UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA

Craig Pederson and David Brown, ***on behalf of themselves and all others similarly situated,*** **Plaintiffs,** **v.** **AAA Collections, Inc.,** **Defendant.**	4:22-CV-04166-RAL JURY TRIAL DEMANDED

AMENDED CLASS ACTION COMPLAINT

Plaintiffs Craig Pederson and David Brown ("Plaintiffs") bring this Amended Class Action Complaint against AAA Collections, Inc. ("AAA" or "Defendant"), 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:

1. Defendant AAA is a third-party collection and debt resolution services company located in Sioux Falls, South Dakota.

2. Plaintiffs bring this class action against AAA for its failure to properly secure and safeguard personally identifiable information ("PII"), including full names, addresses, phone numbers, dates of birth, payment history, Social Security numbers, financial information, and for the patients of medical providers, protected health information ("PHI"), including medical record numbers, medical provider or facility names; medical conditions, diagnoses, treatment

information, insurance payment information, and dates of service (collectively, PII and PHI are "Private Information").

3. From September 5, 2022 until September 7, 2022, an unauthorized third party had unfettered access to AAA's network and exfiltrated documents containing Plaintiffs' and Class Members' Private Information (the "Data Breach").

4. Despite learning of the Data Breach on September 7, 2022, Defendant did not begin notifying victims like Plaintiff Pederson until on or around November 16, 2022. Other Class Members, like Plaintiff Brown, were not sent notice of the Data Breach until on or after December 15, 2022.

5. Defendant has disclosed that the Data Breach exposed the sensitive Private Information of 56,848 individuals.

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

7. The unencrypted, unredacted Private Information of Plaintiffs and Class Members likely has been—and will continue to be—sold to criminals on the dark web. 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.

8. This PII was compromised due to Defendant's negligent and/or reckless conduct. In addition to Defendant's failure to prevent the Data Breach, after discovering the breach, Defendant waited an unreasonable amount of time to notify victims of the Data Breach.

9. Plaintiffs bring this action on behalf of all persons whose Private Information was compromised as a result of Defendant's failure to: (i) adequately protect the Private Information

of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendant's inadequate information security practices; (iii) effectively secure hardware and software containing Private Information using reasonable, effective security procedures free of vulnerabilities and incidents; and (iv) properly train employees and agents to recognize and avoid foreseeable social engineering hacking techniques. Defendant's conduct violates federal and state law.

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

11. Defendant 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 Private Information 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 Private Information of Plaintiffs and Class Members was compromised through disclosure to an 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.

PARTIES

Plaintiffs Craig Pederson and David Brown

12. Plaintiff Craig Pederson is a natural person and citizen of South Dakota, residing in Madison, South Dakota, where he intends to remain.

13. Plaintiff, David Brown is a natural person and citizen of Minnesota, residing in Staples, Minnesota, where he intends to remain.

Defendant AAA Collections, Inc.

14. Defendant AAA Collections, Inc., which also does business as Advanced Asset Alliance, Inc., is a company incorporated under the laws of South Dakota and headquartered at 3500 S. 1st Ave Cir, Suite #100, Sioux Falls, South Dakota 57105.

JURISDICTION AND VENUE

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

16. This Court has personal jurisdiction over Defendant because its principal place of business is in this District and the acts and omissions giving rise to Plaintiffs' claims occurred in and emanated from this District.

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

FACTUAL ALLEGATIONS

Background

18. AAA most commonly does business under the names "Advanced Asset Alliance" or "AAA Collections." However, it also does business under the names "Accounts Receivable Management Group," "Credit Management Services," and "Guardian."

19. According to AAA, it is a "collection of accounts receivable management companies that specialize in the accelerated recovery of accounts receivable."[1] AAA states that it "partner[s] with clients of all sizes from industries of all types."[2]

20. AAA provides services to thousands of clients nationwide, including several medical providers. AAA generates millions of dollars in revenue every year collecting consumer debts on behalf of their clients.

AAA Collects and Maintains Private Information in the Ordinary Course of Business

21. In the ordinary course of business, AAA collects the Private Information of its clients' customers and patients. This information is provided to Defendant by its clients for use in collecting debts. Defendant often receives information and payments directly from Class Members as well. For example, Defendant provides an online payment portal that encourages Class Members to submit, *inter alia*, their name, contact information, payment information, and Social Security numbers as a form of "payment reference."[3]

22. The Private Information collected and maintained includes, upon information and belief, full names, dates of birth, Social Security numbers, phone numbers, addresses, email addresses, account numbers, original creditor information, current creditor information, balances,

[1] https://www.aaa-coll.com/our-history (last visited February 19, 2023).
[2] *Id.*
[3] https://consumer.aaa-coll.com/Authorize/ (last visited February 23, 2023).

and payment history. Where the debtor is a patient, the information collected and maintained also includes provider or facility name, condition, diagnosis and/or treatment information, payment amount history information, insurance payment amount information and date of service.

23. AAA promises clients and those clients' customers or patients that it will safeguard that data from theft and misuse using reasonable security measures. Such representations include, but are not limited to, statements on AAA's website that it will "treat [its] clients' customers and patients with the dignity and respect they deserve while zealously safeguarding their information."[4]

24. AAA's website's terms and conditions demonstrate AAA's recognition of the risk it faces from external threat actors. For example, AAA's policy is that it will not communicate with customers via email, stating:

> E-mail posted or sent through this website may not be secure against interception by unauthorized individuals. To protect against interception by unauthorized individuals, we will not respond to e-mail requests concerning accounts placed for collection. Therefore, if you are communicating with [AAA] regarding a debt that has been placed for collection with [AAA], all correspondence regarding that account should be sent by U.S. Postal Service.

25. AAA's website terms and conditions further state that,

> [AAA] has implemented physical, electronic, and procedural security safeguards to protect against the unauthorized release of or access to personal information. Additionally, to further safeguard this information, our employees are asked to agree to [AAA's] Standards of Conduct and Work Rules as well as Confidentiality Agreements, and are subject to disciplinary action up to and including termination of employment if they fail to follow signed agreements.

26. According to Defendant's own admissions, the Data Breach involved Private Information that was stored on Defendant's internal systems, as discussed below. AAA understood its obligations to protect this information, as evidenced in part by letters sent to victims after the

[4] https://client.aaa-coll.com/Home/AAA (last visited February 19, 2023).

Data Breach, which stated that "The confidentiality, privacy, and security of information within our care are among AAA's highest priorities."

27. Plaintiffs, Class Members, and Defendant's clients relied on Defendant to implement and follow adequate data security policies and protocols, to keep their Private Information confidential and securely maintained, to use such Private Information solely for business purposes, and to prevent the unauthorized disclosures of the Private Information. It is common sense that Plaintiffs and Class Members would not have voluntarily provided Private Information to Defendant and/or Defendant's clients without the mutual understanding that reasonable efforts would be used to secure Private Information.

The Data Breach

28. According to letters that AAA sent to state attorneys general, AAA learned on September 7, 2022 that it experienced a cyber event.[5] AAA then conducted an investigation, which determined that "certain documents stored within AAA's environment were copied from [its] system as part of the cyber incident between September 5, 2022, and September 7, 2022."[6]

29. According to the Notice of Data Event posted on AAA's website, the documents copied from its systems during the Data Breach included: names, addresses, phone numbers, dates of birth, payment history, and for the patients of medical providers, medical record numbers, medical provider or facility names; medical conditions, diagnoses, treatment information, insurance payment information, and dates of service.[7]

---

[5] *See, e.g.*, https://apps.web.maine.gov/online/aeviewer/ME/40/b853362c-e2c9-45be-ba1e-d91bf2610e29.shtml (last visited February 19, 2023). https://www.iowaattorneygeneral.gov/media/cms/11162022_AAA_Collections_Inc_22964BAC5CE6D.pdf (last visited February 19, 2023).

[6] *Id.*

[7] https://www.aaa-coll.com/assets/images/AAA-Website-Notice12.15.2022.pdf (last visited February 19, 2023).

30. The Notice of Data Event of AAA's website is misleading as AAA has also disclosed to state attorneys general that the Data Breach exposed Social Security numbers and financial account information.[8] The letter received by Plaintiff Pederson specifically referenced his Social Security number as well.

31. AAA has disclosed that in total, the Data Breach compromised the PII of 56,848 individuals.[9] According to a disclosure that AAA made to the Department of Health and Human Services Office of Civil Rights, 4,635 of these individuals had PHI impacted in addition to PII.[10]

32. AAA classified the Data Breach as an "External system breach (hacking)" on the reporting form that it provided to the Maine Attorney General.[11] This classification is commonly selected after a company has affirmatively provided hackers with access to their systems in response to foreseeable social engineering techniques like phishing. One example includes the recent Highmark Health data breach, which was caused by phishing and categorized on the Maine Attorney General website as "External system breach (hacking)."[12]

33. The other classifications on the reporting form that AAA could have selected, but did not, were: "loss or theft of device or media (computer, laptop, external hard drive, thumb drive, CD, tape, etc.)"; "internal system breach"; "insider wrongdoing"; "inadvertent disclosure"; and

---

[8] *See, e.g.*, https://apps.web.maine.gov/online/aeviewer/ME/40/b853362c-e2c9-45be-ba1e-d91bf2610e29.shtml (last visited February 19, 2023). https://www.iowaattorneygeneral.gov/media/cms/11162022_AAA_Collections_Inc_22964BAC5CE6D.pdf (last visited February 19, 2023).

[9] https://apps.web.maine.gov/online/aeviewer/ME/40/b853362c-e2c9-45be-ba1e-d91bf2610e29.shtml (last visited February 19, 2023).

[10] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited February 21, 2023).

[11] ttps://apps.web.maine.gov/online/aeviewer/ME/40/b853362c-e2c9-45be-ba1e-d91bf2610e29.shtml (last visited February 19, 2023).

[12] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/67bb2ced-9a70-4248-b728-68a92a56c860.shtml (last visited February 19, 2023); https://healthitsecurity.com/news/highmark-health-suffers-phishing-attack-300k-individuals-impacted (last visited February 19, 2023).

"other."[13]

34. AAA's clients recognize the impact that the Data Breach will have on their customers and patients. For example, Prairie Lakes Health Care System released a statement saying that it "understands the inconvenience or concern that this matter may cause and encourages affected individuals to remain vigilant, monitor accounts, and immediately report any suspicious activity or suspected misuse of personal information."[14] AAA did not notify these victims of the Data Breach until December 15, 2022.

35. Defendant similarly acknowledged the risk the Data Breach posed when notifying Plaintiffs and Class Members, instructing them to "remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors."

36. Independent experts have advised recipients of notice letters to "quickly work to protect themselves from any further harm."[15]

37. According to the notice letters that Defendant sent Plaintiffs and Class Members, Defendant has "taken additional steps to further enhance the security of our systems." However, Defendant does not explain what these additional steps are or why it believes they are sufficient. Moreover, this is too little too late. Such measures—which Defendant now recognizes as necessary—should have been implemented *before* the Data Breach.

The Data Breach Was Foreseeable

38. At all relevant times, Defendant knew, or reasonably should have known, of the

[13] https://appengine.egov.com/apps/me/maine/ag/reportingform (last visited February 19, 2023).
[14] https://www.prairielakes.com/latest-news/prairie-lakes-healthcare-system-receives-notice-of-third-party-vendor-s-data-security-incident-10576.html (last visited February 19, 2023).
[15] https://www.dakotanewsnow.com/2022/11/22/data-breach-compromises-local-social-security-numbers/ (last visited February 19, 2023).

importance of safeguarding the Private Information of Plaintiffs and Class Members, especially Social Security numbers and PHI, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

39. There were many high-profile data breaches in the months and years leading up to the Data Breach, including within the debt collection industry. For example, in July 2022, it was widely reported that a January 2022 data breach involving Professional Finance Company exposed the Social Security numbers and other sensitive PII of approximately two-million consumer debtors.[16]

40. In 2021, a record 1,862 data breaches occurred, exposing approximately 293,927,708 sensitive records—a 68% increase from 2020.[17]

41. Moreover, 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."[18] Yet, Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiffs and Class Members, causing the exposure of Private Information.

42. AAA had no effective means to quickly detect, prevent, stop, undo, or remediate the effects of the Data Breach, meaning cybercriminals could easily access and steal Private

[16] https://www.healthcaredive.com/news/data-breach-at-debt-collector-affects-almost-2m-healthcare-patients/627450/ (last visited February 19, 2023).

[17] *See 2021 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2022)https://www.idtheftcenter.org/wp-content/uploads/2022/06/ITRC-Annual-Report-2021_Final-1.pdf.

[18] *See* How to Protect Your Networks from RANSOMWARE, at 3, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited: Nov. 24, 2022).

Information.

Securing Private Information and Preventing Breaches

43. Defendant could have prevented this Data Breach by properly securing and encrypting the systems containing the Private Information of Plaintiffs and Class Members. Alternatively, Defendant could have destroyed the data, especially for individuals with whom it no longer had an active relationship.

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

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- 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.

- 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.[19]

45. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the 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

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

attachments are compressed files or ZIP files.

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

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

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

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[20]

46. To prevent and detect cyberattacks, including the cyber-attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

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

[20] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://us-cert.cisa.gov/ncas/tips/ST19-001 (last accessed Nov. 24, 2022).

securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

Apply principle of least-privilege

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

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[21]

47. Given that Defendant was storing the Private Information of Plaintiffs and Class Members, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

48. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the Private Information of Plaintiffs and Class Members.

49. As the result of computer systems in need of security upgrades, inadequate procedures for handling email phishing attacks, viruses, malignant computer code, hacking attacks, Defendant negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private

[21] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last accessed Nov. 24, 2022).

Information.

50. Because Defendant failed to properly safeguard Plaintiffs' and Class Members' Private Information, an unauthorized third party was able to access Defendant's systems, maintain unfettered and undetected access to those systems for three days, and during that time, copy unencrypted and non-password protected files from those systems containing the highly sensitive Private Information stored on Defendant's system.

Defendant Failed to Comply with FTC Guidelines

51. Defendant was also prohibited by the Federal Trade Commission Act ("FTC Act") (15 U.S.C. §45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

52. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[22]

53. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.[23] The guidelines note that businesses should protect the personal customer information that they keep; properly

[22] FEDERAL TRADE COMMISSION, *Start With Security: A Guide for Business, available at:* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Nov. 24, 2022).
[23] FEDERAL TRADE COMMISSION, *Protecting Personal Information: A Guide for Business, available at*: https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Nov. 24, 2022).

dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

54. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[24]

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

56. Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

57. Defendant was at all times fully aware of its obligation to protect the PII stored within its systems because of its position as a leading debt collector. Defendant was also aware of the significant repercussions that would result from its failure to do so.

[24] FTC, *Start With Security*, *supra*.

Plaintiffs and Class Members Have Been, and Will Continue to Be, Harmed by the Theft of their Private Information

58. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[25] 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."[26]

59. 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 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.[27]

60. Similarly, the South Dakota Attorney General warns consumers that,

> If the breach involved disclosure of your SSN, a fraudster could use that information to open *new accounts* in your name. You will not immediately know of the new accounts because criminals usually use an address other than your own

[25] 17 C.F.R. § 248.201 (2013).
[26] *Id*.
[27] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Oct. 27, 2021).

> for the account. Since you will not be receiving the monthly account statements, you are likely to be unaware of the account(s). That is why it is so important to place a fraud alert with the three credit reporting agencies immediately when you learn that your SSN has been compromised, and then to monitor your credit reports on an ongoing basis. Other evidence of new account fraud include receiving credit cards in the mail that you did not apply for, being denied credit when you know you've had a good credit score, and being contacted by debt collectors for payments that you do not owe.[28]

61. The time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used, is discussed in an oft-cited report by the U.S. Government Accountability Office ("GAO"), which states that:

> [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.[29]

62. 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. 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."[30]

63. The recommended steps for responding to a data breach involving Social Security

---

[28] https://consumer.sd.gov/fastfacts/securitybreach.aspx (last visited February 19, 2023).
[29] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last accessed Nov. 24, 2022).
[30] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last accessed Oct. 27, 2021).

numbers are onerous, costly, and time consuming. For example, the South Dakota Attorney General states:[31]

> For security breach situations involving your Social Security Number (SSN) - in other words, breaches in which there is an opportunity for new accounts to be opened in your name you should consider taking the following actions:
>
> - **Notify the credit reporting agencies and establish a fraud alert.** Immediately call the fraud department of one of the three credit reporting agencies ï¿½ Experian, Equifax, or TransUnion. As soon as the agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file.
> - **Order your credit reports.** If you are a victim of identity theft, you will see evidence of it on your credit report. Surveys have found that the sooner individuals learn of the identity theft, the more quickly they can clean up their credit reports and regain their financial health.
> - **Examine your credit reports carefully.** When you receive your credit reports, look for signs of fraud such as credit accounts that are not yours. Check if there are numerous inquiries on your credit report. If a thief is attempting to open up several accounts, an inquiry will be listed on your credit report for each of those attempts. Usually identity thieves do not succeed in opening all of the accounts that they apply for, only some. Multiple inquiries that you yourself have not generated are a sign of potential fraud. Also, check that your SSN, address(es), phone number(s), and employment information are correct.
> - **If your credit report indicates you are a victim of identity theft, you will want to immediately take steps to remove the fraudulent accounts.** If you are a victim you may contact the Federal Trade Commission or the SD Office of Attorney General website for step-by-step information on what you should do.
> - **Contact Social Security Administration at 1-800-772-1213.** Do this to verify earnings reported to your social security number and to request a copy of your Social Security Statement.
> - **Continue to monitor your credit reports.** Be aware that these measures may not entirely stop new fraudulent accounts from being opened by an imposter. Credit issuers do not always pay attention to fraud alerts. Once you have received the first free copy of your credit report, follow up in a few months and order another.
> - **Consider a security freeze.** The three credit reporting agencies ï¿½ Equifax, Experian, and TransUnion, offer security freezes nationwide. Read on for further information.

64. Theft of PHI is also gravely serious: "[a] thief may use your name or health

[31] https://consumer.sd.gov/fastfacts/securitybreach.aspx

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."

65. 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 Private Information.

66. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's 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.

67. To date, Defendant has offered Plaintiffs and Class Members only 12 months of identity and credit monitoring services through IDX. The offered service is inadequate to protect Plaintiffs and Class Members from the threats they face for years to come, particularly in light of the Private Information at issue here. Moreover, Defendant put the burden squarely on Plaintiffs and Class Members to enroll in the inadequate monitoring services.

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

Value of Private Information

69. The Private Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price

ranging from $40 to $200, and bank details have a price range of $50 to $200.[32] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[33] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[34]

70. Social Security numbers are 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. As a result, Social Security numbers demand a comparatively high 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 black market."[35]

71. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase Private Information, and PHI in particular, 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.

72. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[36] In fact, the data marketplace

---

[32] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at* https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Oct. 27, 2021).

[33] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at* https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Oct. 27, 2021).

[34] *In the Dark*, VPNOverview, 2019, *available at* https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Oct. 27, 2021).

[35] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Nov. 24, 2022).

[36] *Data Brokers*, Los Angeles Times, Nov. 5, 2019, *available at*

is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[37] [38] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[39]

73. The integrity of Private Information gives it its value because Private Information is used to secure loans, open lines of credit, verify identities, and unlock government benefits. When Private Information is used to commit fraud, these simple everyday necessities become more difficult, if not impossible, due to lowered credit scores and tarnished credit histories from credit fraud and identity theft.[40]

74. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its acquisition by cybercriminals and is likely already available on the dark web due to its high value for threat actors. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss.

Plaintiff Brown's Experience

75. Plaintiff Brown greatly values his privacy and is very careful with his Private Information. Plaintiff Brown stores any documents containing sensitive Private Information like his Social Security number, financial information, or PHI in a safe and secure location or destroys such documents when they are no longer needed. Plaintiff Brown has never knowingly transmitted

https://www.latimes.com/business/story/2019-11-05/column-data-brokers
[37] https://datacoup.com/
[38] https://digi.me/what-is-digime/
[39] *Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at* https://computermobilepanel.nielsen.com/ui/US/en/faqen.html
[40] https://lifelock.norton.com/learn/identity-theft-resources/lasting-effects-of-identity-theft

unencrypted Private Information over the internet or any other unsecured source. Moreover, Plaintiff Brown diligently chooses unique usernames and passwords for his various online accounts. When Plaintiff Brown does entrust a third-party with his Private Information, it is only because he understands such information will be reasonably safeguarded from foreseeable threats, and that he will be timely notified if his data is exposed.

76. Plaintiff Brown provided Private Information, including his full name, date of birth, Social Security number, phone number, email address, financial information, and PHI to one of Defendant's clients as a condition of receiving medical services. Defendant thereafter acquired this Private Information from Plaintiff Brown's medical provider and used it when attempting to collect a purported debt. Plaintiff Brown also provided certain Private Information to Defendant directly in the course of providing payments to Defendant.

77. Plaintiff Brown reasonably understood that a portion of the funds paid to Defendant and Defendant's client would be used to pay for adequate cybersecurity and protection of Private Information.

78. Plaintiff Brown received a letter dated December 15, 2022 from Defendant notifying him of the Data Breach. The letter stated that after the Data Breach, AAA "worked diligently to investigate this incident and confirm any information that may be affected. Through the investigation, we determined that certain documents stored within AAA's environment were copied from the system as part of the cyber incident between September 5, 2022 and September 7, 2022. Based on the investigation, AAA conducted a detailed review of data involved to determine the type of information present and to whom it related…. You are receiving this notice because we determined that your information may be included." AAA stated that this information included Plaintiff's name, address, phone number, date of birth, medical record number, medical provider

or facility name, condition, diagnosis and/or treatment information; payment amount history; insurance payment amount information; and date of service. Upon information and belief, Plaintiff Brown's Social Security number also would have been contained in documents unlawfully copied from Defendant's systems.

79. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Brown faces, the letter offered Plaintiff Brown a twelve-month subscription to credit monitoring services.

80. Through the Data Breach, Defendant compromised Plaintiff Brown's Private Information leading to at least the following consequences:

a. publishing of Plaintiff Brown's Private Information on the criminal Dark Web (shortly after the Data Breach, Plaintiff Brown received an alert from Experian notifying him of such);

b. hard inquiries on Plaintiff Brown's credit report; and

c. increasing spam phones calls and texts directed to Plaintiff Brown.

81. Shortly after the Data Breach occurred, Plaintiff Brown received hard inquiries on his credit report that he did not approve, a form of identity theft indicating that someone has fraudulently applied for lines of credit in his name. And as consumer advocates report, unauthorized credit inquiries harm consumers for years[41]:

[41] *See* CreditKarma's *5 things to do if you spot an unauthorized credit inquiry* at https://www.creditkarma.com/credit-cards/i/unauthorized-credit-inquiry (last visited Jan. 31, 2023).

> Multiple hard inquiries within a short period of time might alarm potential creditors, who may worry that you've taken out too much credit to pay back, says Linda Sherry, a spokeswoman for Consumer Action, a consumer education and advocacy organization.

> A hard inquiry, which can stay on your credit reports for up to two years, can also lower your credit scores by a few points. This might not sound serious, but according to FICO, it may have a greater impact on your scores if you have few accounts or a short credit history.

82. Plaintiff Brown anticipates spending significant time, money, and effort on an ongoing basis to try to mitigate and address the present and impending injuries caused by the Data Breach. The letter Plaintiff Brown received encourage him to take such steps.

83. The Data Breach and exfiltration of Plaintiff Brown's Private Information has caused him to suffer a loss of privacy. This loss of privacy is analogous to the injury caused by the commission of well-recognized common law privacy torts like invasion of privacy.

84. Plaintiff Brown suffered actual injury in the form of damages to and diminution in the value of his Private Information —a form of intangible property Defendant was required to adequately protect.

85. Plaintiff Brown suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff Brown's PII right in the hands of criminals. Plaintiff Brown now faces an ongoing, substantial risk of suffering identity theft and fraud in the future, as he has *already* suffered identity theft multiple times and because the breach involved sensitive private

information, including his insurance and payment information and his private medical information. As a result, Plaintiff Brown has spent considerable time and effort monitoring his accounts to protect himself from further identity theft. Plaintiff Brown fears for his personal financial security and uncertainty over what information was revealed in the Data Breach.

86. The misuse of his Private Information, loss of privacy, and substantial risk of harm that Plaintiff Brown faced and continues to face has caused him to suffer proportional fear, stress, anxiety, and nuisance.

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

Plaintiff Pederson's Experience

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

89. Plaintiff Pederson provided PII, including his full name, date of birth, Social Security number, phone number, email address, and financial information to one of Defendant's clients as a condition of receiving services. Defendant thereafter acquired this PII and used it when

attempting to collect a purported consumer debt.

90. Plaintiff Pederson reasonably understood that a portion of the funds paid to Defendant and/or Defendant's client would be used to pay for adequate cybersecurity and protection of PII.

91. Plaintiff Pederson received a letter dated November 16, 2022 from Defendant notifying him of the Data Breach. The letter stated that after the Data Breach, AAA "worked diligently to investigate this incident and confirm any information that may be affected. Through the investigation, we determined that certain documents stored within AAA's environment were copied from the system as part of the cyber incident between September 5, 2022 and September 7, 2022. Based on the investigation, AAA conducted a detailed review of data involved to determine the type of information present and to whom it related…. You are receiving this notice because we determined that your information may be included." AAA stated that this information included Plaintiff's name and Social Security number.

92. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Pederson faces, the letter offered Plaintiff Pederson a twelve-month subscription to credit monitoring services, which he signed up for. However, Plaintiff Pederson was forced to spend time signing up for this service. Moreover, this is an inadequate remedy because, *inter alia*, Plaintiff Pederson will be at a substantial risk of harm for the rest of his life.

93. As a result of the Data Breach notice, Plaintiff Pederson has spent several hours 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 and credit reports. Plaintiff Pederson also spent significant time changing the passwords to all of his online accounts containing sensitive PII.

94. Following the Data Breach, Plaintiff Pederson suffered fraudulent activity on his PayPal account. Roughly one month before receiving the letter notifying Plaintiff Pederson of the Data Breach, an unknown third-party made an unauthorized purchase on Plaintiff Pederson's PayPal account for several hundred dollars. This money was withdrawn from Plaintiff Pederson's bank account, leaving Plaintiff Pederson without access to his funds. Plaintiff Pederson spent several hours resolving the fraud, ultimately closing his PayPal account on October 11, 2022.

95. Shortly after the Data Breach, Plaintiff Pederson experienced a substantial increase in spam and suspicious phone calls, emails, and text messages. Upon information and belief, Plaintiff Pederson's contact information was included in any documents within AAA's possession containing Plaintiff Pederson's Social Security number.

96. Plaintiff Pederson anticipates spending significant time, money, and effort on an ongoing basis to try to mitigate and address the present and impending injuries caused by the Data Breach. The letter Plaintiff Pederson received encourage him to take such steps.

97. The Data Breach and exfiltration of Plaintiff Pederson's Private Information has caused him to suffer a loss of privacy. This loss of privacy is analogous to the injury caused by the commission of well-recognized common law privacy torts like invasion of privacy.

98. As a result of the Data Breach, Plaintiff Pederson will face a substantial risk of imminent harm for the rest of his life.

99. The fraud, loss of privacy, and substantial risk of harm that Plaintiff Pederson faced and continues to face has caused Plaintiff Pederson to suffer proportional fear, stress, anxiety, and nuisance.

100. Plaintiff Pederson has suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property Defendant was required to

adequately protect.

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

CLASS ALLEGATIONS

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

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

> **All United States residents whose Private Information was compromised in the Data Breach discovered by Defendant in September 2022.**

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

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

106. Numerosity, Fed R. Civ. P. 23(a)(1): Class Members are so numerous that joinder of all members is impracticable. There are over 50,000 individuals whose Private Information may

have been improperly accessed in the Data Breach, and each Class is apparently identifiable within Defendant's records.

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

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

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

c. Whether Defendant had duties not to use the Private Information of Plaintiffs and Class Members for non-business purposes;

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

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

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

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

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

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

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiffs and Class Members;

k. Whether Defendant 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 Defendant's wrongful conduct;

m. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendant's 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.

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

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

110. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that Plaintiffs have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights

and the damages Plaintiffs have suffered are typical of other Class Members. Plaintiffs have also retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

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

112. The nature of this action and the nature of laws available to Plaintiffs and Class Members makes the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it 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.

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

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

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

116. Further, Defendant has acted or refused to act on grounds generally applicable to the Class 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.

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

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

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

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

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

e. Whether Defendant breached the implied contract;

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

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

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiffs and Class Members;

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

CAUSES OF ACTION

COUNT 1
NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class)

118. Plaintiffs and the Nationwide Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

119. Plaintiffs and the Class entrusted Defendant with their Private Information.

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

unauthorized third parties.

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

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

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

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

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

126. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiffs and the Class. That special relationship arose because Plaintiffs and the Class entrusted Defendant with their confidential Private Information, a necessary part of obtaining services from Defendant. That duty further arose because Defendant chose to collect and maintain the Private Information for its own pecuniary benefit.

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

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

129. Plaintiffs' and the Class's injuries were foreseeable and Plaintiffs and the Class were the probable victims of any inadequate security practices and procedures by Defendant. Defendant knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiffs and the Class, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendant's systems.

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

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

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

133. Defendant had and continues to have a duty to adequately disclose that the Private Information of Plaintiffs and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised

and when the Private Information was compromised. Such notice was necessary to allow Plaintiffs and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

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

135. Defendant has admitted that the Private Information of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

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

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

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

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

140. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove Private Information that was no longer required to retain pursuant to regulations.

141. Defendant, through its actions and/or omissions, unlawfully breached its duty to

adequately and timely disclose to Plaintiffs and the Class the existence and scope of the Data Breach.

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

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

144. 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 Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

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

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

147. Plaintiffs and the Class are within the class of persons that the FTC Act was

intended to protect.

148. 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 Class.

149. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and the Class have suffered and will suffer injuries and damages, including but not limited to: (i) actual theft, fraud, and/or the unauthorized use of Private Information; (ii) the loss of the opportunity to control how their Private Information is used; (iii) loss of time; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from theft, fraud, and/or unauthorized use of their Private Information; (v) loss of privacy; (vi) anxiety, stress, nuisance, and inconvenience proportional to the risk of harm they face; and (vii) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information of Plaintiffs and the Class.

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

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

COUNT 2
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class)

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

153. Plaintiffs and the Class provided their Private Information and/or payments to Defendant, either directly or indirectly through Defendant's clients, as part of Defendant's regular business practices.

154. As a condition of obtaining care and/or services from Defendant or its clients, Plaintiffs and the Class provided and entrusted their Private Information. In so doing, Plaintiffs and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and the Class if their data had been breached and compromised or stolen.

155. A meeting of the minds occurred when Plaintiffs and the Class agreed to, and did, provide their Private Information to Defendant and/or Defendant's clients with the reasonable understanding that their Private Information would be adequately protected by any business associates, like Defendant, from foreseeable threats. This inherent understanding exists independent of any other law or contractual obligation any time that highly sensitive PII and PHI is exchanged as a condition of receiving services. It is common sense that but for this implicit and/or explicit agreement, Plaintiffs and Class Members would not have provided their Private Information.

156. Defendant separately has contractual obligations arising from and/or supported by, *inter alia*, the consumer facing statements in its privacy policies.

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

158. Defendant breached the implied contracts it made with Plaintiffs and the Class by failing to reasonably safeguard and protect their Private Information and by failing to provide timely and accurate notice that Private Information was compromised as a result of the Data Breach.

159. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending harm.

160. As a result of Defendant's breach of implied contract, Plaintiffs and the Class are entitled to and demand actual, consequential, and nominal damages.

COUNT 3
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class)

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

162. AAA entered into various contracts with its clients to provide accounts receivable management services.

163. These contracts are virtually identical to each other and were made expressly for the benefit of Plaintiffs and the Class, as it was their Private Information that AAA agreed to collect and protect through its services. Thus, the benefit of collection and protection of the Private Information belonging to Plaintiffs and the Class was the direct and primary objective of the contracting parties.

164. AAA knew that if it were to breach these contracts with its clients, the clients'

patients, including Plaintiffs and the Class, would be harmed by, among other things, fraudulent misuse of their Private Information.

165. AAA breached its contracts with its clients when it failed to use reasonable data security measures that could have prevented the Data Breach and resulting compromise of Plaintiffs' and Class Members' Private Information.

166. As was reasonably foreseeable, Plaintiffs and the Class were harmed by AAA's failure to use reasonable data security measures to store their Private Information, including but not limited to, the actual harm through the loss of their Private Information to cybercriminals.

167. Accordingly, Plaintiffs and the Class are entitled to and demand actual, consequential, and nominal damages.

COUNT 4
UNJUST ENRICHMENT
(On behalf of Plaintiffs and the Nationwide Class)

168. Plaintiffs repeat and re-allege each and every allegation in the Complaint as if fully set forth herein, with the exception that this claim is brought in the alternative to any claim for breach of contract.

169. Plaintiffs and Class Members conferred a monetary benefit on Defendant by providing Defendant, directly or indirectly, with their valuable Private Information.

170. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information.

171. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid its 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 Defendant's failure

to provide the requisite security.

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

173. Defendant acquired the monetary benefit and Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

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

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

176. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer injuries

177. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that it unjustly received from them.

COUNT 5
INVASION OF PRIVACY
(On Behalf of Plaintiffs and the Nationwide Class)

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

179. Plaintiffs and Class Members had a legitimate expectation of privacy regarding their Private Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

180. Defendant owed a duty to Plaintiffs and Class Members to keep their Private Information confidential. Rather than comply with this duty, Defendant recklessly and

intentionally stored Private Information in a manner that it knew was susceptible to foreseeable threats.

181. According to a report from Deloitte, 91 percent of all cyber-attacks begin with a phishing attack.[42] Upon information and belief, Defendant affirmatively provided unauthorized third parties with access to Plaintiffs' and Class Members' Private Information through its interaction with and/or response to foreseeable social engineering techniques like phishing.

182. The unauthorized disclosure of Plaintiffs' and Class Members' Private Information to an unauthorized third party is highly offensive to a reasonable person.

183. Defendant's reckless and intentional failure to protect Plaintiffs' and Class Members' Private Information from unauthorized disclosure constitutes an intentional interference with Plaintiffs' and the Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

184. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

185. Defendant knowingly failed to notify Plaintiffs and Class Members in a timely fashion about the Data Breach.

186. Because Defendant failed to properly safeguard Plaintiffs' and Class Members' Private Information, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and the Class.

187. As a proximate result of Defendant's acts and omissions, the Private Information

[42] https://www2.deloitte.com/my/en/pages/risk/articles/91-percent-of-all-cyber-attacks-begin-with-a-phishing-email-to-an-unexpected-victim.html

of Plaintiffs and Class Members was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class to suffer damages.

188. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their Private Information is still maintained by Defendant with its inadequate cybersecurity system and policies.

189. Plaintiffs and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's refusal to safeguard the Private Information of Plaintiffs and the Class.

190. Plaintiffs, on behalf of themselves and Class Members, seek injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiffs' and Class Members' Private Information.

191. Plaintiffs, on behalf of themselves and Class Members, seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant and the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

COUNT 6
DECLARATORY RELIEF
(On Behalf of Plaintiffs and the Nationwide Class)

192. Plaintiffs and the Nationwide Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein

193. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and granting

further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

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

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

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

197. To Plaintiffs' knowledge, Defendant has made no announcement that it has changed its data storage or security practices relating to the Private Information.

198. To Plaintiffs' knowledge, Defendant has made no announcement or notification that it has remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

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

200. The hardship to Plaintiffs and Class Members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another data breach occurs at AAA, Plaintiffs and Class Members will likely continue to be subjected to fraud,

identify theft, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

201. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at AAA, thus eliminating the additional injuries that would result to Plaintiffs and Class Members, along with other patients and/or current and former AAA employees whose Private Information would be further compromised.

202. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that AAA implement and maintain reasonable security measures, including but not limited to the following:

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

b. engaging third-party security auditors and internal personnel to run automated security monitoring;

c. auditing, testing, and training its security personnel regarding any new or modified procedures;

d. purging, deleting, and destroying Private Information not necessary for its provisions of services in a reasonably secure manner;

e. conducting regular database scans and security checks; and

f. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

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 Class, and appointing Plaintiffs and their Counsel to represent the Class;

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

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

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

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

iii. requiring Defendant to delete, destroy, and purge the Private Information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when

weighed against the privacy interests of Plaintiffs and Class Members;

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

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

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

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

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

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

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

xi. requiring Defendant to establish an information security training program

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

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

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

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

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

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

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

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

F. For prejudgment interest on all amounts awarded; and

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

DEMAND FOR JURY TRIAL

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

Date: February 24, 2023

Respectfully Submitted,

REITER LAW FIRM, LLC

BY */s/ Pamela Reiter*
Pamela R. Reiter
Anthony P. Sutton
5032 S. Bur Oak Place, Suite 205
Sioux Falls, SD 57108
Phone: 605-705-2900
pamela@reiterlawfirmsd.com
anthony@reiterlawfirmsd.com

Terence R, Coates*
Jonathan T. Deters**
Dylan J. Gould**
MARKOVITS, STOCK & DEMARCO, LLC
119 E. Court Street, Suite 530

Cincinnati, OH 45202
Telephone: 513.651.3700
Facsimile: 513.665.0219
tcoates@msdlegal.com
jdeters@msdlegal.com
dgould@msdlegal.com

Joseph M. Lyon*
THE LYON FIRM, LLC
2754 Erie Avenue
Cincinnati, OH 45208
Phone: (513) 381-2333
Fax:(513) 766-9011
jlyon@thelyonfirm.com

Raina C. Borrelli**
Samuel J. Strauss**
Brittany Resch**
TURKE & STRAUSS LLP
613 Williamson St., Suite 201
Madison, WI 53703
Telephone (608) 237-1775
Facsimile: (608) 509-4423
raina@turkestrauss.com
sam@turkestrauss.com
brittanyr@turkestrauss.com

**Pro Hac Vice Application Granted*
***Pro Hac Vice Application forthcoming*

Counsel for Plaintiffs and Putative Class