IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

ALDREAMER SMITH, individually and on behalf of all others similarly situated, Plaintiff, v. ALACRITY SOLUTIONS GROUP, LLC. Defendant.	)	**Case No.:** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Aldreamer Smith ("Plaintiff Smith" or "Smith"), individually and on behalf of all others similarly situated, through the undersigned counsel, hereby alleges the following against Defendant Alacrity Solutions Group, LLC ("ASG" or "Defendant"). Facts pertaining to Plaintiff and her personal experiences and circumstances are alleged based upon personal knowledge and all other facts herein are alleged based upon information and belief, *inter alia*, the investigation of Plaintiff's counsel.

NATURE OF THE ACTION

1. This is a class action for damages with respect to Alacrity Solutions Group, LLC for its failure to exercise reasonable care in securing and safeguarding its client's sensitive information—including names and Social Security numbers (the "PII" or "Private Information").

2. This class action is brought on behalf of individuals whose information was stored on ASG's computer networks and had their sensitive PII accessed by unauthorized parties because of a lapse in network security in or around March of 2021 (the "Data Breach").

3. The Data Breach affected individuals whose information was stored on ASG's servers in multiple states.

4. ASG reported to Plaintiff that information compromised in the Data Breach included her PII.

5. Plaintiff was not notified of the Data Breach until April of 2022, over a year after her Private Information was first accessed.

6. As a result of the Data Breach, Plaintiff and Class members will experience various types of misuse of their PII in the coming years, including but not limited to unauthorized credit card charges, unauthorized access to email accounts, and other fraudulent use of their financial information.

7. There has been no assurance offered from ASG that all personal data or copies of data have been recovered or destroyed. ASG offered 12 months of credit monitoring through Equifax, which does not guarantee the security of Plaintiff's and Class members' Private Information. To mitigate further harm, Plaintiff chose not to disclose any more information to receive these services connected with ASG.

8. Accordingly, Plaintiff asserts claims for negligence, breach of third-party beneficiary contract, breach of implied contract, breach of fiduciary duty, bailment, unjust enrichment, breach of confidence, violations of Indiana consumer protection statutes, and declaratory and injunctive relief.

PARTIES

A. Plaintiff Aldreamer Smith

9. Plaintiff Aldreamer Smith is a citizen and resident of Allen, Texas and brings this action in her individual capacity and on behalf of all others similarly situated. Plaintiff Smith

maintains car and renter's insurance for her home, but otherwise is unsure how Alacrity Solutions would have obtained her Private Information. In maintaining Plaintiff Smith's Private Information, Defendant expressly and impliedly promised to safeguard Plaintiff Smith's PII. Defendant, however, did not take proper care of Plaintiff Smith's PII, leading to its exposure as a direct result of Defendant's inadequate security measures. In April of 2022, Plaintiff Smith received a notification letter from Defendant stating that her PII, which included her name and Social Security number, was compromised.

10. The letter also offered one year of credit monitoring through Equifax, which was and continues to be ineffective for Plaintiff Smith and the Class members. In order to receive the free credit monitoring services, Plaintiff Smith would have had to share additional sensitive private information with third parties connected to ASG.

11. In the months and years following the Data Breach, Plaintiff Smith and Class members will experience a slew of harms as a result of Defendant's ineffective data security measures. Some of these harms will include fraudulent charges, requests for services taken out in individuals' names, and targeted advertising without consent.

12. These harms are not just theoretical. Plaintiff Smith has already spent approximately five hours on the phone, monitoring her credit accounts, and attempting to learn more about the scope of the Data Breach.

13. Plaintiff Smith greatly values her privacy, especially in the administration of her finances, and would not have done business with ASG if she had known that her information would be maintained using inadequate data security systems.

B. Defendant

14. Defendant Alacrity Solutions Group, LLC is a Delaware limited liability company

with its principal place of business located in the State of Indiana at 9725 Windermere Boulevard in Fishers, Indiana. ASG is an insurance claims administrator that operates nationally, including in Texas. ASG's corporate policies and practices, including those used for data privacy, are established in, and emanate from the state of Indiana.

JURISDICTION AND VENUE

15. The Court has jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2) ("CAFA"), because (a) there are 100 or more class members, (b) at least one Class member is a citizen of a state that is diverse from Defendant's citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

16. The Court has personal jurisdiction over Defendant because Defendant is a Delaware limited liability company.

17. Venue is proper in this district under 28 U.S.C. § 1391(b)(1) because Defendant is incorporated in this District and therefore resides in this District pursuant to 28 U.S.C. § 1391(c)(2).

18. Plaintiff is informed and believes, and thereon alleges, that each of the acts and omissions alleged herein were performed by, and/or attributable to, Defendant.

FACTS

19. Defendant services and administers insurance claims for companies of all sizes across the country. As part of its business, Defendant was entrusted with, and obligated to safeguard and protect the Private Information of Plaintiff and the Class in accordance with all applicable law.

20. Defendant learned of a "security incident" that occurred between March 1 and March 3 of 2021 in which an unauthorized actor accessed the private information of individuals

on Defendant's computer network including their names and Social Security numbers. Defendant sent the following notice letter template to various state attorneys general:[1]

> Alacrity Solutions Group, LLC ("Alacrity Solutions") is writing to inform you of an incident that could affect the security of some of your information. This notice provides information about the incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it necessary to do so.
>
> **What Happened?** On or about March 3, 2021, Alacrity Solutions became aware of suspicious activity on our network. Following this, we promptly launched an investigation with the assistance of third-party forensic specialists to assess the security of our systems and determine the nature and scope of this incident. This investigation determined that certain files on Alacrity Solutions' systems could have been subject to unauthorized access and/or acquisition between March 1 and March 3, 2021, but could not confirm which specific data was impacted. As a result, Alacrity Solutions then embarked on a diligent and comprehensive review of all data at risk to determine: the full universe of information present in the potentially impacted files; to whom the information related; and accurate mailing addresses for all potentially impacted individuals. On February 22, 2022, Alacrity Solutions completed this time intensive review and confirmed that information related to you was potentially impacted by this event.
>
> **What Information Was Involved?** The information present in the affected systems and potentially subject to unauthorized access and/or acquisition includes your name, <<Breached Elements>>. While we have no evidence to suggest that any identity theft or unauthorized use of the affected information has occurred, we are making you aware of this incident in an abundance of caution.
>
> **What We Are Doing.** Data privacy and security are among Alacrity Solutions' highest priorities, and there are extensive measures in place to protect information in our care. Upon discovery, Alacrity Solutions promptly commenced an investigation with the assistance of third-party cyber security specialists to confirm the nature and scope of this incident. Alacrity Solutions is providing notice of this incident to potentially impacted individuals and pertinent state

[1] Montana Attorney General's Office, *Alacrity Solutions Group Data Notification Letter*, https://media.dojmt.gov/wp-content/uploads/Consumer-Notification-41.pdf.

and/or federal regulators. As part of Alacrity Solutions' ongoing commitment to the security of information, all policies and procedures are being reviewed and enhanced where possible, additional safeguards are being implemented, and workforce training is being conducted to reduce the likelihood of a similar event in the future.

As an added precaution, we are also offering you complimentary access to <<CM Length>> months of credit monitoring and identity theft restoration services, through Equifax. You will need to enroll yourself in these services if you wish to do so, as we are not able to activate them on your behalf. Please review the instructions contained in the attached Steps You Can Take to Help Protect Your Personal Information for additional information on these services.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, explanation of benefits, and credit reports for suspicious activity. You may also review the enclosed Steps You Can Take To Help Protect Your Personal Information for additional steps you may take and information on what you can do to better protect against the possibility of identity theft and fraud, should you feel it is appropriate to do so. We also encourage you to enroll in the complimentary credit monitoring services we are offering you.

For More Information. If you have questions about this letter, please call 844-985-2420 between the hours of 9:00 a.m. and 9:00 p.m., Eastern Time, Monday through Friday. Individuals may also write to Alacrity Solutions at 9725 Windmere Blvd, Fishers, Indiana 46037.

Sincerely,

Alacrity Solutions Group, LLC
https://www.alacritysolutions.com/.

21. Upon learning of the Data Breach in March of 2021, Defendant investigated. Although Defendant has not provided an estimate of how many individuals were affected by the

Data Breach, Defendant reported that the incident affected people in multiple states including California, Montana, Massachusetts, and Vermont.[2]

22. In March of 2022 Defendant announced through notice letters sent to individuals affected by the data breach and notifications to various state attorneys general that it had concluded an investigation into the data breach incident on February 22, 2022.

23. Defendant offered no explanation for the delay between the initial discovery of the Breach and the belated notification to affected individuals, which resulted in Plaintiff and Class members suffering harm they otherwise could have avoided had a timely disclosure been made.

24. ASG's notice of Data Breach was not just untimely but woefully deficient, failing to provide basic details of the Data Breach, including but not limited to, how unauthorized parties accessed ASG's networks, whether the impacted information was encrypted or otherwise protected, how ASG learned of the Data Breach, whether the Data Breach occurred system-wide, whether servers storing information were accessed, and how many people were affected by the Data Breach. Even worse, ASG offered only one year of credit monitoring for Plaintiff and Class members, which required their disclosure of additional PII with which ASG had just demonstrated it could not be trusted.

25. Plaintiff and Class members' PII is likely for sale to criminals on the dark web, meaning that unauthorized parties will have accessed and viewed Plaintiff's and Class members' unencrypted, unredacted information, including names and Social Security numbers.

[2] Various states require that data breach incidents affecting citizens within that state be reported to the attorney general's office within a reasonable period of time after the breach. Defendant sent notice of the Data Breach to several states and its generic notice letter is recorded in multiple state attorneys general consumer protection data breach portals. *See, e.g.*, *id.*

26. The Breach occurred because Defendant failed to take reasonable measures to protect the Private Information it collected and stored. Among other things, Defendant failed to implement data security measures designed to prevent this release of information, despite repeated warnings to financial and insurance companies about the risk of cyberattacks and the highly publicized occurrence of many similar attacks in the recent past.

27. Defendant disregarded the rights of Plaintiff and Class members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff's and Class members' PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and negligently failing to follow applicable, required, and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiff and Class members was compromised through unauthorized access by cybercriminals intending to steal and profit from the stolen Private Information. Plaintiff and Class members have a continuing interest in ensuring that their Private Information (which is still in Defendant's possession and control) is safe.

A. Defendant's Privacy Promises

28. ASG made, and continues to make, various promises to the individuals, including Plaintiff, whose Private Information is stored on their systems that it will adequately maintain the security and privacy of their Private Information in accordance with applicable law and industry standards.

29. In its Notice of Privacy Practices, which was updated for 2020 and is therefore applicable to Plaintiff, Defendant stated the following under the section bolded and titled "**HOW**

WE USE INFORMATION":[3]

> We may use the information we collect for a range of business purposes, including to:
>
> - Provide and deliver products and services and fulfill your requests;
> - Communicate with you through various channels;
> - Offer you our goods or services or those of trusted partners;
> - Evaluate and respond to your requests, inquiries, and applications;
> - Create and manage your account registration;
> - Conduct and administer contests, surveys, and sweepstakes;
> - Customize your experiences on our Sites;
> - Operate, evaluate, and improve our business, products, and services (including developing new products and services; managing our communications; performing market research and data analytics; determining and managing the effectiveness of our advertising and marketing; analyzing our products, services, and websites; administering our websites; and perform accounting, auditing, billing, reconciliation and collection activities);
> - Protect against and prevent fraud and unauthorized transactions, investigate and manage claims, risk exposure, and quality, and generally provide and improve security; and
> - Comply with and enforce applicable legal requirements, industry standards, and our policies and terms and conditions.
>
> We may also use the information in other ways for which we provide notice at the time of collection . . .
>
> **HOW WE PROTECT INFORMATION**
>
> We maintain administrative, technical, and physical safeguards designed and intended to protect personal information against accidental, unlawful, or unauthorized destruction, loss, alteration, access, disclosure or use. Despite these safeguards, due to inherent uncertainty in the use of the Internet and information systems and the potential for unlawful attacks by third parties, we cannot guarantee that the use of our Sites or computer systems will be completely safe or secure.

[3] *Privacy Statement*, ALACRITY SOLS. (Mar. 9, 2020), https://www.alacritysolutions.com/privacy/.

> Information we collect and use may be transferred, stored, and accessed globally to support our operations. We retain information for as long as it is needed or useful to provide and improve our products and services, comply with our legal obligations, resolve disputes, and enforce our agreements.

30. ASG describes how it may use and disclose financial information for each category of uses or disclosures, none of which provide it a right to expose peoples' Private Information in the manner it was exposed to unauthorized third parties in the Data Breach.

31. By failing to protect Plaintiff's and Class members' Private Information, and by allowing the Data Breach to occur, ASG broke these promises to Plaintiff and Class members.

B. Defendant Failed to Maintain Reasonable and Adequate Security Measures to Safeguard the Private Information of Individuals on its Systems.

32. ASG acquires, collects, and stores a massive amount of the personal information of individuals who purchase insurance policies and other products from its customers. Protected PII of these individuals, including financial information and other personally identifiable data, was contained within ASG's systems at the time of the data breach incident.

33. As a condition of engaging in insurance and financial-related services, ASG requires that these customers entrust them with highly confidential Private Information of the individuals on their systems.

34. By obtaining, collecting, using, and deriving a benefit from Plaintiff and Class members' Private Information, ASG assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff and Class members' Private Information from disclosure.

35. Defendant had obligations created by industry standards, common law, and representations made to Plaintiff and Class members, to keep the Private Information confidential and to protect it from unauthorized access and disclosure.

36. Defendant failed to properly safeguard Class members' Private Information, allowing hackers to access their Private Information.

37. Plaintiff and Class members provided their Private Information to ASG's customers with the reasonable expectation and mutual understanding that if the information were provided to any third parties such as Defendant, Defendant and any of its affiliates would comply with their obligation to keep such information confidential and secure from unauthorized access.

38. Prior to and during the Data Breach, Defendant promised the individuals whose information it collected that their Private Information would be kept confidential.

39. Defendant's failure to provide adequate security measures to safeguard individuals' Private Information is especially egregious because Defendant operates in a field which has recently been a frequent target of scammers attempting to fraudulently gain access to customers' highly confidential Private Information.

40. In fact, Defendant has been on notice for years that Plaintiff's and Class members' PII was a target for malicious actors. Despite such knowledge, ASG failed to implement and maintain reasonable and appropriate security measures to protect Plaintiff's and Class members' PII from unauthorized access that ASG should have anticipated and guarded against.

41. Defendant was also on recent notice that the federal government is concerned about data security. In 2021, the FTC updated its consumer information Safeguards Rule, requiring non-banking financial institutions such as mortgage brokers, motor vehicle dealers, and payday lenders, to develop, implement, and maintain comprehensive security systems to keep their customer's

information safe. Against the backdrop of a rapid increase in cybersecurity incidents related to consumer financial information, Samuel Levine, the director of the FTC's Bureau of Consumer Protection, issued a warning stating that, "Financial institutions and other entities that collect sensitive consumer data have a responsibility to protect it."[4]

42. The number of U.S. data breaches surpassed 1,000 in 2016, a record high and a forty percent increase in the number of data breaches from the previous year.[5] In 2017, a new record high of 1,579 breaches were reported—representing a 44.7 percent increase.[6] That trend continues. The First American Financial Mortgage data breach incident in 2019, for example, exposed hundreds of millions of users' financial information to cybercriminals.[7]

43. The average time to identify and contain a data breach is 287 days,[8] with some breaches going unrecognized for months leading to costly recover efforts and financial impact. Additionally, the median cost per US consumer incurred on each fraud-related data breach incident

---

[4] *FTC Strengthens Security Safeguards for Consumer Financial Information Following Widespread Data Breaches*, https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-strengthens-security-safeguards-consumer-financial-information-following-widespread-data

[5] Identity Theft Resource Center, *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout* (Jan. 19, 2017), https://www.idtheftcenter.org/surveys-studys.

[6] Identity Theft Resource Center, *2017 Annual Data Breach Year-End Review*, https://www.idtheftcenter.org/2017-data-breaches/.

[7] *First American Financial Breach Exposes Millions of Complete Identities*, IDENTITY THEFT RESOURCE CTR (MAY 28, 2019), https://www.idtheftcenter.org/post/first-american-financial-breach-exposes-millions-of-complete-identities/.

[8] IBM SECURITY, COST OF A DATA BREACH REPORT 6 (2021) [hereinafter COST OF A DATA BREACH REPORT]

in 2020 was $450.[9] Data breaches and identity theft have a crippling effect on individuals and detrimental impact on the economy as a whole.[10]

44. A 2021 study conducted by Verizon showed that internal mismanagement of data security, including mis-delivery of emails, represents nearly 44 percent of the data breaches in the financial sector.[11] The majority of these incidents involve the sending or releasing of information to unauthorized actors.[12]

45. PII related data breaches continued to rapidly increase into 2021 when ASG was breached.[13]

46. Almost half of the data breaches globally are caused by internal errors, being either human mismanagement of sensitive information or system errors.[14] Cybersecurity firm Proofpoint reports that since 2020, there has been an increase of internal threats through the misuse of security credentials or the negligent release of sensitive information.[15] To mitigate these threats, Proofpoint recommends that firms take the time to train their employees about the risks of such errors.[16]

---

[9] Insurance Information Institute, *Facts + Statistics: Identity Theft and Cybercrime* (2020), https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#top

[10] *Id.*

[11] *Financial and Insurance Data Breaches*, VERIZON 2021 DIBR DATA BREACH SURVEY (2021), https://www.verizon.com/business/resources/reports/dbir/2021/data-breach-statistics-by-industry/financial-services-data-breaches/.

[12] *Id.*

[13] *2019 HIMSS Cybersecurity Survey*, https://www.himss.org/2019-himsscybersecurity-survey.

[14] COST OF A DATA BREACH REPORT, *supra* note 8, at 30.

[15] *The Human Factor 2021*, PROOFPOINT (July 27, 2021), https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-human-factor-report.pdf.

[16] *Id.*

47. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precaution for protection."[17]

48. To prevent and detect unauthorized access, including the systems changes that resulted in the Data Breach, 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.

[17] *See How to Protect Your Networks from RANSOMWARE*, FBI (2016) https ://www. fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

- 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.

49. To prevent and detect unauthorized access to its systems, including the unauthorized access that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks . . .

- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear

> almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net) . . .
>
> - **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
>
> - **Keep your personal information safe.** Check a website's security to ensure the 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 . . .[18]

50. To prevent the unauthorized access 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 the latest security updates
  - Use threat and vulnerability management
  - Perform regular audit; remove privilege credentials;

[18] *See Security Tip (ST19-001) Protecting Against Ransomware*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (Apr. 11, 2019), https://us-cert.cisa.gov/ncas/tips/ST19-001.

- **Thoroughly investigate and remediate alerts**
  - Prioritize and treat commodity malware infections as potential full compromise

- **Include IT Pros in security discussions**
  - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

- **Build credential hygiene**
  - use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

- **Apply principle of least-privilege**
  - Monitor for adversarial activities
  - Hunt for brute force attempts
  - Monitor for cleanup of Event Logs
  - Analyze logon events

- **Harden infrastructure**
  - Use Windows Defender Firewall
  - Enable tamper protection
  - Enable cloud-delivered protection
  - Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[19]

51. These are basic, common-sense email security measures that every business, not only those who handle sensitive financial information, should be doing. ASG, with its heightened standard of care should be doing even more. But by adequately taking these common-sense solutions, ASG could have prevented this Data Breach from occurring.

[19] *See Human-operated ransomware attacks: A preventable disaster*, MICROSOFT (Mar. 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-apreventable-disaster/.

52. Charged with handling sensitive PII including financial information, ASG knew, or should have known, the importance of safeguarding the Private Information that was entrusted to it by its customers and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on the individuals whose information was stored on ASG's systems as a result of a breach. ASG failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

53. With respect to training, ASG specifically failed to:

- Implement a variety of anti-ransomware training tools, in combination, such as computer-based training, classroom training, monthly newsletters, posters, login alerts, email alerts, and team-based discussions;
- Perform regular training at defined intervals such as bi-annual training and/or monthly security updates; and
- Craft and tailor different approaches to different employees based on their base knowledge about technology and cybersecurity.

54. The PII was also maintained on ASG's computer system in a condition vulnerable to cyberattacks such as through the infiltration of Defendant's negligently maintained systems. The mechanism of the unauthorized access and the potential for improper disclosure of Plaintiff's and Class members' PII was a known risk to ASG, and thus ASG was on notice that failing to take reasonable steps necessary to secure the PII from those risks left the PII in a vulnerable position.

C. The Monetary Value of Privacy Protections and Private Information

55. The fact that Plaintiff's and Class members' Private Information was stolen—and is likely presently being offered for sale to cyber criminals—demonstrates the monetary value of the Private Information.

56. At all relevant times, Defendant was well aware that Private Information it collects from Plaintiff and Class members is highly sensitive and of significant property value to those who would use it for wrongful purposes.

57. Private Information is a valuable property right that is an important commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identify theft and financial fraud.[20] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII including sensitive financial information on multiple underground Internet websites, commonly referred to as the dark web.

58. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[21]

59. Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 Billion per

---

[20] Federal Trade Commission, *Warning Signs of Identity Theft* (Sept. 2018), https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft .

21 *Public Workshop: The Information Marketplace: Merging and Exchanging Consumer Data*, FED. TRADE COMM'N Tr. at 8:2-8 (Mar. 13, 2001), https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf.

year online advertising industry in the United States.[22]

60. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[23]

61. Recognizing the high value that consumers place on their Private Information, many companies now offer consumers an opportunity to sell this information.[24] The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from their Private Information. This business has created a new market for the sale and purchase of this valuable data.

62. Consumers place a high value not only on their Private Information, but also on the privacy of that data. Researchers have begun to shed light on how much consumers value their

---

[22] *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, The Wall Street Journal (Feb. 28, 2011), http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html [hereinafter *Web's New Hot Commodity*].

[23] *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, FED. TRADE COMM'N (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.

24 *Web's Hot New Commodity*, *supra* note 17.

data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was $1,349.[25]

63. The value of Plaintiff's and Class members' Private Information on the black market is substantial. Sensitive financial information can sell for as much as $1000.[26] This information is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's information.

64. The ramifications of ASG's failure to keep the Private Information of the individuals on its system secure are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to 12 months or even longer.

65. Approximately 21% of victims do not realize their identify has been compromised until more than two years after it has happened.[27] This gives thieves ample time to make fraudulent charges under the victim's name.

66. At all relevant times, Defendant was well-aware, or reasonably should have been aware, that the Private Information it maintains is highly sensitive and could be used for wrongful purposes by third parties, such as identity theft and fraud. Defendant should have particularly been aware of these risks given the significant number of data breaches affecting the insurance industry and related industries.

---

25 *See* U.S. Dep't of Justice, *Victims of Identity Theft,* OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf [hereinafter *Victims of Identity Theft*].

26 *See* Zachary Ignoffo, *Dark Web Price Index 2021*, PRIVACY AFFAIRS (Nov. 21, 2021), https://www.privacyaffairs.com/dark-web-price-index-2021/

27 *See Medical ID Theft Checklist*, IDENTITYFORCE https://www.identityforce.com/blog/medical-id-theft-checklist-2.

67. Had Defendant remedied the deficiencies in its security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, Defendant would have prevented the ransomware attack into its systems and, ultimately, the theft of the Privtae Information of the individuals on its system.

68. The compromised Private Information in the Data Breach is of great value to hackers and thieves and can be used in a variety of ways. Information about, or related to, an individual for which there is a possibility of logical association with other information is of great value to hackers and thieves. Indeed, "there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII."[28] For example, different PII elements from various sources may be able to be linked in order to identify an individual, or access additional information about or relating to the individual.[29] Based upon information and belief, the unauthorized parties utilized the Private Information they obtained through the Data Breach to obtain additional information from Plaintiff and Class members that has been misused.

69. In addition, as technology advances, computer programs may scan the Internet with wider scope to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible. This is known as the "mosaic effect."

---

[28] *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report*, FED. TRADE COMM'N 35-38 (Dec. 2010), https://www.ftc.gov/reports/preliminary-ftc-staff-report-protecting-consumer-privacy-era-rapid-change-proposed-framework.

[29] *See id.* (evaluating privacy framework for entities collecting or using consumer data with can be "reasonably linked to a specific consumer, computer, or other device").

70. Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts. Thus, even if payment card information were not involved in the Data Breach, the unauthorized parties could use Plaintiff's and Class members' Private Information to access accounts, including, but not limited to email accounts and financial accounts.

71. Given these facts, any company that transacts business with customers and then compromises the Private Information of individuals provided to it as part of that transaction, has thus deprived those individuals of the full monetary value of their transaction, implied or explicit, with the company.

72. Acknowledging the damage already realized (and substantially likely to continue to become realized in the future) to Plaintiff and Class members, Defendant instructed individuals like Plaintiff to "remain vigilant against incidents of identity theft and fraud, to review your account statements, explanation of benefits, and credit reports for suspicious activity." Plaintiff and Class members now face a greater risk of identity theft.

73. In short, the Private Information exposed is of great value to hackers and cyber criminals and the data compromised in the Data Breaches can be used in a variety of unlawful manners, including opening new credit and financial accounts in users' names. Plaintiff and Class members have a property interest in their information and were deprived of this property when it was released to unauthorized actors through the negligent maintenance of Defendant's systems.

D. ASG Failed to Comply with FTC Guidelines

74. ASG was 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).

75. 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.[30]

76. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses.[31] The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

77. The FTC further recommends that companies not maintain Private Information 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.[32]

---

[30] *Start With Security: A Guide for Business*, FED. TRADE. COMM'N (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf [hereinafter *Start with Security*].

[31] *Protecting Personal Information: A Guide for Business*, FED. TRADE. COMM'M (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf- 0136_proteting-personal-information.pdf.

[32] *Start With Security: A Guide for Business*, FED. TRADE. COMM'N (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf [hereinafter Start with Security].

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

79. ASG was at all times fully aware of its obligation to protect the Private Information of individuals on its systems as a company that provides insurance services. ASG was also aware of the significant repercussions that would result from its failure to do so.

E. Damages to Plaintiff and the Class

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

81. The ramifications of ASG's failure to keep Plaintiff's and Class members' Private Information secure are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to the victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.[33]

82. In addition to its obligations under state laws and regulations, Defendant owed a common law duty to Plaintiff and Class members to protect Private Information entrusted to it, including to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized parties.

[33] *2014 LexisNexis True Cost of Fraud Study*, LEXISNEXIS (Aug. 2014), https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf.

83. Defendant further owed and breached its duty to Plaintiff and Class members to implement processes and specifications that would detect a breach of its security systems in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

84. As a direct result of Defendant's intentional, willful, reckless, and negligent conduct which resulted in the Data Breach, unauthorized parties were able to access, acquire, view, publicize Plaintiff's and Class members' Private Information as detailed above, and Plaintiff and Class members are now at a heightened and increased risk of identity theft and fraud.

85. The risks associated with identity theft are serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or denied loans for education, housing, or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

86. Some of the risks associated with the loss of personal information have already manifested themselves in Plaintiff Smith's case. Plaintiff Smith received a cryptically written notice letter from Defendant stating that her information was released, and that she should remain vigilant of fraudulent activity on her accounts, with no other explanation of where this information could have gone, or who might have access to it. Plaintiff Zelenski has already spent hours on the phone trying to determine what negative effects may occur from the loss of her personal information.

87. Plaintiff and the Class have suffered or face a substantial risk of suffering out-of-pocket losses such as fraudulent charges on online accounts, credit card fraud, loans opened in their names, and similar identity theft.

88. Plaintiff and Class members have, may have, and/or will have incurred out of pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

89. Plaintiff and Class members did not receive the full benefit of their implicit bargain, and instead received services that were of a diminished value to that described in their agreements with ASG. They were damaged in an amount at least equal to the difference in the value of the services with data security protection they paid for and the services they received.

90. Plaintiff and Class members would not have obtained services from Defendant had Defendant told them that it failed to properly train its employees, lacked safety controls over its computer network, and did not have proper data security practices to safeguard their Private Information from theft.

91. Plaintiff and the Class will continue to spend significant amounts of time to monitor their financial accounts for fraudulent misuse of their compromised Private Information.

92. The theft of Social Security Numbers, which were purloined as part of the Data Breach, is particularly detrimental to victims. The U.S. Social Security Administration ("SSA") warns that "[i]dentity theft is one of the fastest growing crimes in America."[34] The SSA has stated that "[i]dentity 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

34 *Identity Theft And Your Social Security Number*, SOCIAL SECURITY ADMIN. (Dec. 2013), http://www.ssa.gov/pubs/EN-05-10064.pdf.

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."[35] In short, "[s]omeone illegally using your Social Security number and assuming your identity can cause a lot of problems."[36]

93. In fact, a new Social Security number is substantially less effective where "other personal information, such as [the victim's] name and address, remains the same" and for some victims, "a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under your new number may make it more difficult for you to get credit."[37]

94. Identity thieves can use the victim's Private Information to commit any number of frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest. Private Information can be used to submit false insurance claims. As a result, Plaintiff and Class members now face a real and continuing immediate risk of identity theft and other problems associated with the disclosure of their Social Security numbers and will need to monitor their credit for an indefinite duration. For Plaintiff and Class members, this risk creates unending feelings of fear and annoyance. Private information is especially valuable to identity thieves. Defendant knew or should have known this and strengthened its data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

[35] *Id.*
[36] *Id.*
[37] *Id.*

95. As a result of the Data Breach, Plaintiff and Class members' Private Information has diminished in value.

96. The Private Information belonging to Plaintiff and Class members is private, private in nature, and was left inadequately protected by Defendant who did not obtain Plaintiff's or Class members' consent to disclose such Private Information to any other person as required by applicable law and industry standards. Defendant disclosed information about Plaintiff and the class that was of an extremely personal, sensitive nature as a direct result of its inadequate security measures.

97. The Data Breach was a direct and proximate result of Defendant's failure to (a) properly safeguard and protect Plaintiff's and Class members' Private Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class members' Private Information; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

98. Defendant had the resources necessary to prevent the Data Breach, but neglected to adequately implement data security measures, despite its obligation to protect consumer data.

99. Defendant did not properly train its employees to identify and avoid unauthorized access to the network.

100. Had Defendant remedied the deficiencies in their data security systems and adopted security measures recommended by experts in the field, they would have prevented the intrusions into its systems and, ultimately, the theft of Plaintiff's and Class members' Private Information.

101. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

102. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, twenty-nine percent spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[38]

103. Other than offering one year of credit monitoring, Defendant did not take any measures to assist Plaintiff and Class members other than telling them to simply do the following:

- remain vigilant for incidents of fraud and identity theft;
- review account statements and monitor credit reports for unauthorized activity;
- obtain a copy of free credit reports;
- contact the FTC and/or the state Attorney General's office;
- enact a security freeze on credit files; and
- create a fraud alert.

None of these recommendations, however, require Defendant to expend any effort to protect Plaintiff's and Class members' Private Information.

[38] *See* U.S. Dep't of Justice, *Victims of Identity Theft,* OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf [hereinafter *Victims of Identity Theft*].

104. Defendant's failure to adequately protect Plaintiff's and Class members' Private Information has resulted in Plaintiff and Class members having to undertake these tasks, which require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money–while Defendant sits by and does nothing to assist those affected by the incident. Instead, as ASG's Data Breach Notice indicates, it is putting the burden on Plaintiff and Class members to discover possible fraudulent activity and identity theft.

105. While Defendant offered one year of credit monitoring, Plaintiff could not trust a company that had already breached her data. The credit monitoring offered from Equifax does not guarantee privacy or data security for Plaintiff, who would have to expose her information once more to get monitoring services. Thus, to mitigate harm, Plaintiff and Class members are now burdened with indefinite monitoring and vigilance of their accounts.

106. Moreover, the offer of one year of identity monitoring to Plaintiff and Class members is woefully inadequate. While some harm has already begun, the worst may be yet to come. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is acquired and when it is used. Furthermore, identity monitoring only alerts someone to the fact that they have already been the victim of identity theft (i.e., fraudulent acquisition and use of another person's Private Information) – it does not prevent identity theft.[39] This is especially true for many kinds of financial identity theft, for which most credit monitoring plans provide little or no monitoring or protection.

[39] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, CNBC (Nov. 30, 2017), https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-beworth-the-cost.html.

107. Plaintiff and Class members have been damaged in several other ways as well. Plaintiff and Class members have been exposed to an impending, imminent, and ongoing increased risk of fraud, identity theft, and other misuse of their Private Information. Plaintiff and Class members must now and indefinitely closely monitor their financial and other accounts to guard against fraud. This is a burdensome and time-consuming activity. Plaintiff and Class members also suffered a loss of the inherent value of their Private Information.

108. The Private Information stolen in the Data Breach can be misused on its own or can be combined with personal information from other sources of publicly available information, including but not limited to, social media accounts, to create a package of information capable of being used to commit further identity theft. Thieves can also use the stolen Private Information to send spear-phishing emails to Plaintiff and Class members to defraud them into revealing sensitive information. Lulled by a false sense of trust and familiarity from a seemingly valid sender (for example Wells Fargo, Amazon, or a government entity), the individual agrees to provide sensitive information requested in the email, such as login credentials, account numbers, and the like.

109. As a result of Defendant's failures to prevent the Data Breach, Plaintiff and Class members have suffered, will suffer, and are at increased risk of suffering:

- The compromise, publication, theft and/or unauthorized use of their Private Information;
- Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;
- Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

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

- Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class members; and

- Anxiety and distress resulting fear of misuse of their Private Information.

110. In addition to a remedy for the economic harm, Plaintiff and Class members maintain an undeniable interest in ensuring that their Private Information remains secure and is not subject to further misappropriation and theft.

CLASS ACTION ALLEGATIONS

111. Plaintiff incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

112. Plaintiff brings this action individually and on behalf of all other persons similarly situated (the "Class") pursuant to Federal Rule of Civil Procedure 23.

113. Plaintiff proposes the following Class definition subject to amendment based on information obtained through discovery. Notwithstanding, at this time, Plaintiff brings this action and seeks certification of the following Nationwide Class and Texas Subclass (collectively defined herein as the "Class"):

Nationwide Class

> All persons nationwide whose Private Information was compromised as a result of the Data Breach discovered on or about March of 2021 and who were sent notice of the Data Breach.

Texas Subclass

> All persons residing in Texas whose Private Information was compromised as a result of the Data Breach discovered on or about March of 2021 and who were sent notice of the Data Breach.

Excluded from the Class are Defendant and Defendant's affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

114. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

115. **Numerosity—Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that joinder of all Class members would be impracticable. On information and belief, the Nationwide Class numbers in the thousands.

116. **Commonality and Predominance—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all members of the Class and predominate over questions affecting only individual members of the Class. Such common questions of law or fact include, *inter alia*:

- Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;
- Whether Defendant properly implemented its purported security measures to protect Plaintiff's and the Class's Private Information from unauthorized capture, dissemination, and misuse;

- Whether Defendant took reasonable measures to determine the extent of the Data Breach after it first learned of same;
- Whether Defendant disclosed Plaintiff's and the Class's Private Information in violation of the understanding that the Private Information was being disclosed in confidence and should be maintained;
- Whether Defendant willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiff's and the Class's Private Information;
- Whether Defendant was negligent in failing to properly secure and protect Plaintiff's and the Class's Private Information;
- Whether Defendant was unjustly enriched by its actions; and
- Whether Plaintiff and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

117. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of herself and other members of the Class. Similar or identical common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that predominate in this action.

118. **Typicality—Federal Rule of Civil Procedure 23(a)(3).** Plaintiff's claims are typical of the claims of the other members of the Class because, among other things, all Class members were similarly injured through Defendant's uniform misconduct described above and were thus all subject to the Data Breach alleged herein. Further, there are no defenses available to Defendant that are unique to Plaintiff.

119. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4).** Plaintiff is an adequate representative of the Nationwide Class because her interests do not conflict

with the interests of the Classes she seeks to represent, she has retained counsel competent and experienced in complex class action litigation, and Plaintiff will prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiff and their counsel.

120. **Injunctive Relief—Federal Rule of Civil Procedure 23(b)(2).** Defendant has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. Civ. P. 23 (b)(2).

121. **Superiority—Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and the other members of the Class are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for members of the Class to individually seek redress for Defendant's wrongful conduct. Even if members of the Class could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

COUNT I
Negligence
(On Behalf of Plaintiff and the Nationwide Class, or Alternatively, Plaintiff and the Texas Subclass)

122. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

123. Upon Defendant's accepting and storing the Private Information of Plaintiff and the Class in its computer systems and on its networks, Defendant undertook and owed a duty to Plaintiff and the Class to exercise reasonable care to secure and safeguard that Information and to use commercially reasonable methods to do so. Defendant knew that the Private Information was private and confidential and should be protected as such.

124. Defendant owed a duty of care not to subject Plaintiff's and the Class's Private Information to an unreasonable risk of exposure and theft because Plaintiff and the Class were foreseeable and probable victims of any inadequate data security practices.

125. Defendant owed numerous duties to Plaintiff and the Class, including the following:

- to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting Private Information in their possession;
- to protect Private Information using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and
- to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

126. Defendant also breached its duty to Plaintiff and Class members to adequately protect and safeguard Private Information by disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to

unsecured Private Information. Furthering their dilatory practices, Defendant failed to provide adequate supervision and oversight of the Private Information with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted a malicious third party to gather Plaintiff's and Class members' Private Information and potentially misuse the Private Information and intentionally disclose it to others without consent.

127. Defendant knew, or should have known, of the risks inherent in collecting and storing Private Information and the importance of adequate security. Defendant knew or should have known about numerous well-publicized data breaches.

128. Defendant knew, or should have known, that its data systems and networks did not adequately safeguard Plaintiff's and Class members' Private Information.

129. Defendant breached its duties to Plaintiff and Class members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff and Class members' Private Information.

130. Because Defendant knew that a breach of its systems would damage thousands, including Plaintiff and Class members, Defendant had a duty to adequately protect its data systems and the Private Information contained thereon.

131. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Class members, which is recognized by laws and regulations including but not limited to common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class members from a data breach.

132. As further evidence of its negligence, Defendant also failed in its duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. §

45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

133. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

134. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff and Class members and their Private Information. Defendant's misconduct included failing to: (1) secure Plaintiff's and Class member's Private Information; (2) comply with industry standard security practices; (3) implement adequate system and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

135. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class members' Private Information, and by failing to provide timely notice of the Data Breach. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- Failing to adopt, implement, and maintain adequate security measures to safeguard Class members' Private Information;
- Failing to adequately monitor the security of Defendant's networks and systems;
- Allowing unauthorized access to Class members' Private Information;
- Failing to detect in a timely manner that Class members' Private Information had been compromised; and

  Failing to timely notify Class members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages

136. Through Defendant's acts and omissions described in this Complaint, including its failure to provide adequate security and failure to protect Plaintiff's and Class members' Private Information from being foreseeably captured, accessed, disseminated, stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiff's and Class members' Private Information during the time it was within Defendant's possession or control.

137. Defendant's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to failing to adequately protect the Private Information and failing to provide Plaintiff and Class members with timely notice that their sensitive Private Information had been compromised.

138. Neither Plaintiff nor other Class members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint.

139. As a direct and proximate cause of Defendant's conduct, Plaintiff and Class members suffered damages as alleged above.

140. Plaintiff and Class members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide lifetime free credit monitoring to all Class members.

COUNT II
Breach of Third-Party Beneficiary Contract
(On Behalf of Plaintiff and the Nationwide Class, or Alternatively, Plaintiff and the Texas Subclass)

141. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

142. Plaintiff brings this claim for breach of third-party beneficiary contract against ASG.

143. Alacrity Solutions Group entered into contracts with its business customers to provide insurance claims services to consumers, such as Plaintiff and Class members. Upon information and belief, these contracts are virtually identical and similarly contemplate the adequate safeguarding of Plaintiff's and Class members' Private Information.

144. These contracts were made expressly for the benefit of Plaintiff and the Class, as it was their confidential Private Information that ASG agreed to collect and protect through its services. Thus, the benefit of collection and protection of the Private Information belonging to Plaintiff and the Class was the direct and primary objective of the contracting parties.

145. ASG knew that if it were to breach these contracts with its customers, the information of the insured individuals provided to ASG, including Plaintiff and the Class, would be harmed by, among other harms, fraudulent transactions.

146. ASG breached its contract with the medical providers affected by this Data Breach when it failed to use reasonable data security measures that could have prevented the Data Breach.

147. As foreseen, Plaintiff and the Class were harmed by ASG's failure to use reasonable security measures to store private information, including but not limited to the risk of harm through the loss of their personal information.

148. Accordingly, Plaintiff and the Class are entitled to damages in an amount to be determined at trial, along with their costs and attorney fees incurred in this action.

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiff and the Nationwide Class, or Alternatively, Plaintiff and the Texas Subclass)

149. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

150. Plaintiff brings this claim for breach of implied contract alternatively to her breach of third-party beneficiary contract claim.

151. Through their course of conduct, Defendant, Plaintiff, and Class members entered into implied contracts for the provision of insurance services, as well as implied contracts for the Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class members' Private Information.

152. Specifically, Plaintiff entered into a valid and enforceable implied contract with Defendant when she first entered into the insurance services agreement with Defendant.

153. The valid and enforceable implied contracts to provide insurance services that Plaintiff and Class members entered into with Defendant include Defendant's promise to protect nonpublic Private Information given to Defendant or that Defendant creates on its own from disclosure.

154. When Plaintiff and Class members provided their Private Information to Defendant in exchange for Defendant's services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

155. Defendant solicited and invited Class members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class members accepted Defendant's offers and provided their Private Information to Defendant.

156. In entering into such implied contracts, Plaintiff and Class members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, and were consistent with industry standards.

157. Class members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

158. Under implied contracts, Defendant and/or its affiliated providers promised and were obligated to: (a) provide insurance services to Plaintiff and Class members; and (b) protect Plaintiff's and the Class members' Private Information provided to obtain such benefits of such services. In exchange, Plaintiff and Members of the Class agreed to pay money for these services, and to turn over their Private Information.

159. Both the provision of financial services and the protection of Plaintiff's and Class members' Private Information were material aspects of these implied contracts.

160. The implied contracts for the provision of insurance services—contracts that include the contractual obligations to maintain the privacy of Plaintiff's and Class members' Private Information—are also acknowledged, memorialized, and embodied in multiple documents, including (among other documents) Defendant's Data Breach notification letter.

161. Defendant's express representations, including, but not limited to the express representations found in its Privacy Notice, memorialize and embody the implied contractual

obligation requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and protect the privacy of Plaintiff's and Class members Private Information.

162. Consumers of financial and insurance services value their privacy, the privacy of their dependents, and the ability to keep their Private Information associated with obtaining such services. Plaintiff and Class members would not have entrusted their Private Information to Defendant and entered into these implied contracts with Defendant without an understanding that their Private Information would be safeguarded and protected or entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

163. A meeting of the minds occurred, as Plaintiff and Class members agreed and provided their Private Information to Defendant and/or its affiliated companies, and paid for the provided services in exchange for, amongst other things, both the provision of insurance services and the protection of their Private Information.

164. Plaintiff and Class members performed their obligations under the contract when they paid for Defendant's services and provided their Private Information.

165. Defendant materially breached its contractual obligation to protect the nonpublic Private Information Defendant gathered when the information was accessed and exfiltrated by the Data Breach.

166. Defendant materially breached the terms of the implied contracts, including, but not limited to, the terms stated in the relevant Notice of Privacy Practices. Defendant did not maintain the privacy of Plaintiff's and Class members' Private Information as evidenced by its notifications of the Data Breach to Plaintiff and Class members. Specifically, Defendant did not

comply with industry standards, standards of conduct embodied in statutes like Section 5 of the FTCA, or otherwise protect Plaintiff's and Class members' private information as set forth above.

167. The Data Breach was a reasonably foreseeable consequence of Defendant's action in breach of these contracts.

168. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiff and Class members did not receive full benefit of the bargain, and instead received financial and other services that were of a diminished value to that described in the contracts. Plaintiff and Class members therefore were damaged in an amount at least equal to the difference in the value of the lending services with data security protection they paid for and the services they received.

169. Had Defendant disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiff, Class members, nor any reasonable person would have utilized services from Defendant and/or its affiliated entities by entering into these implied contracts.

170. As a direct and proximate result of the Data Breach, Plaintiff and Class members have been harmed and suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the future, out of pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

171. Plaintiff and Class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

172. Plaintiff and Class members are also entitled to injunctive relief requiring Defendant to, *e.g.,* (i) strengthen its data security systems and monitoring procedures; (ii) submit

to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class members.

COUNT IV
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Nationwide Class, or Alternatively, Plaintiff and the Texas Subclass)

173. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

174. In providing their Private Information to Defendant, Plaintiff and Class members justifiably placed a special confidence in Defendant to act in good faith and with due regard to interests of Plaintiff and Class members to safeguard and keep confidential that Private Information.

175. Defendant accepted the special confidence Plaintiff and Class members placed in it, as evidenced by its assertion that it is "committed to protecting the privacy of [Plaintiff's] personal information" as included in the Data Breach notification letter.

176. In light of the special relationship between Defendant and Plaintiff and Class members, whereby Defendant became a guardian of Plaintiff's and Class members Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for the benefit of the individuals it provides insurance claims services to, including Plaintiff and Class members for the safeguarding of Plaintiff and Class member's Private Information.

177. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of its customer's relationship, in particular, to keep secure the Private Information of the individuals on its computer systems.

178. Defendant breached its fiduciary duties to Plaintiff and Class members by failing to protect the integrity of the systems containing Plaintiff's and Class member's Private Information.

179. Defendant breached its fiduciary duties to Plaintiff and Class members by otherwise failing to safeguard Plaintiff's and Class members' Private Information.

180. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Cyber-Attack and Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Cyber-Attack and Data Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of Defendant's services they received.

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

COUNT V
Declaratory Relief
(On Behalf of Plaintiff and the Nationwide Class)

182. Plaintiff realleges and incorporates by reference all preceding allegations as if fully set forth herein.

183. 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.

184. 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 Plaintiff's and Class members' PII, and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and Class members from future data breaches that compromise their Private Information. Plaintiff and the Class remain at imminent risk that further compromises of their PII will occur in the future.

185. The Court should also issue prospective injunctive relief requiring Defendant to employ adequate security practices consistent with law and industry standards to protect consumers' PII.

186. Defendant still possesses the PII of Plaintiff and the Class.

187. To Plaintiff's knowledge, Defendant has made no changes to its data storage or security practices relating to the PII.

188. To Plaintiff's 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.

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

190. The hardship to Plaintiff 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 ASG, Plaintiff 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.

191. 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 ASG, thus eliminating the additional injuries that would result to Plaintiff and Class members, along with other consumers whose PII would be further compromised.

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

- 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 ASG's systems on a periodic basis, and ordering ASG to promptly correct any problems or issues detected by such third-party security auditors;
- engaging third-party security auditors and internal personnel to run automated security monitoring;

- auditing, testing, and training its security personnel regarding any new or modified procedures;
- purging, deleting, and destroying Private Information not necessary for its provisions of services in a reasonably secure manner;
- conducting regular database scans and security checks; and
- 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, Plaintiff, individually and on behalf of the other members of the Class proposed in this Complaint, respectfully requests that the Court enter judgment in favor of Plaintiff and the Class and against Defendant, as follows:

A. For an Order certifying this action as a class action and appointing Plaintiff and her counsel to represent the Class;

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

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

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained by Defendant as a result of its wrongful conduct;

E. Ordering Defendant to pay for no less than three (3) years of credit monitoring services for Plaintiff and the Class;

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

G. For an award of punitive damages, as allowable by law;

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

I. Pre- and post-judgment interest on any amounts awarded; and

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

JURY DEMAND

Plaintiff demands a trial by jury on all issues so triable.

Dated: May 18, 2022

/s/ P. Bradford deLeeuw
P. Bradford deLeeuw (#3569)
DELEEUW LAW LLC
1301 Walnut Green Road
Wilmington, DE 19807
(302) 274-2180
(302) 351-6905 (fax)
brad@deleeuwlaw.com

OF COUNSEL:

Nicholas A. Migliaccio
Jason S. Rathod
Tyler Bean
Kevin Leddy
MIGLIACCIO & RATHOD LLP
412 H Street NE
Washington, DC 20002
Tel: (202) 470-3520
Email: nmigliaccio@classlawdc.com
Email: jrathod@classlawdc.com