly transmitted unencrypted sensitive PII and PHI over the internet or any other unsecured source.

114. Plaintiff Villalobos stores any documents containing his sensitive PII and PHI in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

115. Plaintiff Villalobos suffered actual injury in the form of damages to and diminution in the value of his PII and PHI—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

116. Plaintiff Villalobos suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

117. Plaintiff Villalobos has suffered imminent and impending injury arising from the

substantially increased risk of fraud, identity theft, and misuse resulting from his PII and PHI being placed in the hands of unauthorized third parties and possibly criminals.

118. Plaintiff Villalobos has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remain backed up in Defendants' possession, is protected and safeguarded from future breaches.

***Plaintiff Christopher Caswell's Experience***

119. From in or around 2016 to in or around December 2020, Plaintiff Caswell worked for Saddle Creek Logistics Services.

120. In connection with his employment with Saddle Creek Logistics Services and a workers compensation claim, Plaintiff Caswell entrusted his PII and/or PHI to Defendant, possibly through a third-party that provided human resources services to Saddle Creek Logistics Services.

121. At the time of the Data Breach (June 3, 2020 to September 26, 2020), Defendant retained Plaintiff Caswell's personal information in its system.

122. Plaintiff Caswell received Defendant's Notice of Data Breach, dated August 17, 2021, on August 20, 2021. The notice stated that Plaintiff's personal information was among the information accessed or acquired during the Data Breach.

123. As a result of the Data Breach notice, Plaintiff Caswell spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

124. Additionally, Plaintiff Caswell is very careful about sharing his sensitive PII and PHI. He has never knowingly transmitted unencrypted sensitive PII and PHI over the internet or any other unsecured source.

125. Plaintiff Caswell stores any documents containing his sensitive PII and PHI in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

126. Plaintiff Caswell suffered actual injury in the form of damages to and diminution in the value of his PII and PHI—a form of intangible property that Plaintiff Caswell entrusted to Defendant, which was compromised in and as a result of the Data Breach.

127. Plaintiff Caswell suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

128. Plaintiff Caswell has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII and PHI being placed in the hands of unauthorized third parties and possibly criminals.

129. Plaintiff Caswell has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remain backed up in Defendant's possession, are protected and safeguarded from future breaches.

***Plaintiff Robert Davie's Experience***

130. From approximately August 1998 to October 2008, Plaintiff Davie worked for Whirlpool Corporation in Vacaville and Hesperia, California

131. In connection with his employment with Whirlpool Corporation, Plaintiff Davie entrusted his PII and/or PHI to Gallagher Bassett as the third-party administrator for Whirlpool Corporation's Workers Compensation claims.

132. At the time of the Data Breach (June 3, 2020 to September 26, 2020), Defendant retained Plaintiff Davie's name, Social Security number, medical record number, medical

diagnosis, medical treatment information, health insurance information and medical claim information in its system.

133. Plaintiff Davie received Defendant's Notice of Data Breach, dated July 21, 2021, on shortly after that date. The notice stated that Plaintiff Davie's name, Social Security number, medical record number, medical diagnosis, medical treatment information, health insurance information and medical claim information were among the information accessed or acquired during the Data Breach. Plaintiff Davie also received a letter from Whirlpool Corporation dated July 28, 2021, on or shortly after that date, stating that its third-party Workers Compensation administrator, Gallagher Basset, had experienced a ransomware attack on its system and that some of his employee information was impacted.

134. Since the Data Breach, Plaintiff Davie has experienced an increase in the number of suspicious phone calls and emails he has received. To contend with this problem, Plaintiff Davie purchased Robokiller for $4.99 per month from approximately July through September of 2021.

135. Also, since the Data Breach, Plaintiff Davie has experienced a decline in his credit score he believes is, at least in part, due to a "hard inquiry" by ADT on his credit report; however, Plaintiff Davie has not used ADT's services. Plaintiff Davie believe this unauthorized inquiry is related to the Data Breach.

136. As a result of the Data Breach notice, Plaintiff Davie spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, self-monitoring his accounts, dealing with fraudulent emails and phone calls, and placing a credit freeze on his credit at all three credit bureaus. This time has been lost forever and cannot be recaptured.

137. Plaintiff Davie is very careful about sharing his sensitive PII and PHI. He has never knowingly transmitted unencrypted sensitive PII and PHI over the internet or any other unsecured source.

138. Plaintiff Davie stores any documents containing his sensitive PII and PHI in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for her various online accounts.

139. Plaintiff Davie suffered actual injury in the form of damages to and diminution in the value of his PII and PHI—a form of intangible property that Plaintiff Davie entrusted to Defendant, which was compromised in and as a result of the Data Breach.

140. Plaintiff Davie suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

141. Plaintiff Davie has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII and PHI being placed in the hands of unauthorized third parties and possibly criminals.

142. Plaintiff Davie has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remain backed up in Defendant's possession, is protected and safeguarded from future breaches.

***Plaintiff Peter Horning's Experience***

143. From 2001 to 2003 and again from 2014 to 2019, Plaintiff Horning worked for the Pinellas County Sheriff's Office in Pinellas County, Florida and from 2003-2014 Plaintiff Horning worked for the Gulf Port Police Department, in Gulf Port, Florida.

144. In connection with his employment with the Pinellas County Sheriff's Office and the Gulf Port Police Department, Plaintiff Horning entrusted his PII and PHI to Defendants,

possibly through Defendant's provision of workers' compensation insurance to either the Pinellas County Sheriff's Office or the Gulf Port Police Department or both.

145. At the time of the Data Breach (June 3, 2020 to September 26, 2020), Defendant retained Plaintiff Horning's name, medical diagnosis, and medical claim information in its system.

146. Plaintiff Horning received Defendant's Notice of Data Breach, dated September 10, 2021 on or about September 14, 2021. The notice stated that Plaintiff Horning's name, medical diagnosis, and medical claim information were among the information accessed or acquired during the Data Breach.

147. As a result of the Data Breach notice, Plaintiff Horning spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

148. Additionally, Plaintiff Horning is very careful about sharing his sensitive PII and PHI. He has never knowingly transmitted unencrypted sensitive PII and PHI over the internet or any other unsecured source.

149. Plaintiff Horning stores any documents containing his sensitive PII and PHI in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

150. Plaintiff Horning suffered actual injury in the form of damages to and diminution in the value of his PII and PHI—a form of intangible property that Plaintiff Horning entrusted to Defendant, which was compromised in and as a result of the Data Breach.

151. Plaintiff Horning suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

152. Plaintiff Horning has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII and PHI being placed in the hands of unauthorized third parties and possibly criminals.

153. Plaintiff Horning has also experienced a substantial increase in suspicious telephone calls, emails, and text messages which he believes is related to his PII and PHI being placed in the hands of unauthorized third parties and possibly criminals.

154. Plaintiff Horning has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remain backed up in Defendant's possession, is protected and safeguarded from future breaches.

***Plaintiff Julia Kroll's Experience***

155. From approximately August to November 2018, Plaintiff Kroll worked for Glenbard School District 87 in Glen Ellyn, Illinois.

156. In connection with her employment with Glenbard School District 87, Plaintiff Kroll entrusted her PII and/or PHI to Defendants, likely through the Suburban School Cooperative Insurance Pool.

157. At the time of the Data Breach (June 3, 2020 to September 26, 2020), Defendant retained Plaintiff Kroll's name and medical claim information in its system.

158. Plaintiff Kroll received Defendant's Notice of Data Breach, dated September 29, 2021 on or shortly after that date. The notice stated that Plaintiff Kroll's name and medical claim information were among the information accessed or acquired during the Data Breach.

159. Since the Data Breach, Plaintiff Kroll has experienced fraudulent charges on her credit card in December 2020 and April 2021, and was unable to purchase furniture and could not, due to the previous fraudulent charge on her credit card. Even now, it is difficult for Plaintiff to

use a credit card for larger purchases due to the fraudulent charges. Plaintiff Kroll has also experienced an increase in suspicious phone calls and emails in general and, in particular, solicitation emails concerning sales of insulin.

160. As a result of the Data Breach notice, Plaintiff Kroll spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, resetting automatic billing instructions tied to compromised credit card accounts, and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

161. Plaintiff Kroll is very careful about sharing her sensitive PII and PHI. She has never knowingly transmitted unencrypted sensitive PII and PHI over the internet or any other unsecured source.

162. Plaintiff Kroll stores any documents containing her sensitive PII and PHI in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

163. Plaintiff Kroll suffered actual injury in the form of damages to and diminution in the value of her PII and PHI—a form of intangible property that Plaintiff Kroll entrusted to Defendant, which was compromised in and as a result of the Data Breach.

164. Plaintiff Kroll suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

165. Plaintiff Kroll has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII and PHI being placed in the hands of unauthorized third parties and possibly criminals.

166. Plaintiff Kroll has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remain backed up in Defendant's possession, is protected and safeguarded from future breaches.

***Plaintiff Amanda Marr's Experience***

167. From approximately 2013 to 2019, Plaintiff Marr worked for Omni Hotels and Resorts ("Omni") in Rancho Mirage, California. Plaintiff Marr has continued since that time to work for Omni on an on-call employee basis.

168. In connection with her employment with Omni, Plaintiff Marr entrusted her PII and/or PHI to Defendant, possibly when she filed a workers' compensation claim for an on-the-job injury she sustained while working for Omni.

169. At the time of the Data Breach (June 3, 2020 to September 26, 2020), Defendant retained Plaintiff Marr's name, Social Security number, medical diagnosis, medical treatment information, medication information, health insurance information, and medical claim information in its system.

170. Plaintiff Marr received Defendant's Notice of Data Breach, dated July 21, 2021, on or shortly after that date. The notice stated that Plaintiff Marr's name, Social Security number, medical diagnosis, medical treatment information, medication information, health insurance information, and medical claim information were among the information accessed or acquired during the Data Breach.

171. As a result of the Data Breach notice, Plaintiff Marr spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach and self-monitoring her bank checking accounts. Plaintiff Marr is also a special needs trustee for her mother and has had to closely monitor her mother's multiple bank accounts

as well. This time has been lost forever and cannot be recaptured.

172. Furthermore, Plaintiff Marr believes that as a result of the Data Breach, in or about the summer of 2020 a criminal used her identity to apply for unemployment benefits with the California Employment Development Department ("EDD"). She received two debit cards from EDD, and when she called to inquire about why she received two, she was instructed to discard the first one.

173. Plaintiff Marr has also received notices since the Data Breach from gotpwned.com indicating that she needed to change her email passwords. Since the Data Breach she has also experienced an increase in scam emails and phone calls; she has received so many scam phone calls that they have filled her voicemail inbox, causing her to miss important voicemails, including from her son's doctor.

174. Plaintiff Marr is very careful about sharing her sensitive PII and PHI. She has never knowingly transmitted unencrypted sensitive PII and PHI over the internet or any other unsecured source.

175. Plaintiff Marr stores any documents containing her sensitive PII and PHI in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

176. Plaintiff Marr suffered actual injury in the form of damages to and diminution in the value of her PII and PHI—a form of intangible property that Plaintiff Marr entrusted to Defendant, which was compromised in and as a result of the Data Breach.

177. Plaintiff Marr suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

178. Plaintiff Marr has suffered imminent and impending injury arising from the

substantially increased risk of fraud, identity theft, and misuse resulting from her PII and PHI being placed in the hands of unauthorized third parties and possibly criminals.

179. Plaintiff Marr has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remain backed up in Defendant's possession, is protected and safeguarded from future breaches.

***Plaintiff Brent McDonald's Experience***

180. From September 2018 through January 2019, Plaintiff McDonald worked for Labor Finders in Carlsbad, California.

181. In connection with his employment with Labor Finders, Plaintiff McDonald entrusted his PII and PHI to Defendant, possibly through Defendant's provision of workers' compensation insurance to Labor Finders.

182. At the time of the Data Breach (June 3, 2020 to September 26, 2020), Defendant retained Plaintiff McDonald's name, social security number, medical diagnosis, medical treatment information, and medical claim information in its system.

183. Plaintiff McDonald received Defendant's Notice of Data Breach, dated July 21, 2021 on or about July 27, 2021. The notice stated that Plaintiff McDonald's name, social security number, medical diagnosis, medical treatment information, and medical claim information were among the information accessed or acquired during the Data Breach.

184. As a result of the Data Breach notice, Plaintiff McDonald spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

185. Additionally, Plaintiff McDonald is very careful about sharing his sensitive PII and PHI. He has never knowingly transmitted unencrypted sensitive PII and PHI over the internet or any other unsecured source.

186. Plaintiff McDonald stores any documents containing his sensitive PII and PHI in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

187. Plaintiff McDonald suffered actual injury in the form of damages to and diminution in the value of his PII and PHI—a form of intangible property that Plaintiff McDonald entrusted to Defendant, which was compromised in and as a result of the Data Breach.

188. Plaintiff McDonald suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

189. Plaintiff McDonald has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII and PHI being placed in the hands of unauthorized third parties and possibly criminals.

190. Furthermore, Plaintiff McDonald has experienced fraud and identity theft which he believes is a result of the Data Breach. This fraud and identity theft has been in the form of unauthorized charges on his bank accounts, which has resulted from his PII and PHI being placed in the hands of unauthorized third parties and possibly criminals.

191. These unauthorized charges have led to him being charged late fees by his bank.

192. These unauthorized charges have also led to legitimate payments by Plaintiff McDonald being rejected which have led to late and declined payment fees with utilities and Plaintiff McDonald's landlord.

193. Plaintiff McDonald has not been reimbursed by any party for the declined payment fees imposed upon him as a result of failed automatic payments which resulted from unauthorized charges caused by his PII and PHI being placed in the hands of unauthorized third parties and possibly criminals.

194. Plaintiff McDonald has spent over 25 hours addressing these issues which resulted from the unauthorized charges on his bank accounts.

195. Plaintiff McDonald has also received mail from credit card companies stating that he was not approved for credit cards which he did not apply for, indicating that he is experiencing identity theft resulting from his PII and PHI being placed in the hands of unauthorized third parties and possibly criminals.

196. Plaintiff McDonald has also experienced a substantial increase in suspicious telephone calls, emails, and text messages which he believes is related to his PII and PHI being placed in the hands of unauthorized third parties and possibly criminals.

197. Plaintiff McDonald has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remain backed up in Defendant's possession, is protected and safeguarded from future breaches.

***Plaintiff Jonathon Mitchell's Experience***

198. From May 2012 to present, Plaintiff Mitchell has worked for Circle Home, Inc., aka VNA of Greater Lowell, Inc. in Lowell, Massachusetts.

199. Circle Home, Inc., is a subsidiary or affiliate of Wellforce and/or the Home Health Foundation.

200. In connection with his employment with Circle Home, Inc., Plaintiff Mitchell entrusted his PII and PHI to Defendant, possibly through Defendant's provision of workers' compensation insurance to Circle Home, Inc., or its other business dealings with Wellforce.

201. At the time of the Data Breach (June 3, 2020 to September 26, 2020), Defendant retained Plaintiff Mitchell's name and social security number in its system.

202. Plaintiff Mitchell received Defendant's Notice of Data Breach, dated July 21, 2021 on or about July 27, 2021. The notice stated that Plaintiff Mitchell's name and social security number were among the information accessed or acquired during the Data Breach.

203. As a result of the Data Breach notice, Plaintiff Mitchell spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

204. Additionally, Plaintiff Mitchell is very careful about sharing his sensitive PII and PHI. He has never knowingly transmitted unencrypted sensitive PII and PHI over the internet or any other unsecured source.

205. Plaintiff Mitchell stores any documents containing his sensitive PII and PHI in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

206. Plaintiff Mitchell suffered actual injury in the form of damages to and diminution in the value of his PII and PHI—a form of intangible property that Plaintiff Mitchell entrusted to Defendant, which was compromised in and as a result of the Data Breach.

207. Plaintiff Mitchell suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

208. Plaintiff Mitchell has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII and PHI being placed in the hands of unauthorized third parties and possibly criminals.

209. Plaintiff Mitchell has also experienced a substantial increase in suspicious telephone calls, emails, and text messages which he believes is related to his PII and PHI being placed in the hands of unauthorized third parties and possibly criminals.

210. Plaintiff Mitchell has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remain backed up in Defendant's possession, is protected and safeguarded from future breaches.

***Plaintiff John Owens' Experience***

211. From 1986-2014, Plaintiff Owens worked for the Montgomery County Fire and Rescue ("Montgomery County") in the State of Maryland.

212. In connection with his employment with Montgomery County, Plaintiff Owens was provided health insurance. He also submitted multiple workers compensation claims from 2001 to 2011. As part of the insurance process, he entrusted his PII and/or PHI to Defendants, possibly through a third party that provided Human Resources to Montgomery County.

213. At the time of the Data Breach (June 2, 2020 to September 26, 2020), Defendants retained Plaintiff Owens' name and medical information in its systems and potentially other PII and PHI.

214. Plaintiff received Defendants' Notice of Data Breach, dated August 10, 2021, in mid-August, 2021. The notice stated that Plaintiff Owens' name and medical information were among the information accessed or acquired during the Data Breach.

215. As a result of the Data Breach notice, Plaintiff Owens spent time dealing with the

consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of the Data Breach and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

216. Additionally, Plaintiff Owens is very careful about sharing his sensitive PII and PHI. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

217. Plaintiff Owens stores any documents containing his PII and PHI in a safe and secure location or destroys documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

218. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PI and PHI—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

219. Plaintiff Owens has suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his and his family's privacy.

220. Furthermore, following the Data Breach, Plaintiff Owens also experienced an increase in spam phone calls and emails. In response, Plaintiff purchased and installed a spam phone system that cost $100.00.

221. Plaintiff Owens has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of his PII and PHI resulting from his PII and PHI being placed in the hands of unauthorized criminal third parties.

222. Plaintiff Owens has a continuing interest in ensuring that his PII and PHI, which upon information and belief, remain backed up in Defendant's possession, is protected and

safeguarded from future breaches.

***Plaintiff Alan Welikoff's Experience***

223. Plaintiff is unaware of how Defendants came into possession of his PII.

224. Plaintiff Wellikoff received Defendant's Notice of Data Breach, dated August 17, 2021, on or shortly after that date. The notice stated that Plaintiff Wellikoff's name and medical claim information were among the information accessed or acquired during the Data Breach.

225. Since the Data Breach, Plaintiff Wellikoff has received text message notifications with password reset and verification codes from several of his accounts, including Xfinity and GoDaddy, when he has not attempted to change his username or password for any accounts. This indicates that one or more unknown third parties have been attempting to access his accounts. An unauthorized third party has also attempted to access his bank accounts.

226. Furthermore, on October 12, 2021, Plaintiff Wellikoff received a notification from McAfee that his Comcast email address was found on the dark web.

227. Since the Data Breach, Plaintiff Wellikoff has also experienced an increase in suspicious phone calls and emails.

228. As a result of the Data Breach notice, Plaintiff Wellikoff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, signing up for two-factor authentication for his bank accounts, self-monitoring his accounts and dealing with the increase in suspicious phone calls and emails. This time has been lost forever and cannot be recaptured.

229. Plaintiff Wellikoff is very careful about sharing his sensitive PII and PHI. He has never knowingly transmitted unencrypted sensitive PII and PHI over the internet or any other unsecured source.

230. Plaintiff Wellikoff stores any documents containing his sensitive PII and PHI in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

231. Plaintiff Wellikoff suffered actual injury in the form of damages to and diminution in the value of his PII and PHI—a form of intangible property that Plaintiff Wellikoff entrusted to Defendant, which was compromised in and as a result of the Data Breach. Plaintiff Wellikoff also paid for a credit freeze after learning of the Data Breach.

232. Plaintiff Wellikoff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

233. Plaintiff Wellikoff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII and PHI being placed in the hands of unauthorized third parties and possibly criminals.

234. Plaintiff Wellikoff has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remain backed up in Defendant's possession, is protected and safeguarded from future breaches.

***Plaintiff Chandra Wilson's Experience***

235. From approximately 1997 to approximately 2006, and again from June 2012 to the present, Plaintiff Wilson has worked for United Airlines in Denver, Colorado.

236. In connection with her employment with United Airlines, Plaintiff Wilson entrusted her PII and/or PHI to Defendant, possibly in connection with one or more Workers Compensation claims.

237. At the time of the Data Breach (June 3, 2020 to September 26, 2020), Defendant retained Plaintiff Wilson's name, Social Security number, medical diagnosis, medical treatment information, health insurance information, and medical claim information in its system.

238. Plaintiff Wilson received Defendant's Notice of Data Breach, dated September 29, 2021, on or shortly after that date. The notice stated that Plaintiff Wilson's name, Social Security number, medical diagnosis, medical treatment information, health insurance information, and medical claim information were among the information accessed or acquired during the Data Breach.

239. Since the Data Breach and beginning in October 2020, Plaintiff Wilson has suffered from identity theft. In February and March 2021, Plaintiff Wilson discovered that someone had opened five utility accounts in her name using her Social Security number and date of birth in Texas at three different utility companies: Reliant Energy, TXU Energy and First Choice Power.

240. Furthermore, since the Data Breach Plaintiff Wilson received a notification from LifeLock that her email address is on the dark web, and she has experienced an increase in suspicious phone calls and emails.

241. As a result of the Data Breach that resulted in the theft of her identity, Plaintiff Wilson has suffered adverse effects to her credit score, has been denied credit, and has spent money on LifeLock to protect her identity. Plaintiff Wilson has also spent numerous hours dealing with the consequences of the Data Breach, including time spent disputing the charges from and the legitimacy of the five fraudulent accounts at the Texas power companies, attempting to correct her credit report, placing a freeze on her credit, and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

242. Plaintiff Wilson is very careful about sharing her sensitive PII and PHI. She has never knowingly transmitted unencrypted sensitive PII and PHI over the internet or any other unsecured source.

243. Plaintiff Wilson stores any documents containing her sensitive PII and PHI in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

244. Plaintiff Wilson suffered actual injury in the form of damages to and diminution in the value of her PII and PHI—a form of intangible property that Plaintiff Wilson entrusted to Defendant, which was compromised in and as a result of the Data Breach.

245. Plaintiff Wilson suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

246. Plaintiff Wilson has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII and PHI being placed in the hands of unauthorized third parties and possibly criminals.

247. Plaintiff Wilson has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remain backed up in Defendant's possession, is protected and safeguarded from future breaches.

***Plaintiff Arda Yeremian's Experience***

248. From approximately 2014 to approximately July of 2017 and then again in 2020 for a couple of months, Plaintiff Yeremian worked for Arthur J. Gallagher & Co. in Glendale, California and San Francisco, California.

249. In connection with her employment with Arthur J. Gallagher & Co., Plaintiff Yeremian entrusted her PII and/or PHI to Defendant.

250. At the time of the Data Breach (June 3, 2020 to September 26, 2020), Defendant retained Plaintiff Yeremian's name, Social Security number and employee identification number in its system.

251. Plaintiff Yeremian received Defendant's Notice of Data Breach, dated August 10, 2021, on or shortly after that date. The notice stated that Plaintiff Yeremian's name, Social Security number and employee identification number were among the information accessed or acquired during the Data Breach.

252. Beginning in or around July 2021, Plaintiff Yeremian experienced several instances of identity theft, including: someone using her identity to file a false tax return; someone using her identity to claim MediCal benefits; someone using her identity to obtain health insurance through Covered California; and someone using her identity to claim her stimulus disbursement from the Internal Revenue Service.

253. Plaintiff Yeremian has also received emailed notifications from LifeLock and Microsoft Exchange Enterprise indicating that her PII, including her name, Social Security number, telephone number, email address, and home address, is on the dark web. The email notifications indicate that the source of her PII found on the dark web is Microsoft Exchange Enterprise Portal, a system used by Defendant.

254. Since the Data Breach, Plaintiff Yeremian has also experienced an increase in healthcare related solicitation emails, texts and calls as well as suspicious phone calls and emails in general.

255. Also, as a result of the Data Breach, Plaintiff Yeremian's credit score has plummeted.

256. As a result of the Data Breach notice and the identity theft she has experienced, Plaintiff Yeremian has spent numerous hours dealing with the consequences of the Data Breach, which includes time spent: verifying the legitimacy of the Notice of Data Breach; self-monitoring her accounts; speaking to bank representatives concerning her accounts; speaking with representatives at the Social Security office; driving to the Post Office and the Social Security office; filing a police report; filing a report with the Federal Trade Commission; contacting all of her credit card companies; and contacting Experian, Equifax and TransUnion. This time has been lost forever and cannot be recaptured.

257. Plaintiff Yeremian is very careful about sharing her sensitive PII and PHI. She has never knowingly transmitted unencrypted sensitive PII and PHI over the internet or any other unsecured source.

258. Plaintiff Yeremian stores any documents containing her sensitive PII and PHI in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

259. Plaintiff Yeremian suffered actual injury in the form of damages to and diminution in the value of her PII and PHI—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach. Plaintiff Yeremian has also incurred out-of-pocket expense since the Data Breach to protect herself from identity theft including, but not limited to, her purchases of Norton 360 with LifeLock in or about December 2020, and Webroot in or about March 2021, to protect against identity theft.

260. Plaintiff Yeremian suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

261. Plaintiff Yeremian has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII and PHI being placed in the hands of unauthorized third parties and possibly criminals.

262. Plaintiff Yeremian has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remain backed up in Defendant's possession, is protected and safeguarded from future breaches.

***Plaintiff Tracey Bock's Experience***

263. While employed as a flight attendant for Miami Air International in January 2017, Plaintiff Bock was injured while on the premise of a local hotel while on a layover in Fargo, North Dakota. Plaintiff Bock's personal injury claims in North Dakota were ultimately settled as well as her Workers Compensation claims.

264. In connection with, and through her employment with Miami Air International, Plaintiff Bock entrusted her PII and/or PHI to Gallagher Bassett as the third-party administrator to process her Workers Compensation claims.

265. At the time of the Data Breach (June 3, 2020 to September 26, 2020), Defendant retained Plaintiff Bock's name and Social Security number, medical record number, medical diagnosis, medical treatment information, health insurance information and medical claim information in its systems.

266. Plaintiff Bock received the Data Breach notice letter, dated July 21, 2021, on or shortly after that date. The notice letter stated that Plaintiff Bock's name, medical diagnosis, and medical claim information were among the information accessed or acquired during the Data Breach.

267. As a result of the Data Breach, Plaintiff Bock has spent valuable time dealing with the consequences of the breach including confirming the legitimacy of the Data Breach, reviewing accounts potentially compromised by the Data Breach, self-monitoring accounts, and working with her financial institution for numerous unauthorized account purchases through her Apple iCloud account with her associated debit card, which she has had to replace twice as a result of the Data Breach.

268. Additionally, Plaintiff Bock is very careful about sharing her sensitive PHI and/or PII. She has never knowingly transmitted unencrypted sensitive PHI and/or PII over the internet or any other unsecured source.

269. Plaintiff Bock stores any documents containing her sensitive PHI and/or PII in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

270. Plaintiff Bock suffered actual injury in the form of damages to and diminution in the value of her PHI and/or PII—a form of intangible property that Plaintiff Bock entrusted to Defendant, which was compromised in and as a result of the Data Breach.

271. Plaintiff Bock suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

272. Plaintiff Bock has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII and PHI being placed in the hands of unauthorized third parties and possibly criminals.

273. Plaintiff Bock has also experienced a substantial increase in suspicious spam telephone calls, and text messages which she believes is related to her PII and/or PHI being placed in the hands of unauthorized third parties and possibly criminals in the Data Breach.

274. Plaintiff Bock has a continuing interest in ensuring that her PII and/or PHI, which, upon information and belief, remain backed up in Defendant's possession, is protected and safeguarded from future data breaches.

## V. CLASS ALLEGATIONS

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

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

> All United States residents whose PII and/or PHI was accessed or acquired during the ransomware event that is the subject of the Notice of Data Breach that Defendants sent to Plaintiffs and other Class Members on or around August 17, 2021 (the "Nationwide Class").

277. In the alternative to claims asserted on behalf of the Nationwide Class, Plaintiffs Villalobos, Robert Davie, Amanda Marr, Brent McDonald, and Arda Yeremian ("California Plaintiffs") assert claims on behalf of a separate subclass, defined as follows:

> All individuals residing in California whose PII and/or PHI was actually or potentially accessed or acquired during the ransomware event that is the subject of the Notice of Data Breach that Defendants sent to Plaintiffs and other Class Members on or around August 17, 2021 (the "California Class").

278. In the alternative the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff Chandra Wilson asserts claims on behalf of a separate subclass, defined as follows:

> All individuals residing in Colorado whose PII and/or PHI was actually or potentially accessed or acquired during the ransomware event that is the subject of the Notice of Data Breach that Defendants sent to Plaintiffs and other Class Members on or around August 17, 2021 (the "Colorado Class").

279. In the alternative the alternative to claims asserted on behalf of the Nationwide

Class, Plaintiff Peter Horning asserts claims on behalf of a separate subclass, defined as follows:

> All individuals residing in Florida whose PII and/or PHI was actually or potentially accessed or acquired during the ransomware event that is the subject of the Notice of Data Breach that Defendants sent to Plaintiffs and other Class Members on or around August 17, 2021 (the "Florida Class").

280. In the alternative the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff Christopher Caswell asserts claims on behalf of a separate subclass, defined as follows:

> All individuals residing in Georgia whose PII and/or PHI was actually or potentially accessed or acquired during the ransomware event that is the subject of the Notice of Data Breach that Defendants sent to Plaintiffs and other Class Members on or around August 17, 2021 (the "Georgia Class").

281. In the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff Julia Kroll asserts claims on behalf of a separate subclass, defined as follows:

> All individuals residing in Illinois whose PII and/or PHI was actually or potentially accessed or acquired during the ransomware event that is the subject of the Notice of Data Breach that Defendants sent to Plaintiffs and other Class Members on or around August 17, 2021 (the "Illinois Class").

282. In the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff John Parsons asserts claims on behalf of a separate subclass, defined as follows:

> All individuals residing in Louisiana whose PII and/or PHI was actually or potentially accessed or acquired during the ransomware event that is the subject of the Notice of Data Breach that Defendants sent to Plaintiffs and other Class Members on or around August 17, 2021 (the "Louisiana Class").

283. In the alternative to claims asserted on behalf of the Nationwide Class, Plaintiffs John Owens and Alan Wellikoff ("Maryland Plaintiffs") assert claims on behalf of a separate subclass, defined as follows:

> All individuals residing in Maryland whose PII and/or PHI was actually or potentially accessed or acquired during the ransomware event that is the subject of the Notice of Data Breach that Defendants sent to Plaintiffs and other Class Members on or around August 17, 2021 (the "Maryland Class").

284. In the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff Johnathon Mitchell asserts claims on behalf of a separate subclass, defined as follows:

> All individuals residing in New Hampshire whose PII and/or PHI was actually or potentially accessed or acquired during the ransomware event that is the subject of the Notice of Data Breach that Defendants sent to Plaintiffs and other Class Members on or around August 17, 2021 (the "New Hampshire Class").

285. In the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff Tracey Bock asserts claims on behalf of a separate subclass, defined as follows:

> All individuals residing in West Virginia whose PII and/or PHI was actually or potentially accessed or acquired during the ransomware event that is the subject of the Notice of Data Breach that Defendants sent to Plaintiffs and other Class Members on or around August 17, 2021 (the "West Virginia Class").

286. Excluded from the Classes are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants 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.

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

288. Numerosity, Fed R. Civ. P. 23(a)(1): The Nationwide Class (the "Class") are so

numerous that joinder of all members is impracticable. Defendants have identified millions of individuals whose PII and/or PHI may have been improperly accessed in the Data Breach, and the Class is apparently identifiable within Defendants' records. Defendants advised Maine Attorney General Frey that the Data Breach affected more than 3 million individuals.

289. 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 Defendants had a duty to protect the PII and PHI of Plaintiffs and Class Members;

b. Whether Defendants had duties not to disclose the PII and PHI of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendants had duties not to use the PII and PHI of Plaintiffs and Class Members for non-business purposes;

d. Whether Defendants failed to adequately safeguard the PII and PHI of Plaintiffs and Class Members;

e. Whether and when Defendants actually learned of the Data Breach;

f. Whether Defendants adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII and PHI had been compromised;

g. Whether Defendants violated the law by failing to promptly notify Plaintiffs and Class Members that their PII and PHI had been compromised;

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

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

j. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiffs and Class Members;

k. Whether Defendants violated the consumer protection statutes invoked herein;

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

m. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendants' wrongful conduct; and

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

290. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of those of other Class Members because all had their PII and PHI compromised as a result of the Data Breach, due to Defendants' misfeasance.

291. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendants 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. Defendants' policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

292. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that he has no disabling conflicts of interest that

would be antagonistic to those of the other Members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages he has suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

293. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The 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 Defendants. 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.

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

of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

295. The litigation of the claims brought herein is manageable. Defendants' 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.

296. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

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

298. Further, Defendants 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.

299. 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 Defendants owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII and PHI;

b. Whether Defendants breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII and PHI;

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

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

e. Whether Defendants breached the implied contract;

f. Whether Defendants adequately and accurately informed Plaintiffs and Class Members that their PII and PHI had been compromised;

g. Whether Defendants 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 Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiffs and Class Members; and,

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

## COUNT I

**Negligence**
**(On Behalf of Plaintiffs and the Nationwide Class or, alternatively, the Subclasses)**

300. Plaintiffs and the Nationwide Class or, alternatively, the Subclasses (collectively, the "Classes"), re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 299.

301. Plaintiff and the Classes entrusted Defendants with their PII and/or PHI.

302. Plaintiff and the Classes entrusted their PII and/or PHI to Defendants on the premise and with the understanding that Defendants would safeguard their information, use their PII and/or PHI for business purposes only, and/or not disclose their PII and/or PHI to unauthorized third parties.

303. Defendants have full knowledge of the sensitivity of the PII and/or PHI and the types of harm that Plaintiffs and the Classes could and would suffer if the PII and/or PHI were wrongfully disclosed.

304. Defendants knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII and/or PHI of Plaintiffs and the Classes involved an unreasonable risk of harm to Plaintiffs and the Classes, even if the harm occurred through the criminal acts of a third party.

305. Defendants 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, designing, maintaining, and testing Defendants' security protocols to ensure that the PII and PHI of Plaintiff and the Classes in Defendants' possession was adequately secured and protected.

306. Defendants also had a duty to exercise appropriate clearinghouse practices to remove PII and/or PHI they were no longer required to retain pursuant to regulations.

307. Defendants also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII and/or PHI of Plaintiffs and the Classes.

308. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between Defendants and Plaintiffs and the Classes. That special relationship arose because Plaintiffs and the Classes entrusted Defendants with their confidential PII and/or PHI, a necessary part of obtaining services from Defendants.

309. Defendants were subject to an "independent duty," untethered to any contract between Defendants and Plaintiffs or the Classes.

310. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Classes was reasonably foreseeable, particularly in light of Defendants' inadequate security practices.

311. Plaintiffs and the Classes were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the PII and/or PHI of Plaintiffs and the Classes, the critical importance of providing adequate security of that PII and/or PHI, and the necessity for encrypting PII and/or PHI stored on Defendants' systems.

312. Defendants' own conduct created a foreseeable risk of harm to Plaintiffs and the Classes. Defendants' misconduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendants' misconduct also included their decisions not to comply with industry standards for the safekeeping of the PII and PHI of Plaintiff and the Classes, including basic encryption techniques freely available to

Defendants.

313. Plaintiffs and the Classes had no ability to protect their PII and/or PHI that was in, and possibly remains in, Defendants' possession.

314. Defendants were in a position to protect against the harm suffered by Plaintiffs and the Classes as a result of the Data Breach.

315. Defendants had and continue to have a duty to adequately disclose that the PII and PHI of Plaintiffs and the Classes within Defendants' 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 Classes to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII and/or PHI by third parties.

316. Defendants had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII and/or PHI of Plaintiffs and the Classes.

317. Defendants have admitted that the PII and/or PHI of Plaintiffs and the Classes was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

318. Defendants, through their actions and/or omissions, unlawfully breached their duties to Plaintiffs and the Classes by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII and PHI of Plaintiffs and the Classes during the time the PII and/or PHI was within Defendants' possession or control.

319. Defendants improperly and inadequately safeguarded the PII and/or PHI of Plaintiffs and the Classes in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

320. Defendants failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII and/or PHI of Plaintiffs and the Classes in the face of increased risk

of theft.

321. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiffs and the Classes by failing to have appropriate procedures in place to detect and prevent dissemination of PII and/or PHI.

322. Defendants breached their duty to exercise appropriate clearinghouse practices by failing to remove PII and/or PHI they were no longer required to retain pursuant to regulations.

323. Defendants, through their actions and/or omissions, unlawfully breached their duty to adequately and timely disclose to Plaintiffs and the Classes the existence and scope of the Data Breach.

324. But for Defendants' wrongful and negligent breach of duties owed to Plaintiffs and the Nationwide Class, the PII and/or PHI of Plaintiffs and the Classes would not have been compromised.

325. There is a close causal connection between Defendants' failure to implement security measures to protect the PII and/or PHI of Plaintiffs and the Classes and the harm, or risk of imminent harm, suffered by Plaintiffs and the Nationwide Class. The PII and/or PHI of Plaintiffs and the Classes was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such PII and/or PHI by adopting, implementing, and maintaining appropriate security measures.

326. Additionally, 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 and/or PHI. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

327. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and/or PHI and not complying with applicable industry standards, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of PII and/or PHI it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Classes.

328. Defendants' violation of Section 5 of the FTC Act constitutes negligence *per se*.

329. Plaintiffs and the Classes are within the class of persons that the FTC Act was intended to protect.

330. 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 Plaintiffs and the Classes.

331. As a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiffs and the Classes 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 and/or PHI is used; (iii) the compromise, publication, and/or theft of their PII and/or PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and/or PHI; (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 and/or PHI, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants

fail to undertake appropriate and adequate measures to protect the PII and/or PHI of Plaintiff and the Classes; 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 and/or PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Classes.

332. As a direct and proximate result of Defendant' negligence and negligence *per se*, Plaintiffs and the Classes 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.

333. Additionally, as a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiffs and the Classes have suffered and will suffer the continued risks of exposure of their PII and/or PHI, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII and/or PHI in its continued possession.

334. As a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiffs and the Classes are entitled to recover actual, consequential, and nominal damages.

## COUNT II

### Breach of Implied Contract
### (On Behalf of Plaintiffs and the Nationwide Class or, alternatively, the Subclasses)

335. Plaintiffs and the Nationwide Class or, alternatively, the Subclasses (collectively, the "Classes"), re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 299.

336. Plaintiffs and the Classes entrusted their PII and/or PHI to Defendants. In so doing, Plaintiffs and the Classes entered into implied contracts with Defendants by which Defendants agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and the Classes if their data had been breached and compromised or stolen.

337. In their Privacy Policy, Defendants represented that they (i) implemented measures to help ensure an appropriate level of security for the PII and PHI and (ii) would delete the PII of PHI of individuals with which Defendants no longer had a relationship unless certain enumerated conditions existed.

338. Plaintiffs and the Classes fully performed their obligations under the implied contracts with Defendants.

339. Defendants breached the implied contracts they made with Plaintiffs and the Classes by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiffs and the Classes once the relationship ended, and by failing to provide timely and accurate notice to them that personal information was compromised as a result of the Data Breach.

340. As a direct and proximate result of Defendants' above-described breach of implied contract, Plaintiffs and the Classes 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.

341. As a direct and proximate result of Defendants' above-described breach of implied contract, Plaintiffs and the Classes are entitled to recover actual, consequential, and nominal damages.

## COUNT III

### Unjust Enrichment
### (On Behalf of Plaintiffs and the Nationwide Class or, alternatively, the Subclasses and in the Alternative to Count II)

342. Plaintiffs and the Nationwide Class or, alternatively, the Subclasses (collectively, the "Classes"), re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 299. Plaintiffs plead this Count in the alternative to Count II.

343. Plaintiff and Class Members conferred a monetary benefit on Defendants, by providing Defendants with their valuable PII and PHI.

344. Defendants enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII and PHI.

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

346. Under the principles of equity and good conscience, Defendants should not be permitted to retain the monetary value of the benefit belonging to Plaintiffs and Class Members, because Defendants failed to implement appropriate data management and security measures that

are mandated by industry standards.

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

348. If Plaintiffs and Class Members knew that Defendants had not secured their PII and PHI, they would not have agreed to provide their PII and PHI to Defendants.

349. Plaintiffs and Class Members have no adequate remedy at law.

350. As a direct and proximate result of Defendants' 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 PII is used; (iii) the compromise, publication, and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and PHI; (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 PII and PHI, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect PII and PHI 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 PII and PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

351. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

352. Defendants should be compelled to disgorge into a common fund or constructive

trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them.

## COUNT IV

### Violation of California's Consumer Privacy Act, Cal. Civ. Code. § 1798.150 (On behalf of Plaintiff Jason Myers and the California Class)

353. Plaintiff Jason Myers and the California Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 299.

354. Defendants violated Section 1798.150(a) of the California Consumer Privacy Act ("CCPA") by failing to prevent Plaintiff's and the California Class's nonencrypted and nonredacted PII and PHI from unauthorized access and exfiltration, theft, or disclosure as a result of Defendants' violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII and PHI of Plaintiff and the California Class.

355. As a direct and proximate result of Defendants' acts, Plaintiff's, and the California Class's PII and/or PHI was subjected to unauthorized access and exfiltration, theft, or disclosure through Defendants' computer network.

356. As a direct and proximate result of Defendants' acts, Plaintiff and the California Class were injured and lost money or property, including but not limited to the loss of the California Class's legally protected interest in the confidentiality and privacy of their PII and/or PHI, nominal damages, and additional losses as described above.

357. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard the California Class's PII and/or PHI and that the risk of a data breach or theft was highly likely. Defendants failed to implement and maintain

reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiff and the California Class.

358. Defendants are organized or operated for the profit or financial benefit of their shareholders. Defendants collected Plaintiff's and the California Class's PII and/or PHI as defined in Cal. Civ. Code § 1798.140.

359. Defendants (a) have a gross annual revenue of over $25 million and (b) buy, receive, or sell the personal information of 50,000 or more California residents, households, or devices.

360. Pursuant to Section 1798.150(b) of the CCPA, Plaintiff Myers has given written notice to Defendants of their violations of Section 1798.150(a) by a certified mail letter. Defendants, however, have failed to "actually cure" their violations within 30 days of the written notice.

361. As a result, Plaintiff Myers and the California Class seek relief under § 1798.150(a), including, but not limited to, statutory damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater; injunctive or declaratory relief; any other relief the Court deems proper; and attorneys' fees and costs pursuant to Cal. Code Civ. Proc. § 1021.5.

## COUNT V

**Violation of California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq.***
**(On behalf of Plaintiff Jason Myers and the California Class)**

362. Plaintiff Jason Myers and the California Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 299.

363. The California Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq.* ("CLRA"), was enacted to protect consumers against unfair and deceptive business practices. It

extends to transactions that are intended to result, or which have resulted, in the sale or lease of goods or services to consumers. Defendants' acts, omissions, representations, and practices as described herein fall within the CLRA because the design, development, and marketing of Defendants' insurance services are intended to and did result in sales of insurance services.

364. Plaintiff and the California Class are consumers within the meaning of Cal. Civ. Code § 1761(d).

365. Defendants' acts, omissions, misrepresentations, and practices were and are likely to deceive consumers. By omitting key information about the safety and security of their network and deceptively representing that they adequately maintained such information, Defendants violated the CLRA. Defendants had exclusive knowledge of undisclosed material facts, namely, that their network was defective and/or unsecure, and withheld that knowledge from the California Class.

366. Defendants' acts, omissions, misrepresentations, and practices alleged herein violated the following provisions of Section 1770 the CLRA, which provides, in relevant part, that:

> (a) The following unfair methods of competition and unfair or deceptive acts or practices undertaken by any person in a transaction intended to result or which results in the sale or lease of goods or services to any consumer are unlawful:
>
> (5) Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have . . . .
>
> (7) Representing that goods or services are of a particular standard, quality, or grade . . . if they are of another.
>
> (9) Advertising goods or services with intent not to sell them as advertised.
>
> (14) Representing that a transaction confers or involves rights, remedies, or obligations which it does not have or involve, or which are prohibited by law.

> (16) Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

For purposes of the CLRA, omissions are actionable along with representations.

367. Defendants stored Plaintiff's and the California Class's PII and PHI on their network. Defendants represented to Plaintiff and the California Class that their network was secure and that their PII and PHI would remain private. In particular, Gallagher engaged in deceptive acts and business practices by providing in its Privacy Policy: "We implement technical, organizational, administrative and physical measures to help ensure a level of security appropriate to the risk to the personal information we collect, use, disclose and process;" and "[w]e restrict access to your personal information to those who require access to such information for legitimate, relevant business purposes."[31]

368. Defendants knew or should have known that they did not employ reasonable measures that would have kept California Plaintiff's and the California Class's PII and PHI secure and prevented the loss or misuse of their PII and PHI. For example, Defendants failed to take reasonable steps to prevent the loss of PII and PHI through their servers through appropriate encryption and industry best practices.

369. Defendants' deceptive acts and business practices induced Plaintiff and the California Class to provide PII and PHI, including Social Security numbers and driver's license numbers, for the purchase of insurance services. But for these deceptive acts and business practices, Plaintiff and the California Class would not have purchased insurance services or would not have paid the prices they paid for the insurance services.

[31] https://www.ajg.com/us/privacy-policy/ (last visited Oct. 27, 2021).

370. Defendants' representations that they would secure and protect Plaintiff's and the California Class's PII and PHI in their possession were facts that reasonable persons could be expected to rely upon when deciding whether to purchase insurance services.

371. Plaintiff and the California Class were harmed as the result of Defendants' violations of the CLRA, because their PII and PHI were compromised, placing them at a greater risk of identity theft; they lost the unencumbered use of their PII and PHI; and their PII and PHI was disclosed to third parties without their consent.

372. Plaintiff and the California Class suffered injury in fact and lost money or property as the result of Defendants' failure to secure their PII and PHI; the value of their PII and PHI was diminished as the result of Defendants' failure to secure their PII and PHI; and they have expended time and money to rectify or guard against further misuse of their PII and PHI.

373. Defendants' conduct alleged herein was oppressive, fraudulent, and/or malicious, thereby justifying an award of punitive damages.

374. As the result of Defendants' violations of the CLRA, Plaintiff, on behalf of himself, the California Class, and the general public of the State of California, seeks injunctive relief prohibiting Defendants from continuing these unlawful practices pursuant to California Civil Code § 1782(a)(2), and such other equitable relief, including restitution, and a declaration that Defendants' conduct violated the CLRA.

375. Pursuant to Cal. Civ. Code § 1782, Plaintiff Myers mailed Defendants notice in writing, via U.S. certified mail, of the particular violations of Cal. Civ. Code § 1770 of the CLRA and demanded that it rectify the actions described above by providing complete monetary relief, agreeing to be bound by Defendants' legal obligations and to give notice to all affected customers of their intent to do so. Defendants failed to take the actions demanded to rectify its violations of

the CLRA. As a result, Plaintiff Myers seeks monetary damages and attorneys' fees as allowed by the CLRA.

## COUNT VI

### Violation of California's Customer Records Act
### (On behalf of the California Plaintiffs and the California Class)

376. California Plaintiffs and the California Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 299.

377. This Count is brought on behalf of California Plaintiffs and the California Subclass.

378. "[T]o ensure that Personal Information about California residents is protected," the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business that "owns, licenses, or maintains Personal Information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the Personal Information from unauthorized access, destruction, use, modification, or disclosure."

379. Defendants are a business that maintains PII about California Plaintiffs and California Subclass Members within the meaning of Cal. Civ. Code § 1798.81.5. Such PII includes, but is not limited to, the first and last names of California Plaintiffs and the California Subclass Members, along with account numbers or credit or debit card numbers, in combination with any required security code, access code, or password that would permit access to California Plaintiffs and the California Subclass Members' financial accounts. *See* Cal. Civ. Code § 1798.81.5(d)(1)(A)(iii).

380. Businesses that maintain computerized data that includes PII are required to "notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been,

acquired by an unauthorized person." Cal. Civ. Code § 1798.82(b). Among other requirements, the security breach notification must include "the types of Personal Information that were or are reasonably believed to have been the subject of the breach." Cal. Civ. Code § 1798.82.

381. Defendants are a business that maintains computerized data that includes PII as defined by Cal. Civ. Code § 1798.80.

382. California Plaintiffs and California Subclass Members' PII includes Personal Information as covered by Cal. Civ. Code § 1798.82.

383. Because Defendants reasonably believed that California Plaintiffs and California Subclass Members' PII was acquired by unauthorized persons during the Data Breach, Defendants had an obligation to disclose the Data Breach, immediately following its discovery, to the owners or licensees of the PII (*i.e.*, California Plaintiffs and the California Subclass Members) as mandated by Cal. Civ. Code § 1798.82.

384. By failing to disclose the Data Breach immediately following its discovery, Defendants violated Cal. Civ. Code § 1798.82.

385. As a direct and proximate result of Defendants' violations of the Cal. Civ. Code §§ 1798.81.5 and 1798.82, California Plaintiffs and California Subclass Members suffered damages, as described above and as will be proven at trial.

386. California Plaintiffs and California Subclass Members seek relief under Cal. Civ. Code § 1798.84, including actual damages, injunctive relief, and reasonable attorneys' fees and costs.

## COUNT VII

**Violation of the Confidentiality of Medical Information Act ("CMIA"),**
**Cal. Civ. Code §§ 56, *et seq*.**
**(On Behalf of California Plaintiffs and the California Class)**

387. California Plaintiffs and the California Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 299.

388. This Count is brought on behalf of California Plaintiffs and the California Subclass.

389. At all relevant times, Defendants were healthcare providers for the purposes of this cause of action because they had the "purpose of maintaining medical information to make the information available to an individual or to a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage his or her information, or for the diagnosis or treatment of the individual."

390. Defendants are providers of healthcare, health care services plans and/or contractors for the purposes of this cause of action within the meaning of Civil Code § 56.06(a) and maintain medical information as defined by Civil Code § 56.05.

391. Plaintiffs and California Class Members are patients for purposes of this cause of action, as defined in Civil Code § 56.05(k).

392. Plaintiffs and California Class Members provided their PII and PHI to Defendants.

393. At all relevant times, Defendants collected, stored, managed, and transmitted Plaintiffs' and California Class Members' personal medical information.

394. Section 56.10(a) of the California Civil Code provides that "[a] provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization."

395. As a result of the Data Breach, Defendants misused, disclosed, and/or allowed third parties to access and view Plaintiffs' and California Class Members' personal medical information without their written authorization compliant with the provisions of Civil Code §§ 56, *et seq*.

396. As a further result of the Data Breach, the confidential nature of the Plaintiffs' and California Class Members' medical information was breached as a result of Defendant's negligence. Specifically, Defendants knowingly allowed and affirmatively acted in a manner that actually allowed unauthorized parties to access, view, and use Plaintiffs' and California Class Members' PHI.

397. Defendants' misuse and/or disclosure of medical information regarding Plaintiffs and California Class Members constitutes a violation of Civil Code §§ 56.10, 56.11, 56.13, and 56.26.

398. As a direct and proximate result of Defendants' wrongful actions, inaction, omissions, and want of ordinary care, Plaintiffs' and California Class Members' personal medical information was disclosed without written authorization.

399. By disclosing Plaintiffs' and California Class Members' PII and PHI without their written authorization, Defendants violated California Civil Code § 56, *et seq*., and their legal duties to protect the confidentiality of such information.

400. Defendants also violated Sections 56.06 and 56.101 of the California CMIA, which prohibit the negligent creation, maintenance, preservation, storage, abandonment, destruction, or disposal of confidential personal medical information.

401. As a direct and proximate result of Defendants' wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiffs' and California Class Members' personal medical information was viewed by, released

to, and disclosed to third parties without Plaintiffs' and California Class Members' written authorization.

402. As a direct and proximate result of Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and its violations of the CMIA, Plaintiffs and California Class Members are entitled to (i) actual damages, (ii) nominal damages of $1,000 per Plaintiffs and California Class Member, (iii) punitive damages of up to $3,000 per Plaintiff and California Class Member, and (iv) attorneys' fees, litigation expenses and court costs under California Civil Code § 56.35.

## COUNT VIII

**California's Unfair Competition Law**
**Cal. Bus. & Prof. Code §§ 17200, *et seq.*—Unlawful Business Practices**
**(On behalf of California Plaintiffs and the California Class)**

403. Plaintiffs and the Nationwide Class or, alternatively, California Plaintiffs and the California Class, re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 299.

404. Defendants have violated Cal. Bus. and Prof. Code §§ 17200, *et seq.*, by engaging in unlawful, unfair, or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in Cal. Bus. Prof. Code § 17200 with respect to the services provided to the Nationwide Class.

405. Defendants engaged in unlawful acts and practices with respect to their services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiffs' and the Nationwide Class's PII and PHI with knowledge that the information would not be adequately protected; and by storing Plaintiffs' and the Nationwide Class's PII and PHI in an unsecure electronic environment in violation of California's data breach statute, Cal.

Civ. Code § 1798.81.5, which requires Defendants to implement and maintain reasonable security procedures and practices to safeguard the PII and PHI of Plaintiffs and the Nationwide Class. Defendants also violated: the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100, *et seq*. and the California Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq*.; and also, the California Financial Information Privacy Act, Cal. Fin. Code § 4052.5; the Graham Leach Bliley Act Privacy Rule, 16 C.F.R. Part 313, and Reg. P, 12 C.F.R. Part 1016; and Article 1, § 1 of the California Constitution.

406. In addition, Defendants engaged in unlawful acts and practices by failing to disclose the data breach to the Nationwide Class in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82. To date, Defendants still have not provided such information to Plaintiffs and the Nationwide Class.

407. As a direct and proximate result of Defendants' unlawful practices and acts, Plaintiffs and the Nationwide Class were injured and lost money or property, including but not limited to the price received by Defendants for the services, the loss of the Nationwide Class's legally protected interest in the confidentiality and privacy of their PII and PHI, nominal damages, and additional losses as described above.

408. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard Plaintiffs' and the Nationwide Class's PII and PHI and that the risk of a data breach or theft was highly likely. Defendants' actions in engaging in the above-named unlawful practices and acts were negligent, knowing, and willful, and/or wanton and reckless with respect to the rights of members of Plaintiffs and the Nationwide Class.

409. Plaintiffs and the Nationwide Class seek relief under Cal. Bus. & Prof. Code § 17200, *et seq*., including, but not limited to, restitution to Plaintiffs and the Nationwide Class of

money or property that Defendants may have acquired by means of their unlawful, and unfair business practices, restitutionary disgorgement of all profits accruing to Defendants because of their unlawful and unfair business practices, declaratory relief, attorneys' fees and costs, and injunctive or other equitable relief.

## COUNT IX

**California's Unfair Competition Law**
**Cal. Bus. & Prof. Code §§ 17200, *et seq.*—Unfair Business Practices**
**(On behalf of Plaintiffs and the Nationwide Class or,**
**Alternatively, California Plaintiffs and the California Class)**

410. Plaintiffs and the Nationwide Class or, alternatively, California Plaintiffs and the California Class, re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 299.

411. Defendants engaged in unfair acts and practices by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiffs' and the Nationwide Class's PII and PHI with knowledge that the information would not be adequately protected; and by storing Plaintiffs' and the Nationwide Class's PII and PHI in an unsecure electronic environment. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and the Nationwide Class. They were likely to deceive the public into believing their PII and PHI was securely stored when it was not. The harm these practices caused to Plaintiffs and the Nationwide Class outweighed their utility, if any.

412. Defendants engaged in unfair acts and practices with respect to the provision of services by failing to take proper action following the data breach to enact adequate privacy and security measures and protect Plaintiffs' and the Nationwide Class's PII and PHI from further unauthorized disclosure, release, data breaches, and theft. These unfair acts and practices were

immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and the Nationwide Class. They were likely to deceive the public into believing their PII and PHI was securely stored, when it was not. The harm these practices caused to Plaintiffs and the Nationwide Class outweighed their utility, if any.

413. As a direct and proximate result of Defendants' acts of unfair practices, Plaintiffs and the Nationwide Class were injured and lost money or property, including but not limited to the price received by Defendants for the services, the loss of Plaintiffs' and the Nationwide Class's legally protected interest in the confidentiality and privacy of their PII and PHI, nominal damages, and additional losses as described above.

414. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard Plaintiffs' and the Nationwide Class's PII and PHI and that the risk of a data breach or theft was highly likely. Defendants' actions in engaging in the above-named unlawful practices and acts were negligent, knowing, and willful, and/or wanton and reckless with respect to the rights of Plaintiffs and the Nationwide Class.

415. Plaintiffs and the Nationwide Class seek relief under Cal. Bus. & Prof. Code §§ 17200, *et seq*., including, but not limited to, restitution to Plaintiffs and the Nationwide Class of money or property that the Defendants may have acquired by means of their unfair business practices, restitutionary disgorgement of all profits accruing to Defendants because of their unfair business practices, declaratory relief, attorneys' fees and costs, and injunctive or other equitable relief.

## COUNT X

**Violations of the Illinois Consumer Fraud and Deceptive Business Practices Act ("CFA"), 815 Ill. Comp. Stat. §§ 505/1, *et seq*.**
**(On Behalf of Plaintiff Kroll and the Illinois Class)**

416. Plaintiff Kroll and the Illinois Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 299.

417. Plaintiff Kroll and the Illinois Class are "consumers" as defined in 815 Ill. Comp. Stat. § 505/1(e). Plaintiff Kroll, the Illinois Class, and Defendants are "persons" as defined in 815 Ill. Comp. Stat. § 505/1(c).

418. Defendants are engaged in "trade" or "commerce," including the provision of services, as defined under 815 Ill. Comp. Stat. § 505/1(f). Defendants engage in the sale of "merchandise" (including services) as defined by 815 Ill. Comp. Stat. §§ 505/1(b) and (d).

419. Defendants engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment and omission of material facts in connection with the sale and advertisement of their services in violation of the CFA, including: (1) failing to maintain adequate data security to keep Plaintiff Kroll's and the Illinois Class's sensitive PII and PHI from being stolen by cybercriminals and failing to comply with applicable state and federal laws and industry standards pertaining to data security, including the FTC Act; (2) failing to disclose or omitting materials facts to Plaintiff Kroll and the Illinois Class regarding their lack of adequate data security and inability or unwillingness to properly secure and protect the PII and PHI of Plaintiff Kroll and the Illinois Class; (3) failing to disclose or omitting materials facts to Plaintiff Kroll and the Illinois Class about Defendants' failure to comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the PII and PHI of Plaintiff Kroll and the Illinois Class; and (4) failing to take proper action following the Data Breach to enact adequate privacy and

security measures and protect Plaintiff Kroll and the Illinois Class's PII and PHI and other personal information from further unauthorized disclosure, release, data breaches, and theft.

420. These actions also constitute deceptive and unfair acts or practices because Defendants knew the facts about their inadequate data security and failure to comply with applicable state and federal laws and industry standards would be unknown to and not easily discoverable by Plaintiff Kroll and the Illinois Class and defeat their reasonable expectations about the security of their PII and PHI.

421. Defendants intended that Plaintiff Kroll and the Illinois Class rely on its deceptive and unfair acts and practices and the concealment and omission of material facts in connection with Defendants' offering of goods and services.

422. Defendants' wrongful practices were and are injurious to the public because those practices were part of Defendants' generalized course of conduct that applied to the Illinois Class. Plaintiff Kroll and the Illinois Class have been adversely affected by Defendants' conduct and the public was and is at risk as a result thereof.

423. Defendants also violated 815 ILCS 505/2 by failing to immediately notify Plaintiff Kroll and the Illinois Class of the nature and extent of the Data Breach pursuant to the Illinois Personal Information Protection Act, 815 ILCS 530/1, *et seq*.

424. As a result of Defendants' wrongful conduct, Plaintiff Kroll and the Illinois Class were injured in that they never would have provided their PII and PHI to Defendants, or purchased Defendants' services, had they known or been told that Defendants failed to maintain sufficient security to keep their PII and PHI from being hacked and taken and misused by others.

425. As a direct and proximate result of Defendants' violations of the CFA, Plaintiff Kroll and the Illinois Class have suffered harm, including actual instances of identity theft; loss of

time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the payments or services made to Defendants or Defendants' customers that Plaintiff Kroll and the Illinois Class would not have made had they known of Defendants' inadequate data security; lost control over the value of their PII and PHI; unreimbursed losses relating to fraudulent charges; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen PII and PHI, entitling them to damages in an amount to be proven at trial.

426. Pursuant to 815 Ill. Comp. Stat. § 505/10a(a), Plaintiff Kroll and the Illinois Class seek actual and compensatory damages, injunctive relief, and court costs and attorneys' fees as a result of Defendants' violations of the CFA.

## COUNT XI

**Violation of the Louisiana Database Security Breach Notification Law, La. Rev. Stat. Ann. §§ 51:3074(A), *et seq.* (On Behalf of Plaintiff Parsons and the Louisiana Class)**

427. Plaintiff Parsons and the Louisiana Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 299.

428. Defendants are businesses that own or license computerized data that includes personal information as defined by La. Rev. Stat. Ann. § 51:3073(4)(a).

429. Plaintiff Parsons's and the Louisiana Class's PII and PHI include personal information as defined by La. Rev. Stat. Ann. § 51:3073(4)(a) and as covered by La. Rev. Stat. Ann. § 51:3074(C).

430. Defendants are required to accurately notify Plaintiff Parsons and the Louisiana Class if they become aware of a breach of their data security system that was reasonably likely to have caused unauthorized persons to acquire Plaintiff Parsons' and the Louisiana Class's personal

information in the most expedient time possible and without unreasonable delay under La. Rev. Stat. Ann. § 51:3074(D).

431. Because Defendants were aware of a breach of their security system that was reasonably likely to have caused unauthorized persons to acquire Plaintiff Parsons's and the Louisiana Class's personal information, Defendants had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by La. Rev. Stat. Ann. § 51:3074(D).

432. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated La. Rev. Stat. Ann. § 51:3074(D).

433. As a direct and proximate result of Defendants' violations of La. Rev. Stat. Ann. § 51:3074(D), Plaintiff Parsons and the Louisiana Class suffered damages, as described above.

434. Plaintiff Parsons and the Louisiana Class seek all monetary and non-monetary relief allowed by law under La. Rev. Stat. Ann. § 51:3075, including actual damages and any other relief that is just and proper.

## COUNT XII

**Violations of the Maryland Consumer Protection Act,**
**Md. Comm. Code §§ 13-301, *et seq*.**
**(On behalf of Maryland Plaintiffs and the Maryland Class)**

435. Maryland Plaintiffs and the Maryland Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 299.

436. Maryland Plaintiffs and the Maryland Class are "consumers" under Md. Comm. Code § 13-101(c).

437. Defendants are "persons" under Md. Comm. Code § 13-101(h) and offer, advertise, or sell "consumer services" as defined in Md. Comm. Code § 13-101(d).

438. Defendants engaged in the acts and omissions alleged herein in the state of Maryland.

439. Defendants engaged in unfair and deceptive acts and practices in violation of the Maryland Consumer Protection Act, including failing to state a material fact where the failure deceives or tends to deceive, advertising or offering consumer goods or services without the intent to sell or provide them as advertised, and misrepresentation, concealment, suppression, or omission of a material fact with the intent that a consumer rely on the same in connection with the sale of consumer services or the subsequent performance with respect to an agreement, sale, lease, or rental.

440. Defendants engaged in these acts or omissions by failing to comply with common law and statutory requirements for adequate data security, including Section 5 of the FTC Act and the Maryland Personal Information Protection Act, Md. Comm. Code § 14-3503.

441. Maryland Plaintiffs and the Maryland Class acted reasonably in relying on Defendants' misrepresentations and omissions, described fully, *supra*, the truth of which they could not have discovered.

442. As a result of Defendants' unfair and deceptive acts and practices, Maryland Plaintiffs and the Maryland Class have suffered and will continue to suffer injury, losses of money or property, and monetary and non-monetary damages as alleged more fully above.

443. Maryland Plaintiffs and the Maryland Class seek all relief allowed under law for these violations, including damages, disgorgement, injunctive relief, and attorneys' fees and costs.

## COUNT XIII

**Violations of the Maryland Personal Information Protection Act,**
**Md. Code Ann. §§ 14-3501, *et seq.***
**(On behalf of Maryland Plaintiffs and the Maryland Class)**

444. Maryland Plaintiffs and the Maryland Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 299.

445. Under the Maryland Personal Information Protection Act ("MPIPA"), Md. Code Ann., Com. Law § 14-3503(a), "[t]o protect Personal Information from unauthorized access, use, modification, or disclosure, a business that owns or licenses Personal Information of an individual residing in the State shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of Personal Information owned or licensed and the nature and size of the business and its operations."

446. Defendants are businesses that own or license computerized data that includes Personal Information as defined by Md. Code Ann., Com. Law § 14-3501(b)(1).

447. Maryland Plaintiffs and the Maryland Class are "individuals" and "customers" as defined in Md. Code Ann., Com. Law §§ 14-3502(a) and 14-3503.

448. Maryland Plaintiffs' and the Maryland Class's Personal Information includes "[h]ealth information" and "[p]ersonal information" as covered under Md. Code Ann., Com. Law §§ 14-3501(d)-(e).

449. Defendants did not maintain reasonable security procedures and practices appropriate to the nature of the Personal Information owned or licensed and the nature and size of its business and operations in violation of Md. Code Ann., Com. Law § 14-3503.

450. The Data Breach was a "breach of the security system" as defined by Md. Code Ann., Com. Law § 14-3504(1).

451. Under Md. Code Ann., Com. Law § 14-3504(b)(1), "[a] business that owns or licenses computerized data that includes Personal Information of an individual residing in the State, when it discovers or is notified of a breach of the security system, shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that Personal Information of the individual has been or will be misused as a result of the breach."

452. Under Md. Code Ann., Com. Law §§ 14-3504(b)(2) and 14-3504(c)(2), "[i]f, after the investigation is concluded, the business determines that the breach of the security of the system creates a likelihood that personal information has been or will be misused, the owner or licensee of the computerized data shall notify the individual of the breach" and that notification "shall be given as soon as reasonably practical but not later than 45 days after the business discovers or is notified of the breach of a security system."

453. Because Defendants discovered a security breach and had notice of the security breach, Defendants had an obligation to disclose the security data breach in a timely and accurate fashion as mandated by Md. Code Ann., Com. Law §§ 14-3504(b)(2) and 14-3504(c)(2).

454. After discovering the Data Breach, Defendants, waited more than nine months before notifying Maryland Plaintiffs and the Maryland Class. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated Md. Code Ann., Com. Law §§ 14-3504(b)(2) and 14-3504(c)(2).

455. As a direct and proximate result of Defendants' violations of Md. Code Ann., Com. Law §§ 14-3504(b)(2) and 14-3504(c)(2), Maryland Plaintiffs and the Maryland Class have suffered and will continue to suffer damages.

456. Pursuant to Md. Code Ann., Com. Law § 14-3508, Defendants' violations of Md. Code Ann., Com. Law §§ 14-3504(b)(2) and 14-3504(c)(2) are unfair or deceptive trade practices within the meaning of the Maryland Consumer Protection Act (codified at Md. Code Ann., Com. Law §§ 13-301, *et seq.*) ("CPA") and are subject to the enforcement and penalty provisions contained within the CPA.

457. Maryland Plaintiffs and the Maryland Class seek relief under Md. Code Ann., Com. Law § 14-3508, including actual damages and attorneys' fees.

## COUNT XIV

**Violation of the New Hampshire Consumer Protection Act ("NHCPA")**
**N.H. R.S.A. §§ 358-A, *et seq*.**
**(On Behalf of Plaintiff Jonathan Mitchel and the New Hampshire Class)**

458. Plaintiff Mitchell re-alleges and incorporates by reference paragraphs 1-299 as if fully set forth herein.

459. Defendants are considered a "person" under NHCPA. N.H. R.S.A. § 358-A:1(I).

460. NHCPA prohibits a person or entity from:

> [Using] any unfair method of competition or any unfair or deceptive act or practice in the conduct of any trade or commerce within this state.

N.H. R.S.A. § 358-A:2.

461. The New Hampshire statutory scheme provides a non-exhaustive list of acts that constitute violations of the statute, which includes but is not limited to the following:

a. "Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have or that a person has a sponsorship, approval, status, affiliation, or connection that such person does not have[.]" N.H. R.S.A. § 358-A:2(V).

b. "Representing that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another[.]" N.H. R.S.A. § 358-A:2(VII).

c. "Advertising goods or services with intent not to sell them as advertised[.]" N.H. R.S.A. § 358-A:2(IX).

462. The New Hampshire Supreme Court has held that conduct that is not specifically delineated within the statutory scheme is analyzed under the "rascality test." *Axenics v. Turner Const. Co.*, 164 N.H. 659, 675 (2013).

463. Defendants engaged in the conduct alleged in this complaint through transactions in and involving trade and commerce within the State of New Hampshire. N.H. R.S.A. § 358-A:2.

464. While involved in trade or commerce, Defendants violated the NHCPA by engaging in unfair, deceptive, and unconscionable business practices including, among other things, by:

a. Failing to implement and maintain appropriate and reasonable security procedures and practices to safeguard and protect the Private Information of Defendant's client patients from unauthorized access and disclosure;

b. Failing to disclose the material fact that its computer systems and data security practices were inadequate to safeguard and protect the Private Information of Defendants' client patients from being compromised, stolen, lost, or misused; and

c. Failing to disclose the Data Breach to Defendants' client patients "as soon as possible" in violation of N.H. R.S.A. § 359-C:20(I)(a).

465. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard Class Members' Private Information entrusted to it, and that risk of a data breach or theft was highly likely.

466. Defendants should have disclosed this information because Defendants were in a superior position to know the true facts related to the defective data security.

467. Defendants' failures constitute an unfair practice and false, deceptive, and misleading representations regarding the security of Defendants' network and aggregation of Private Information.

468. These unfair practices and misleading representations upon which impacted individuals (including Plaintiffs and Class Members) relied were material facts (*e.g.*, as to Defendants' adequate protection of Private Information), and consumers (including Plaintiff and Class Members) relied on those representations to their detriment.

469. In committing the acts alleged in this amended complaint, Defendants engaged in fraudulent, deceptive, and unfair practices by omitting, failing to disclose, or inadequately disclosing to Plaintiff and Class Members that they did not follow industry best practices for the collection, use, and storage of PII and PHI.

470. Defendants' conduct as described in this complaint constitutes willful and/or knowing violations of the NHCPA.

471. As a direct and proximate result of Defendants' conduct, Plaintiff and other Members of the Class have been harmed and have suffered damages including, but not limited to: damages arising from attempted identity theft and fraud; out-of-pocket expenses associated with procuring identity protection and restoration services; increased risk of future identity theft and fraud, and the costs associated therewith; and time spent monitoring, addressing and correcting the current and future consequences of the Data Breach.

472. As a direct and proximate result of Defendants' fraudulent, deceptive, and unfair practices and omissions, Plaintiff's and Class Members' Private Information was disclosed to third parties without authorization, causing and will continue to cause Plaintiff and Class Members damages. Accordingly, Plaintiff and Class Members are entitled to recover damages in accordance with the NHCPA, an order providing declaratory and injunctive relief, and reasonable attorneys' fees and costs.

## COUNT XV

**Violation of New Hampshire Notice of security Breach**
**N.H. R.S.A. §§ 359-C:20(I)(a), *et seq*.**
**(On Behalf of Plaintiff Johnathon Mitchell and the New Hampshire Class)**

473. Plaintiff re-alleges and incorporates by reference paragraphs 1-299 as if fully set forth herein.

474. The New Hampshire Notice of Security Breach statute states that:

> Any person doing business in this state who owns or licenses computerized data that includes personal information shall, when it becomes aware of a security breach, promptly determine the likelihood that the information has been or will be misused. If the determination is that misuse of the information has occurred or is reasonably likely to occur, or if a determination cannot be made, the person shall notify the affected individuals as soon as possible as required [.]

N.H. R.S.A. § 359-C:20(I)(a).

475. Defendants are businesses that own or license computerized data that includes Personal Information, of Plaintiff and Members of the Class, as defined by N.H. Rev. Stat. Ann. § 359-C:20(I)(a).

476. Plaintiff's and Class Members' Personal Information (*e.g.*, a person's first and last name, and their Social Security number) includes Personal Information as covered under N.H. Rev. Stat. Ann. § 359-C:19(IV)(a)

477. Defendants acted as a licensee of the sensitive PII and PHI in using it to administer claims and by storing this valuable and highly sensitive information on their computer systems and network.

478. The Data Breach occurred in June of 2020, yet shockingly Defendants only began to send out notice to victims of the breach in June of, 2021, approximately one year later.

479. Per New Hampshire Statute § 359-C:20(I)(a), Defendants were required to "notify

the affected individuals as soon as possible[.]" Though Plaintiff's and Class Member's personal information was included in the breach and compromised, Defendants failed to send the requisite notice under New Hampshire law.

480. Because Defendants were aware of the breach of security of its systems, Defendants had an obligation to disclose the Data Breach "as soon as possible."

481. In failing to timely disclose the Data Breach, Plaintiff the Class Members were harmed because they were not able to immediately take precautionary action to prevent and mitigate the effects of identity theft and financial fraud.

482. By failing to disclose the Data Breach in a timely and reasonable manner, Defendants violated New Hampshire Statute § 359-C:20(I)(a).

483. As a direct and proximate result of Defendants' violation of the notice requirement under N.H. R.S.A. § 359-C:20(I)(a), Plaintiff and Class Members suffered the above-mentioned damages. Accordingly, Plaintiff and Class Members are entitled to recover actual damages, injunctive relief, and reasonable attorneys' fees and costs, to the extent permitted by law.

## COUNT XVI

### Violation of Colorado's Data Security Laws, Colo. Rev. Stat. § 6-1-713.5 (On Behalf of Plaintiff Chandra Wilson and the Colorado Class)

484. Plaintiff Wilson re-alleges and incorporates by reference Paragraphs 1 through 299 above as if fully set forth herein.

485. Plaintiff brings this claim on behalf of herself and the Colorado Class.

486. Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach.

487. Colo. Rev. Stat. § 6-1-713.5 requires commercial entities who maintain, own, or license "personal identifying information of an individual residing in the state" to "implement and

maintain reasonable security procedures and practices that are appropriate to the nature of the personal identifying information and the nature and size of the business and its operations."

488. Defendants' conduct violated Colo. Rev. Stat. § 6-1-713.5. Specifically, Defendants voluntarily undertook the act of maintaining and storing Plaintiff's and Class Members' PII and PHI, but Defendant failed to implement safety and security procedures and practices sufficient enough to protect from the data breach that it should have anticipated. Defendants should have known and anticipated that data breaches—especially health data—were on the rise, and that medical institutions were lucrative or likely targets of cybercriminals looking to steal PII. Correspondingly, Defendants should have implemented and maintained procedures and practices appropriate to the nature and scope of information compromised in the data breach.

489. As a result of Defendants' violation of Colo. Rev. Stat. § 6-1-716, Plaintiff and the Class Members incurred economic damages, including expenses associated with necessary credit monitoring.

490. Accordingly, Plaintiff, individually and on behalf of the Colorado Class, respectfully request this Court award all relevant damages.

## COUNT XVII

### Violation of Colorado's Security Breach Notification Laws, Colo. Rev. Stat. § 6-1-716 (On Behalf of Plaintiff Chandra Wilson and All Class Members)

491. Plaintiff Wilson re-alleges and incorporates by reference Paragraphs 1 through 299 above as if fully set forth herein.

492. Plaintiff brings this claim on behalf of herself and the Colorado Class.

493. Defendants' conduct violated Colo. Rev. Stat. § 6-1-716, which requires commercial entities to notify individuals within 30 days of a security that involves personal information.

494. The Data Breach occurred in June of 2020. Defendants claim they did not discover the breach until September of 2020. However, Defendants still did not give notice of the Data Breach until at least June of 2021.

495. Defendants unreasonably delayed informing anyone about the breach of security of Plaintiff's and the Class Members' confidential and non-public information after Defendants knew the Data Breach had occurred.

496. Defendants failed to disclose to Plaintiff or the Class Members, without unreasonable delay, and in the most expedient time possible, the breach of security of their unencrypted—or not properly and securely encrypted—PII and PHI when it knew or reasonably believed such information had been compromised.

497. As a result of Defendants' violation of Colo. Rev. Stat. § 6-1-716, Plaintiff and the Class Members incurred economic damages, including expenses associated with necessary credit monitoring.

498. Accordingly, Plaintiff, individually and on behalf of the Colorado Class, respectfully requests this Court award all relevant damages.

## COUNT XVIII

**Invasion of Privacy**
**(On Behalf of Plaintiffs and the Nationwide Class, or alternatively, the Subclasses)**

499. Plaintiffs and Classes re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 299.

500. Plaintiffs and Class Members had a legitimate expectation of privacy to their PII and PHI and were entitled to the protection of this information against disclosure to unauthorized third parties.

501. Defendants owed a duty to Plaintiffs and Class Members to keep their PII and PHI contained as a part thereof, confidential.

502. Defendants failed to protect and released to unknown and unauthorized third parties the non-redacted and non-encrypted PII and PHI of Plaintiffs and Class Members.

503. Defendants allowed unauthorized and unknown third parties access to and examination of the PII and PHI of Plaintiffs and Class Members, by way of Defendants' failure to protect the PII and PHI.

504. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII and PHI of Plaintiffs and Class Members is highly offensive to a reasonable person.

505. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs and Class Members disclosed their PII and PHI to Defendants as part of their relationships with Defendants, but privately with an intention that the PII and PHI would be kept confidential and would be protected from unauthorized disclosure. Plaintiffs and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

506. The Data Breach at the hands of Defendants constitutes an intentional interference with Plaintiffs' and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

507. Defendants acted with a knowing state of mind when it permitted the Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

508. Because Defendants acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiffs and Class Members.

509. As a proximate result of the above acts and omissions of Defendants, the PII and PHI of Plaintiffs and Class Members was disclosed to third parties without authorization, causing Plaintiffs and Class Members to suffer damages.

510. Unless and until enjoined, and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members in that the PII and PHI maintained by Defendants can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiffs and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and Class Members.

## PRAYER FOR RELIEF

**WHEREFORE**, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Nationwide Class, the California Class, the Illinois Class, the Louisiana Class, and the Maryland Class and appointing Plaintiffs, California Plaintiffs, Illinois Plaintiffs, Louisiana Plaintiffs, and Maryland Plaintiffs and their Counsel to represent each such Class;

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

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

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

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

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

v. prohibiting Defendants from maintaining the PII and PHI of Plaintiffs and Class Members on a cloud-based database;

vi. requiring Defendants 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 Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendants to engage independent third-party security auditors and

internal personnel to run automated security monitoring;

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

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

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

xi. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

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

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

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

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

xvi. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' 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 Defendants' 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 actual, consequential, statutory, and nominal damages, as allowed by law in an amount to be determined;

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

F. For prejudgment interest on all amounts awarded; and

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

**DEMAND FOR JURY TRIAL**

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

Date: October 29 2021

Respectfully Submitted,

*/s/ Gary M. Klinger*

Gary M. Klinger
**MASON LIETZ & KLINGER, LLP**
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (202) 975-0477
Facsimile: (202) 429-2290
gklinger@masonllp.com

M. Anderson Berry
**CLAYEO C. ARNOLD, A PROFESSIONAL LAW CORP.**
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916)777-7777
Facsimile: (916) 924-1829
aberry@justice4you.com

***Interim Class Counsel***

Rachele R. Byrd
**WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP**
750 B Street, Suite 1820
San Diego, CA 92101
Telephone: (619) 239-4599
Facsimile: (619) 234-4599
byrd@whafh.com

Carl Malmstrom
**WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP**
111 W. Jackson Blvd., Suite 1700
Chicago, IL 60604
Telephone: (312) 984-0000
Facsimile: (212) 545-4653
malmstrom@whafh.com

Robert A. Clifford
Shannon M. McNulty
**CLIFFORD LAW OFFICES**
120 N. LaSalle Street, Suite 3100
Chicago, IL 60602

Telephone: (312) 899-9090
rac@cliffordlaw.com
smm@cliffordlaw.com

John A. Yanchunis*
Ryan D. Maxey*
**MORGAN & MORGAN COMPLEX BUSINESS DIVISION**
201 N. Franklin Street, 7th Floor
Tampa, FL33602
Telephone: (813) 223-5505
jyanchunis@ForThePeople.com
rmaxey@ForThePeople.com

David K. Lietz
**MASON LIETZ & KLINGER LLP**
5101 Wisconsin Avenue NW, Suite 305
Washington, D.C. 20016
Telephone: (212) 429-2290
Facsimile: (202) 429-2294
dlietz@masonllp.com

Nathan D. Prosser
**HELLMUTH & JOHNSON, PLLC**
8050 West 78th Street
Edina, MN 55439
Telephone: (952)941-4005
Facsimile: (952) 941-2337
nprosser@hjlawfirm.com

Terence R. Coates
**MARKOVITS, STOCK & DEMARCO, LLC**
3825 Edwards Road, Suite 650
Cincinnati, OH 45209
Telephone: (513) 651-3700
Facsimile: (513) 665-0219
tcoates@msdlegal.com

Bryan L. Bleichner
**CHESTNUT CAMBRONNE PA**
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Telephone: (612) 339-7300
Facsimile: (612) 336-2940
bbleichner@chestnutcambronne.com

Joseph Lyon (OH-0076050)
**THE LYON FIRM, LLC**
2754 Erie Ave
Cincinnati, Ohio 45208
Telephone: (513) 381-2333
jlyon@thelyonfirm.com

***Additional Class Counsel***

**pro hac vice applications forthcoming*

**CERTIFICATE OF SERVICE**

I hereby certify that on October 29, 2021, I filed the foregoing CONSOLIDATED CLASS ACTION COMPLAINT with the Clerk of the Court for the U.S. District Court for the Northern District of Illinois via the Court's CM/ECF system. A copy will be sent electronically to all counsel of record by operation of the ECF system.

*/s/ Gary M. Klinger*
Gary M. Klinger