IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF GEORGIA
COLUMBUS DIVISION

JESSICA BATISTE, *individually and on behalf of all others similarly situated,* Plaintiff, v. AFLAC INCORPORATED, Defendant.	Case No.: 4:25-cv-00185 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff, Jessica Batiste ("Plaintiff"), individually and on behalf of the Class defined below of similarly situated persons, alleges the following against Defendant Aflac Incorporated ("Defendant"), based upon Plaintiff's personal knowledge and on information and belief derived from, among other things, investigation by counsel as to all other matters:

SUMMARY OF THE CASE

1. This action arises from Defendant's failure to secure the personally identifiable information ("PII")[1] and protected health information ("PHI")[2]

[1] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8).
[2] Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d

(collectively, "Private Information") of Plaintiff and the members of the proposed Class, where Plaintiff provided her Private Information to Defendant for supplemental insurance services and products.

2. According to its website,

> [Defendant] is a Fortune 500 company, providing financial protection to millions of policyholders and customers through its subsidiaries in the U.S. and Japan. When a policyholder or insured gets sick or hurt, Aflac pays cash benefits promptly, for eligible claims, directly to the insured (unless assigned otherwise). For more than six decades, Aflac voluntary insurance policies have given policyholders the opportunity to focus on recovery, not financial stress.[3]

3. On or about June 20, 2025, Defendant began sending emails entitled "Aflac Cybersecurity Incident" ("Notice Email") to Plaintiff and Class Members, advising them that it recently detected suspicious activity on its network. In its Notice Email, Defendant advises that its investigation into the cybersecurity incident is ongoing and that it has yet not confirmed the extent of unauthorized activity, potentially impacted data, or the customers or other individuals impacted in the

et seq., and its implementing regulations ("HIPAA"), "protected health information" is defined as individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103 *Protected health information*. "Business Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. *Summary of the HIPAA Privacy Rule*, DEP'T FOR HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

[3] https://www.aflac.com/about-aflac/default.aspx.

cybersecurity incident ("Data Breach").

4. According to the Notice Email, the Private Information intruders accessed and infiltrated from Defendant's systems included claims information, health information, social security numbers, and/or other personal information, related to customers, beneficiaries, employees, agents, and other individuals in Defendant's U.S. business.

5. As a result of the Data Breach, which Defendant failed to prevent, the Private Information of Plaintiff and the proposed Class Members, was stolen.[4]

6. Instead, Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, and/or negligently failing to implement reasonable measures to safeguard the Private Information of its current and former customers, beneficiaries, employees, agents, and other individuals in its U.S. business, and by failing to take necessary steps to prevent unauthorized disclosure of that information. Defendant's woefully inadequate data security measures made the Data Breach a foreseeable, and even likely, consequence of its negligence.

7. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have suffered actual and present injuries, including but not limited to: (a) present, certainly impending, and continuing threats of identity theft crimes, fraud,

[4] *Id*.

scams, and other misuses of their Private Information; (b) diminution of value of their Private Information; (c) loss of benefit of the bargain (price premium damages); (d) loss of value of privacy and confidentiality of the stolen Private Information; (e) illegal sales of the compromised Private Information; (f) mitigation expenses and time spent responding to and remedying the effects of the Data Breach; (g) identity theft insurance costs; (h) "out of pocket" costs incurred due to actual identity theft; (i) credit freezes/unfreezes; (j) expense and time spent on initiating fraud alerts and contacting third parties; (k) decreased credit scores; (l) anxiety, annoyance, and nuisance; and (m) continued risk to their Private Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

8. Plaintiff and Class Members would not have provided their valuable Private Information had they known that Defendant would make their Private Information Internet-accessible, not encrypt personal and sensitive data elements, and not delete the Private Information it no longer had reason to maintain.

9. Through this lawsuit, Plaintiff seeks to hold Defendant responsible for the injuries they inflicted on Plaintiff and Class Members due to their impermissibly inadequate data security measures, and to seek injunctive relief to ensure the implementation of security measures to protect the Private Information that remains

in Defendant's possession.

10. The exposure of one's Private Information to cybercriminals is a bell that cannot be un-rung. Before this Data Breach, Plaintiff's and the Class's Private Information was exactly that—private. Not anymore. Now, their Private Information is forever exposed and unsecure.

JURISDICTION AND VENUE

11. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of Class Members is in the millions, many of whom have different citizenship from Defendant. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

12. This Court has personal jurisdiction over Defendant because it is a Georgia corporation that operates and has its principal place of business in this District and conducts substantial business in this District.

13. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Moreover, Defendant is domiciled in this District, maintains Plaintiff's and Class Members' Private Information in this District, and has caused harm to Plaintiff and Class Members in this District.

PARTIES

14. Plaintiff is, and at all relevant times has been, a resident and citizen of Port Arthur, Texas.

15. Defendant is a Georgia corporation with its headquarters and principal place of business located at 1932 Wynnton Road, Columbus, Georgia 31999.

FACTUAL ALLEGATIONS

A. The Data Breach

16. Plaintiff and Class Members were required to provide Defendant with their sensitive and confidential Private Information, including their names, claims information, health information, Ssocial Security numbers, and other sensitive information, that at the time of the Data Breach were held by Defendant in its computer systems.

17. The Notice Email sent by Defendant to Plaintiff and Class Members states:

> We are writing to inform you of a cybersecurity incident at Aflac that may have impacted data we maintain about our policies.
>
> **What Happened**
>
> Aflac recently detected suspicious activity on its network. Upon detection, we promptly took steps to contain the activity and launched an investigation with the support of third-party experts. While it is unfortunate that this has occurred, we want to let you know what it means for you and what we are doing to support customers as we work diligently to respond to and navigate this incident.

…

> [T]he investigation remains in its early stages. At this time, we have not confirmed the extent of unauthorized activity, potentially impacted data, or the customers or other individuals impacted. We have commenced a review of potentially impacted files. It is important to note that the review is in its early stages, and we are unable to determine the total number of affected individuals until that review is completed. The potentially impacted files may contain claims information, health information, social security numbers, and/or other personal information, related to customers, beneficiaries, employees, agents, and other individuals in its U.S. business. Based on intelligence coming from the cybersecurity community, we have been told that this incident may be part of a broader series of cyber-attacks targeting the insurance industry.

18. In the Notice Email, Defendant offers Plaintiff and Class Members 24 months of credit monitoring and provides a dedicated call center to answer questions they may have about the Data Breach.

19. In the context of notice of data breach communications of this type, Defendant's use of the phrase "may have impacted data" is misleading lawyer language. Companies only send notice letters because data breach notification laws require them to do so. And such letters are only sent to those persons who Defendant itself has a reasonable belief that such personal information was accessed or acquired by an unauthorized individual or entity. Defendant cannot hide behind legalese; by sending a Notice Letter to Plaintiff and Class Members, it admits that Defendant itself has a reasonable belief that Plaintiff's and Class Members' Private Information was accessed or acquired by cybercriminals.

20. On June 20, 2025, Defendant also posted a press release on its website, entitled "Aflac Incorporated Discloses Cybersecurity Incident" ("Online Disclosure"). The Online Disclosure states:

> On June 12, 2025, Aflac Incorporated (NYSE: AFL) identified suspicious activity on our network in the United States. We promptly initiated our cyber incident response protocols and stopped the intrusion within hours. Importantly, our business remains operational, and our systems were not affected by ransomware. We continue to serve our customers as we respond to this incident and can underwrite policies, review claims, and otherwise service our customers as usual. This attack, like many insurance companies are currently experiencing, was caused by a sophisticated cybercrime group. This was part of a cybercrime campaign against the insurance industry.
>
> We have engaged leading third-party cybersecurity experts to support our response to this incident. While the investigation remains in its early stages, in the spirit of transparency and care for our customers, we are sharing that our preliminary findings indicate that the unauthorized party used social engineering tactics to gain access to our network. Additionally, we have commenced a review of potentially impacted files. It is important to note that the review is in its early stages, and we are unable to determine the total number of affected individuals until that review is completed. The potentially impacted files contain claims information, health information, social security numbers, and/or other personal information, related to customers, beneficiaries, employees, agents, and other individuals in our U.S. business. We remain committed to caring for and supporting our customers. While our teams work to review the potentially impacted data and determine the specific information involved, we are offering **any individual who contacts our dedicated call center free credit monitoring and identity theft protection, and Medical Shield for 24 months.**[5]

[5] https://newsroom.aflac.com/2025-06-20-Aflac-Incorporated-Discloses-Cybersecurity-Incident.

21. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiff and Class Members, such as encrypting the information or purging it when it is no longer needed, causing the exposure of Private Information.

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

B. The Value of Private Information

23. In April 2020, ZDNet reported in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year", that "[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize damage, leak corporate information on dark web portals, and even tip journalists to generate negative news for complaints as revenge against those who refuse to pay."[6]

24. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that "[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly

[6] https://www.zdnet.com/article/ransomeware-mentioned-in-1000-sec-filings-over-the-past-year/.

naming and shaming victims as secondary forms of extortion."[7]

25. Stolen Private Information is often trafficked on the dark web, as is the case here. Law enforcement has difficulty policing the dark web due to this encryption, which allows users and criminals to conceal identities and online activity.

26. When malicious actors infiltrate companies and copy and exfiltrate the Private Information that those companies store, that stolen information often ends up on the dark web because the malicious actors buy and sell that information for profit.[8]

27. Another example is when the U.S. Department of Justice announced its seizure of AlphaBay in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another person's identity. Other marketplaces, similar to the now-defunct AlphaBay, "are awash with [Private Information] belonging to victims from countries all over the world. One of the key challenges of protecting Private Information online is its pervasiveness. As data breaches in the news continue to show, Private Information about employees, customers, and the public is housed in all kinds of organizations,

[7] *See* https://www.cisa.gov/sites/default/files/2023-01-CISA_MSISAC_Ransomware%20Guide__8508C.pdf.
[8] *Shining a Light on the Dark Web with Identity Monitoring, IdentityForce*, Dec. 28, 2020, https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring.

and the increasing digital transformation of today's businesses only broadens the number of potential sources for hackers to target."[9]

28. The Private Information of consumers 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, Private Information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $2009.[10] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[11] Criminals can also purchase access to entire company data breaches.[12]

29. Once Private Information is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional Private Information being harvested from the victim, as well as Private Information from family, friends and colleagues of the original victim.

30. According to the FBI's Internet Crime Complaint Center (IC3) 2019

[9] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, Armor, April 3, 2018, https://www.armor.com/resources/blog/stolen-pii- ramifications- identity-theft-fraud-dark-web/.
[10] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, https://www.digitaltrends.com/computing/personal- data-sold-on-the-dark-web- how-much-it-costs/.
[11] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is- selling-for-on-the-dark-web/.
[12] *In the Dark*, VPNOverview, 2019, https://vpnoverview.com/privacy/anonymous-browsing/in-the- dark/.

Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than $3.5 billion in losses to individuals and business victims.

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

32. Data breaches facilitate identity theft as hackers obtain consumers' Private Information and thereafter use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' Private Information to others who do the same.

33. For example, the United States Government Accountability Office noted in a June 2007 report on data breaches (the "GAO Report") that criminals use Private Information to open financial accounts, receive government benefits, and make purchases and secure credit in a victim's name.[13] The GAO Report further notes that this type of identity fraud is the most harmful because it may take some time for a victim to become aware of the fraud, and can adversely impact the victim's credit rating in the meantime. The GAO Report also states that identity theft victims will face "substantial costs and inconveniences repairing damage to their credit

[13] *See* Government Accountability Office, *Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown* (June 2007), https://www.gao.gov/assets/gao- 07-737.pdf.

records . . . [and their] good name."[14]

34. The market for Private Information has continued unabated to the present, and in 2023 the number of reported data breaches in the United States increased by 78% over 2022, reaching 3205 data breaches.[15]

35. The exposure of Plaintiff's and Class Members' Private Information to cybercriminals will continue to cause substantial risk of future harm (including identity theft) that is continuing and imminent in light of the many different avenues of fraud and identity theft utilized by third-party cybercriminals to profit off of this highly sensitive information.

C. Defendant Failed to Comply with Regulatory Requirements and Standards.

36. Federal and state regulators have established security standards and issued recommendations to temper data breaches and the resulting harm to consumers and employees. There are a number of state and federal laws, requirements, and industry standards governing the protection of Private Information.

[14] *Id.*
[15] Beth Maundrill, *Data Privacy Week: US Data Breaches Surge, 2023 Sees 78% Increase in Compromises*, INFOSECURITY MAGAZINE (Jan. 23, 2024); https://www.infosecurity-magazine.com/news/us-data-breaches-surge-2023/; *see also* Identity Theft Resource Center, *2023 Data Breach Report*, https://www.idtheftcenter.org/publication/ 2023-data-breach-report/.

37. For example, at least 24 states have enacted laws addressing data security practices that require businesses that own, license, or maintain Private Information about a resident of that state to implement and maintain "reasonable security procedures and practices" and to protect Private Information from unauthorized access.

38. Additionally, cybersecurity firms have promulgated a series of best practices that at a minimum should be implemented by sector participants including, but not limited to: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting of physical security systems; protecting against any possible communication system; and training staff regarding critical points.[16]

39. The Federal Trade Commission ("FTC") has issued several guides for businesses, highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be considered for all business decision-making.[17]

[16] *See Addressing BPO Information Security: A Three-Front Approach*, DATAMARK, INC. (Nov. 2016), https://insights.datamark.net/addressing-bpo-information-security.

[17] *Start With Security*, Fed. Trade Comm'n ("FTC"), https://www.ftc.gov/system/files/ documents/plain-language/pdf0205-startwithsecurity.pdf.

40. Under the FTC's 2016 *Protecting Personal Information: Guide for Business* publication, the FTC notes that businesses should safeguard the personal information they retain; properly dispose of unnecessary personal information; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to rectify security issues.[18]

41. The guidelines also suggest that businesses use an intrusion detection system to expose a breach as soon as it happens, monitor all incoming traffic for activity indicating someone is trying to hack the system, watch for large amounts of data being siphoned from the system, and have a response plan in the event of a breach.

42. The FTC advises companies to not keep information for periods of time longer than needed to authorize a transaction, restrict access to private information, mandate complex passwords to be used on networks, utilize industry-standard methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.[19]

43. The FTC has brought enforcement actions against companies for failing to adequately and reasonably protect consumer data, treating the failure to do so as an unfair act or practice barred by Section 5 of the Federal Trade Commission Act

[18] *Protecting Personal Information: A Guide for Business*, FTC, https://www.ftc.gov/system/files/ documents/plain-language/pdf-0136_proteting-personal-information.pdf.
[19] *Id.*

("FTC Act"), 15 U.S.C. § 45. Orders originating from these actions further elucidate the measures businesses must take to satisfy their data security obligations.

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

45. Defendant's failure to verify that it had implemented reasonable security measures constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

46. Furthermore, Defendant is required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C. The Privacy Rule and the Security Rule set nationwide standards for protecting health information, including health information stored electronically.

47. The Security Rule requires Defendant to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to

the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.[20]

48. Pursuant to HIPAA's mandate that Defendant follows "applicable standards, implementation specifications, and requirements . . . with respect to electronic protected health information," 45 C.F.R. § 164.302, Defendant was required to, at minimum, "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information," 45 C.F.R. § 164.306(e), and "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

49. Defendant is also required to follow the regulations for safeguarding electronic medical information pursuant to the Health Information Technology Act ("HITECH"). *See* 42 U.S.C. § 17921, 45 C.F.R. § 160.103.

50. Both HIPAA and HITECH obligate Defendant to follow reasonable security standards, respond to, contain, and mitigate security violations, and to

[20] *Summary of the HIPAA Security Rule*, HHS, https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.

protect against disclosure of sensitive patient Private Information. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); 45 C.F.R. § 164.530(f); 42 U.S.C. § 17902.

51. As alleged in this Complaint, Defendant has failed to comply with HIPAA and HITECH. It has failed to maintain adequate security practices, systems, and protocols to prevent data loss, failed to mitigate the risks of a data breach and loss of data, and failed to ensure the confidentiality and protection of PHI.

D. Defendant Failed to Comply with Industry Practices.

52. Various cybersecurity industry best practices have been published and should be consulted as a go-to resource when developing an organization's cybersecurity standards. The Center for Internet Security ("CIS") promulgated its Critical Security Controls, which identify the most commonplace and essential cyber-attacks that affect businesses every day and proposes solutions to defend against those cyber-attacks.[21] All organizations collecting and handling Private Information, such as Defendant, are strongly encouraged to follow these controls.

53. Further, the CIS Benchmarks are the overwhelming option of choice for auditors worldwide when advising organizations on the adoption of a secure build standard for any governance and security initiative, including PCI DSS, NIST 800-53, SOX, FISMA, ISO/IEC 27002, Graham Leach Bliley and ITIL.[22]

[21] Center for Internet Security, *Critical Security Controls*, at 1 (May 2021), https://learn.cisecurity.org/CIS-Controls-v8-guide-pdf.

[22] *See CIS Benchmarks FAQ*, Center for Internet Security, https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq/.

54. Several best practices have been identified that a minimum should be implemented by data management companies like Defendant, including but not limited to securely configuring business software, managing access controls and vulnerabilities to networks, systems, and software, maintaining network infrastructure, defending networks, adopting data encryption while data is both in transit and at rest, and securing application software.[23]

55. Defendant failed to follow these and other industry standards to adequately protect the Private Information of Plaintiff and Class Members.

E. The Data Breach Caused Injury to Class Members and Will Result in Additional Harm Such as Fraud.

56. Without detailed disclosure to the victims of the Data Breach, individuals whose Private Information was compromised by the Data Breach, including Plaintiff and Class Members, were unknowingly and unwittingly exposed to continued misuse and ongoing risk of misuse of their Private Information for months without being able to take available precautions to prevent imminent harm.

57. The ramifications of Defendant's failure to secure Plaintiff's and Class Members' data are severe.

58. Victims of data breaches are much more likely to become victims of identity theft and other types of fraudulent schemes. This conclusion is based on an

[23] *See* Center for Internet Security, *Critical Security Controls* (May 2021), https://learn.cisecurity.org/CIS-Controls-v8-guide-pdf.

analysis of four years of data that correlated each year's data breach victims with those who also reported being victims of identity fraud.

59. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[24] 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."[25]

60. Identity thieves can use Private Information, such as that of Plaintiff and Class Members, which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud, such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

61. As demonstrated herein, these and other instances of fraudulent misuse of the compromised Private Information has already occurred and are likely to continue.

62. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend

[24] 17 C.F.R. § 248.201 (2013).
[25] *Id.*

numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[26]

63. The 2017 Identity Theft Resource Center survey[27] evidences the emotional suffering experienced by victims of identity theft:

- 75% of respondents reported feeling severely distressed;
- 67% reported anxiety;
- 66% reported feelings of fear related to personal financial safety;
- 37% reported fearing for the financial safety of family members;
- 24% reported fear for their physical safety;
- 15.2% reported a relationship ended or was severely and negatively impacted by identity theft; and
- 7% reported feeling suicidal.

64. Identity theft can also exact a physical toll on its victims. The same survey reported that respondents experienced physical symptoms stemming from their experience with identity theft:

- 48.3% of respondents reported sleep disturbances;

[26] *Victims of Identity Theft*, Bureau of Justice Statistics (Sept. 2015) http://www.bjs.gov/content/ pub/pdf/vit14.pdf.
[27] *Id.*

- 37.1% reported an inability to concentrate / lack of focus;
- 28.7% reported they were unable to go to work because of physical symptoms;
- 23.1% reported new physical illnesses (aches and pains, heart palpitations, sweating, stomach issues); and
- 12.6% reported a start or relapse into unhealthy or addictive behaviors.[28]

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

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[29]

Thus, Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights.

[28] *Id.*
[29] GAO, *Report to Congressional Requesters*, at 29 (June 2007), http://www.gao.gov/new.items/d07737.pdf.

F. Plaintiff and Class Members Suffered Damages.

66. As a direct and proximate result of Defendant's wrongful actions and inaction and the resulting Data Breach, Plaintiff and Class Members have already been harmed by the fraudulent misuse of their Private Information, and have been placed at an imminent, immediate, and continuing increased risk of additional harm from identity theft and identity 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 both the actual and potential impact of the Data Breach on their lives. Such mitigatory actions include, *inter alia*, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, sorting through dozens of phishing and spam email, text, and phone communications, and filing police reports. This time has been lost forever and cannot be recaptured.

67. Defendant's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and Class Members' Private Information, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. theft and misuse of their personal and financial information;

b. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Private Information being placed in the hands of criminals and misused via the sale of Plaintiff's and Class Members' information on the Internet's black market;

c. the untimely and inadequate notification of the Data Breach;

d. the improper disclosure of their Private Information;

e. loss of privacy;

f. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

g. ascertainable losses in the form of deprivation of the value of their Private Information, for which there is a well-established national and international market;

h. the loss of productivity and value of their time spent to address, attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised

accounts, and the inconvenience, nuisance and annoyance of dealing with all such issues resulting from the Data Breach; and

i. nominal damages.

68. While Plaintiff's and Class Members' Private Information has been stolen, Defendant continues to hold Plaintiff's and Class Members' Private Information. Particularly because Defendant has demonstrated an inability to prevent a breach or stop it from continuing even after being detected, Plaintiff and Class Members have an undeniable interest in ensuring that their Private Information is secure, remains secure, is properly and promptly destroyed, and is not subject to further theft.

G. Plaintiff's Experience.

69. Plaintiff is a customer of Defendant and provided Defendant with her Private Information, including her Social Security number.

70. Plaintiff provided Private Information to Defendant on the condition that it be maintained as confidential and with the understanding that Defendant would employ reasonable safeguards to protect her Private Information.

71. Plaintiff received a Notice Email from Defendant on or about June 20, 2025, advising her of the Data Breach.

72. Since the Data Breach, Plaintiff has experienced anxiety and increased concerns for the loss of her privacy, as well as anxiety over the impact of

cybercriminals accessing and using her Private Information.

73. Plaintiff would not have entrusted her Private Information to Defendant had she known they would not take reasonable steps to safeguard her information.

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

75. Plaintiff is very careful about sharing sensitive Private Information. She stores documents containing Private Information in safe and secure locations and has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source. Plaintiff would not have entrusted her Private Information to Defendant had she known of Defendant's lax data security policies.

76. As a direct and proximate result of the Data Breach, Plaintiff has made reasonable efforts to mitigate the impact of the Data Breach, including by regularly and closely monitoring her financial accounts.

77. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. She has faced and faces a present and continuing risk of fraud and identity theft for her lifetime.

CLASS ALLEGATIONS

78. Plaintiff brings this class action individually and on behalf of the following nationwide class:

> All persons residing in the United States whose Private Information was compromised in the Data Breach ("Class").

79. Excluded from the Class are Defendant and its affiliates, parents, subsidiaries, officers, agents, and directors, any entities in which Defendant has a controlling interest, as well as the judge(s) presiding over this matter and the clerks, judicial staff, and immediate family members of said judge(s).

80. Plaintiff reserves the right to modify or amend the foregoing Class definition before the Court determines whether certification is appropriate.

81. This action may be certified as a class action because it satisfies the numerosity, commonality, typicality, adequacy, and superiority requirements of Rule 23 of the Federal Rules of Civil Procedure.

82. Numerosity: The Class is so numerous that joinder of all Class Members is impracticable. Although the precise number of such persons is unknown, and the facts are presently within the sole knowledge of Defendant, upon information and belief, Plaintiff estimates that the Class is comprised of millions of Class Members. The Class is sufficiently numerous to warrant certification.

83. Typicality of Claims: Plaintiff's claims are typical of those of other Class Members because Plaintiff, like the unnamed Class, had her Private

Information compromised as a result of the Data Breach. Plaintiff is a member of the Class, and her claims are typical of the claims of the members of the Class. The harm suffered by Plaintiff is similar to that suffered by all other Class Members, which was caused by the same misconduct by Defendant.

84. Adequacy of Representation: Plaintiff will fairly and adequately represent and protect the interests of the Class. Plaintiff has no interests antagonistic to, or in conflict with, the Class. Plaintiff has retained competent counsel who are experienced in consumer and commercial class action litigation and who will prosecute this action vigorously.

85. Superiority: A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Because the monetary damages suffered by individual Class Members are relatively small, the expense and burden of individual litigation make it impossible for individual Class Members to seek redress for the wrongful conduct asserted herein. If Class treatment of these claims is not available, Defendant will likely continue its wrongful conduct, will unjustly retain improperly obtained revenues, or will otherwise escape liability for its wrongdoing as asserted herein.

86. Commonality and Predominance: Common questions of law and fact exist as to all Class Members and predominate over any potential questions affecting

only individual Class Members. These common questions of law or fact include, *inter alia*:

a. 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;

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

c. Whether Defendant's storage of Plaintiff's and Class Member's Private Information was done in a negligent manner;

d. Whether Defendant had a duty to protect and safeguard Plaintiff's and Class Members' Private Information;

e. Whether Defendant's conduct was negligent;

f. Whether Defendant's conduct violated Plaintiff's and Class Members' privacy;

g. Whether Defendant's conduct violated the statutes as set forth herein;

h. Whether Defendant took sufficient steps to secure individuals' Private Information;

i. Whether Defendant was unjustly enriched; and

j. The nature of the relief, including damage and equitable relief, to which Plaintiff and Class Members are entitled.

87. Information concerning Defendant's polices is available from Defendant's records.

88. Plaintiff knows of no difficulty which will be encountered in the management of this litigation which would prelude its maintenance as a class action.

89. The prosecution of separate actions by individual members of the Class would run the risk of inconsistent or varying adjudications and establish incompatible standards of conduct for Defendant. Prosecution as a class action will eliminate the possibility of repetitions and inefficient litigation.

90. Given that Defendant has not indicated any changes to its conduct or security measures, monetary damages are insufficient and there is no complete and adequate remedy at law.

CAUSES OF ACTION
COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

91. Plaintiff restates and realleges paragraphs 1 through 90 above as if fully set forth herein.

92. Defendant requires its customers, beneficiaries, employees, and agents to submit non-public Private Information as a condition of receiving services, products, or employment.

93. Defendant gathered and stored the Private Information of Plaintiff and Class Members as part of its business, which affects commerce.

94. Plaintiff and Class Members entrusted Defendant with their Private Information with the understanding that the information would be safeguarded.

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

96. By assuming the responsibility to collect and store this data, Defendant had duties of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft.

97. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the Private Information.

98. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant, on the one hand, and Plaintiff and Class Members, on the other hand. That special relationship arose because Defendant was entrusted with their confidential Private Information as a condition of receiving services, products, or employment from Defendant.

99. Defendant also had a duty to exercise appropriate clearinghouse practices to remove the Private Information of its former customers, beneficiaries, employees, and agents they were no longer required to retain pursuant to regulations.

100. Moreover, Defendant had a duty to promptly and adequately notify Plaintiff and the Class of the Data Breach, but failed to do so.

101. Defendant had and continues to have duties to adequately disclose that Plaintiff's and Class Members' Private Information within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

102. Defendant breached its duties and thus was negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Allowing unauthorized access to Class Members' Private Information;

d. Failing to detect in a timely manner that Class Members' Private Information had been compromised;

e. Failing to remove Private Information of its former customers, beneficiaries, employees, and agents they were no longer required to retain pursuant to regulations; and

f. Failing to adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

103. 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's and Class Members' Private Information.

104. Defendant knew or should have known that its failure to implement reasonable data security measures to protect and safeguard Plaintiff's and Class Members' Private Information would cause damage to Plaintiff and the Class.

105. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

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

107. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of corporate cyberattacks and data breaches.

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

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

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

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

112. Defendant's duties extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which have been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties

are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

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

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

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

116. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) the actual misuse of their compromised Private Information; (ii) invasion of privacy; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data

Breach; (v) loss of benefit of the bargain; (vi) an increase in spam calls, texts, and/or emails (vii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains 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; (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised Private Information for the rest of their lives; (ix) the present value of ongoing credit monitoring and identity defense services necessitated by the Data Breach; (x) the value of the unauthorized access to their Private Information permitted by Defendant; and (xi) any nominal damages that may be awarded.

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

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

119. Defendant's negligent conduct is ongoing, in that it still possesses Plaintiff's and Class Members' Private Information in an unsafe and insecure manner.

120. Plaintiff and Class Members are entitled to injunctive relief requiring Defendant to: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
NEGLIGENCE PER SE
(On Behalf of Plaintiff and the Class)

121. Plaintiff restates and realleges paragraphs 1 through 90 above as if fully set forth herein.

122. Defendant had duties arising under the FTC Act and HIPAA to protect Plaintiff's and Class Members' Private Information.

123. Defendant breached its duties, pursuant to the FTC Act, HIPAA, and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following: (i) failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information; (ii) failing to adequately monitor the security of their networks and systems; (iii) allowing unauthorized

access to Class Members' Private Information; (iv) failing to detect in a timely manner that Class Members' Private Information had been compromised; (v) failing to remove the Private Information of its former customers, beneficiaries, employees, agents, and other individuals they were no longer required to retain pursuant to regulations; and (vi) failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

124. Defendant's violations of Section 5 of the FTC Act and HIPAA (and similar state statutes) constitute negligence *per se*.

125. Plaintiff and Class Members are consumers within the class of persons that Section 5 of the FTC Act and HIPAA were intended to protect.

126. The harm that has occurred is the type of harm the FTC Act and HIPAA were intended to guard against.

127. The FTC has pursued enforcement actions against businesses that, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

128. 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's and Class Members' Private Information.

129. In addition, under state data security and consumer protection statutes such as those outlined herein, Defendant had a duty to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and Class Members' Private Information.

130. Plaintiff and Class Members were foreseeable victims of Defendant's violations of the FTC Act and HIPAA, and state data security and consumer protection statutes. Defendant knew or should have known that its failure to implement reasonable data security measures to protect and safeguard Plaintiff's and Class Members' Private Information would cause damage to Plaintiff and the Class.

131. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) the actual misuse of their compromised Private Information; (ii) invasion of privacy; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) an increase in spam calls, texts, and/or emails; and (vii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains 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.

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

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

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

134. Plaintiff restates and realleges paragraphs 1 through 90 above as if fully set forth herein.

135. Defendant was entrusted with Plaintiff's and Class Members' Private Information as part of Defendant's regular business practices.

136. In so doing, Plaintiff 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 Plaintiff and the Class if their data had been breached and compromised or stolen, in return for the business services provided by Defendant. Implied in these exchanges was a promise by Defendant to ensure that the Private Information of Plaintiff and Class Members in its possession was secure.

137. Pursuant to these implied contracts, Defendant agreed to (1) take reasonable measures to protect the security and confidentiality of Plaintiff and Class Members' Private Information; and (2) protect Plaintiff and Class Members' Private Information in compliance with federal and state laws and regulations and industry standards.

138. Implied in these exchanges was a promise by Defendant to ensure the Private Information of Plaintiff and Class Members in its possession was only used to provide the agreed-upon reasons, and that Defendant would take adequate measures to protect Plaintiff and Class Members' Private Information.

139. A material term of this contract is a covenant by Defendant that it would take reasonable efforts to safeguard that information. Defendant breached this covenant by allowing Plaintiff and Class Members' Private Information to be accessed in the Data Breach.

140. Indeed, implicit in the agreement between Defendant and Plaintiff and Class Members was the obligation that both parties would maintain information confidentially and securely.

141. These exchanges constituted an agreement and meeting of the minds between the parties.

142. When the parties entered into an agreement, mutual assent occurred. Plaintiff and Class Members would not have disclosed their Private Information to Defendant but for the prospect of utilizing Defendant services. Conversely, Defendant presumably would not have taken Plaintiff and Class Members' Private Information if it did not intend to provide Plaintiff and Class Members with its services.

143. Defendant was therefore required to reasonably safeguard and protect the Private Information of Plaintiff and Class Members from unauthorized disclosure and use.

144. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of their implied contracts with Defendant and would have instead retained the opportunity to control their Private Information.

145. Defendant breached the implied contracts with Plaintiff and Class Members by failing to reasonably safeguard and protect Plaintiff and Class Members' Private Information.

146. Defendant's failure to implement adequate measures to protect the Private Information of Plaintiff and Class Members violated the purpose of the agreement between the parties.

147. As a proximate and direct result of Defendant's breaches of its implied contracts with Plaintiff and Class Members, Plaintiff and the Class Members suffered damages as described in detail above.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

148. Plaintiff restates and realleges paragraphs 1 through 90 above as if fully set forth herein.

149. This count is brought in the alternative to Plaintiff's breach of implied contract count.

150. Plaintiff and Class Members conferred a benefit upon Defendant when Defendant obtained their Private Information.

151. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiff. Defendant also benefited from the receipt of Plaintiff's and Class Members' Private Information.

152. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and the Class Members' Private Information because Defendant failed to adequately protect their Private

Information. Plaintiff and the proposed Class would not have provided their Private Information to Defendant had they known Defendant would not adequately protect their Private Information.

153. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds received by it because of its misconduct and the Data Breach it caused.

COUNT V
BREACH OF CONFIDENCE
(On Behalf of Plaintiff and the Class)

154. Plaintiff realleges and incorporates by reference the allegations contained in paragraphs 1 through 90 above, as if fully set forth herein.

155. At all times during Plaintiff's and Class Members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiffs' and Class Members' Private Information that Plaintiff and Class Members entrusted to Defendant.

156. As alleged herein and above, Defendant's relationship with Plaintiff and the Class were governed by terms and expectations that Plaintiff's and Class Members' Private Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third partis.

157. Defendant was entrusted with Plaintiff and Class Members' Private Information with the explicit and implicit understanding that Defendant would

protect and not permit the Private Information to be disseminated to nay unauthorized third parties.

158. Defendant was entrusted with Plaintiff and Class Members Private Information with the explicit and implicit understandings that Defendant would take precautions to protect that Private Information from unauthorized disclosure.

159. Defendant voluntarily received Plaintiff's and Class Members' Private Information in confidence with the understanding that their Private Information would not be disclosed or disseminated to the public or any unauthorized third parties.

160. As a result of Defendant's failure to prevent and avoid the Data Breach from occurring, Plaintiff's and Class Members' Private Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

161. As a direct and proximate cause of Defendant's actions and omissions, Plaintiff and the Class have suffered damages.

162. But for Defendant's disclosure of Plaintiff's and Class Members' Private Information in violation of the parties' understanding of confidence, their Private Information would not have been compromised stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and

legal cause of the theft of Plaintiff's and Class Members' Private Information as well as the resulting damages.

163. The injury and harm Plaintiff and the Class suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and Class Members' Private Information. Defendant knew or should have known its methods of accepting and securing Plaintiff's and Class Members' Private Information was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiff's and Class Members' Private Information.

164. As a direct and proximate result of Defendant's breach of its confidence with Plaintiff and the Class, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remain

in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information of individuals; and (viii) present and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

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

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of all other members of the Class, respectfully requests that the Court enter judgment in Plaintiff's favor and against Defendant as follows:

A. Certifying the Class as requested herein, designating Plaintiff as Class Representative, and appointing Plaintiff's counsel as Class Counsel;

B. Awarding Plaintiff and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, nominal damages and disgorgement;

C. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, on behalf of herself and the Class, seeks appropriate injunctive relief designed to prevent Defendant from experiencing another data breach by adopting and implementing best data security practices to safeguard Private Information and to provide or extend credit monitoring services and similar services to protect against all types of identity theft;

D. Awarding Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiff and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMAND

Plaintiff demands a trial by jury of all claims herein so triable.

Dated: June 21, 2025.

Respectfully submitted,

/s/ Casondra Turner

Casondra Turner (GA Bar No. 418426)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
800 S. Gay Street, Suite 1100
Knoxville, TN 37929
Telephone: (866) 252-0878
Fax: (771) 772-3086
cturner@milberg.com

Jeff Ostrow*
Kristen Lake Cardoso*
KOPELOWITZ OSTROW P.A.
One West Law Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Tel: (954) 525-4100
ostrow@kolawyers.com
cardoso@kolawyers.com

Counsel for Plaintiff and the Proposed Class
**pro hac vice* forthcoming