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

RENAE ALISON, on behalf of herself, and all others similarly situated, ***Plaintiff*** **v.** **BANKERS LIFE AND CASUALTY COMPANY** ***Defendant***	**Case No. _____**

CLASS ACTION COMPLAINT

Plaintiff, RENAE ALISON (hereinafter, "Plaintiff"), on behalf of herself, and all others similarly situated, for her causes of action against Defendant, BANKERS LIFE AND CASUALTY COMPANY ("Defendant" or "Bankers Life"), alleges upon personal knowledge as to her own actions, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This action arises out of the unauthorized disclosure of the confidential personal information, Personally Identifying Information[1] ("PII"), of Plaintiff and the

[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).

proposed Class Members, approximately 45,842 customers[2] of Defendant Bankers Life from November 28, 2023 to November 29, 2023. Specifically, cybercriminals executed a "SIM swapping" attack on a Bankers Life senior officer's cell phone, which, upon information and belief, exposed the names, dates of birth, social security numbers, and policy numbers of Plaintiff and the Class (the "Data Breach").[3]

2. Bankers Life is an Illinois retirement and insurance solutions and benefits provider that provides "Medicare Supplement insurance, long-term care insurance and other products that help people who are near or in retirement protect their financial security."[4]

3. As a condition of receiving retirement, insurance, or financial services[5] with Bankers Life, customers were required to entrust Defendant with their sensitive, private PII, including names, dates of birth, social security numbers, family member and beneficiary social security numbers, and other information such as other financial account information, financial history, and health history.

4. According to Defendant's January 26, 2024 letter notifying Plaintiff and other affected individuals of the Data Breach (Ex. A) ("Data Breach Notice"), mostly between November 28, 2023, and November 29, 2023 an unauthorized person

---

[2] "Customers" as used throughout this Complaint encompasses current, former, and prospective customers.

[3] *See*: Bankers Life's Data Breach Notification to Maine Attorney General, available at https://apps.web.maine.gov/online/aeviewer/ME/40/1c0e29fa-a97f-4b3e-bd73-4f20e205b77f.shtml (last accessed February 8, 2024); Bankers Life sample Notice of Data Security Incident, , **attached as Exhibit A.**

[4] https://www.bankerslife.com/about-us/ (last accessed Feb. 9, 2024).

[5] Insurance, retirement, and financial services provided by Bankers Life may be collectively referred to as "financial services" throughout this Complaint.

executed a "SIM swapping" attack on the cell phone of a Bankers Life company senior officer, enabling them to access certain company data including Plaintiff's and Class Members' PII, including their Social Security numbers.

5. In the Data Breach Notice, Bankers Life took no responsibility for the attack, and instead blamed the senior officer's wireless carrier, stating the cybercriminal was able to commit the SIM swapping because "a retailer for one of the top nationwide wireless carriers, without proper authorization or appropriate verification from the senior officer, allowed the senior officer's phone number to be swapped to what [Bankers Life] believe[s] was the threat actor's phone."[6]

6. On information and belief, Bankers Life failed to undertake adequate measures to safeguard the PII of Plaintiff and the proposed Class Members, including failing to implement industry standards for data security to protect against SIM swap attacks in the Data Breach.

7. Although Bankers Life discovered the Data Breach on or about November 29, 2023, it failed to notify and warn customers of the unauthorized disclosure of their PII therein until January 26, 2024.

8. As a direct and proximate result of Defendant's failures to protect customers' sensitive PII and warn them promptly and fully about the Data Breach, Plaintiff and the proposed Class Members have suffered widespread injury and damages necessitating Plaintiff seeking relief on a class wide basis.

9. Plaintiff brings this action on behalf of herself, and all others similarly

---

[6] Ex. A.

situated, the proposed Class of persons whose PII was compromised in the Data Breach, asserting causes of action for (I) Negligence; (II) Breach of Implied Contract; (III) Unjust Enrichment; (IV) Breach of Confidence; (V) Invasion of Privacy, Intrusion Upon Seclusion; and (VI) Bailment.

PARTIES

10. Plaintiff is a natural person, and resident and citizen of the State of Kansas with a primary residence in Hesston, Kansas, where she intends to remain, and a victim of Defendant's Data Breach.

11. Bankers Life is an Illinois corporation with its principal place of business located in Chicago, Illinois, in Cook County at 303 E. Wacker Drive., Suite 500, Chicago, Illinois. Bankers Life has tens of thousands of customers located throughout the United States.

JURISDICTION AND VENUE

12. This Court has personal jurisdiction over Defendant because, personally or through its agents, Defendant operates, conducts, engages in, or carries on a business in this State and it maintains its principal place of business and headquarters in Illinois.

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

14. The Court has supplemental jurisdiction over Plaintiff's claims arising under state law under 28 U.S.C. § 1367.

15. Venue is proper under 28 U.S.C. § 1391(b)(1) and (2) because Defendant resides in this district and a substantial part of the events and omissions giving rise to Plaintiff's claims occurred in this district.

FACTUAL BACKGROUND

A. Defendant Bankers Life

16. Bankers Life is a retirement, insurance, and financial services and benefits provider that provides "Medicare Supplement insurance, long-term care insurance and other products that help people who are near or in retirement protect their financial security."[7]

17. Bankers Life is headquartered in Illinois but does business throughout the U.S. Bankers Life has approximately "4,300 Bankers Life insurance agents, including more than 700 financial representatives, working from more than 230 U.S. sales offices offering advice and helping consumers safeguard against unexpected health costs, generate guaranteed income, protect loved ones and promote an enduring legacy."[8]

18. Indeed, Bankers Life provides customers with products such as Medicare Supplement insurance, life insurance, long-term care insurance, and

[7] https://www.bankerslife.com/about-us/ (last accessed Feb. 9, 2024).
[8] https://www.linkedin.com/company/bankers-life-and-casualty/about/ (last accessed Feb. 9, 2024).

annuities.[9]

19. As a condition of receiving retirement, insurance and/or financial services, Bankers Life requires that its applicants and customers disclose their PII, including their names, addresses, social security numbers, dates of birth, account/loan numbers for other financial institutions, financial history, beneficiary social security numbers, health history, and other private information.

20. In exchange for this information, Bankers Life promises to safeguard its customers' PII, and to only use this confidential information for authorized purposes.

21. Defendant acknowledges the importance of properly safeguarding the private data and PII of its customers, maintaining a Privacy Policy (attached hereto as **Exhibit B**) in which promises its customers to keep their PII safe:

> **Protecting your information**
>
> Your trust is important to us. We take your privacy seriously. We limit access to our buildings and our information systems to authorized persons. We have policies, procedures and training designed to keep PII safe and secure. We use privacy and security safeguards that meet state and federal regulations. If the laws differ, then we will follow the stricter applicable law.

Ex. B.

22. As Bankers Life's Privacy Policy goes on to say, the private information it collects and shares may include "name, contact information birthdate and [ ] Social Security number." *Id.* Depending on the type of coverage a customer applies for, Bankers Life states it may also need past or present health status, financial assets,

[9] https://www.bankerslife.com/about-us/ (last accessed Feb. 9, 2024).

or other identifying information. *Id*.

23. In addition, Defendant's Privacy Policy provides certain purposes for which PII may be disclosed. *See, e.g.,* Ex. B ("*Sharing PII fairly and legally*.").

24. None of these permitted purposes for Bankers Life's disclosure of PII as set forth in the Privacy Policy include the Data Breach.

25. In addition, Bankers Life, by and through its agents and employees, represented to its customers that it would adequately protect their PII and not disclose said information other than as authorized, including as set forth in its Privacy Policy.

26. Plaintiff and the proposed Class Members, customers of Bankers Life, would not have entrusted their PII to Defendant in the absence of its promises to safeguard that information, including in the manner set forth in Defendant's Privacy Policy.

27. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and the proposed Class Members' PII, Defendant assumed legal and equitable duties to Plaintiff, and the members of the Proposed Class, and knew or should have known that it was responsible for protecting hers and their PII from unauthorized disclosure.

28. At all times Plaintiff and the members of the Proposed Class, have taken reasonable steps to maintain the confidentiality of their PII; and, Plaintiff and the proposed Class Members, as customers of Bankers Life, relied on Defendant to keep their PII confidential and securely maintained.

B. Bankers Life Fails to Adequately Safeguard Current and Former Customers' PII—the Data Breach

29. Plaintiff and the proposed Class Members are customers of Defendant, Bankers Life.

30. As a condition of receiving or applying to receive Bankers Life's insurance and/or financial services, Defendant required Plaintiff and the proposed Class Members to provide Bankers Life with their sensitive PII, including names, addresses, social security numbers, dates of birth, beneficiary SSNs, financial assets, health history, and other information.

31. Bankers Life then collected and maintained said PII in its computer information technology systems and networks.

32. On information and belief, beginning on or about November 28, 2023, and November 29, 2023 an unauthorized person executed a "SIM swapping" attack on the cell phone of a Bankers Life company senior officer, enabling them to access certain company data including Plaintiff's and Class Members' PII, including their Social Security numbers—the Data Breach.

33. Specifically, according to Bankers Life:

> On November 29, 2023, we discovered that a sophisticated threat actor targeted the cellular account belonging to a company senior officer. The threat actor conducted a highly coordinated, and complex "SIM swapping" attack, which the threat actor was able to do because a retailer for one of the top nationwide wireless carriers, without proper authorization or appropriate verification from the senior officer, allowed the senior officer's phone number to be swapped to what we believe was the threat actor's phone[10]

34. Bankers Life discovered the Data Breach on or about November 29,

---

[10] Ex. A.

2023.[11]

35. Bankers Life admits that customers' PII was unauthorizedly accessed in the Data Breach, including their Social Security numbers.

36. Defendant did not have adequate security protocols to prevent, detect, and stop the cybercriminals from executing the SIM swapping attack on Bankers Life's systems and accessing the voluminous PII of Plaintiff and the proposed Class Members which was stored therein in the Data Breach.

37. Further, Bankers Life failed to implement reasonable security measures, causing it to lose control over customers' PII in the Data Breach.

38. Defendant's tortious conduct and breach of contractual obligations, as explained hereinafter, are evidenced by their failure to recognize the Data Breach until cybercriminals had already accessed the data, meaning Bankers Life had no effective means to detect and prevent attempted data breaches.

39. Despite discovering the Data Breach on November 29, 2023, Defendant waited until January 26, 2024 to notify affected customers, which it did in writing in Bankers Life's Data Breach Notice, Exhibit A.

40. Even then, Bankers Life's Data Breach Notice obfuscated the nature of the breach, blaming the Data Breach on a wireless carrier.[12]

41. According to Defendant, after discovering the Data Breach, Bankers Life took the following steps:

---

[11] *Id.*
[12] *Id.*

> We promptly disabled the senior officer's corporate access, reset passwords for personnel, and blocked the threat actor's potential access. We also scanned our environment, and implemented additional security measures designed to prevent the reoccurrence of this type of an event. In addition, we engaged federal law enforcement and hired an external forensics investigator to conduct an investigation and took steps to further restrict and monitor access to our systems and to enhance security procedures. We have also enhanced our policyholder safeguards to provide added protection to your personal information.[13]

42. Bankers Life's Data Breach Notice minimized the consequences of the Data Breach, stating that, "We have no evidence to suggest that any other company systems, accounts or personnel were impacted," but encouraged Data Breach victims to "remain vigilant in monitoring your account statements and insurance transactions for incidents of fraud and identity theft," and to "routinely review bills, notices, statements, and explanation of benefits that you receive from financial institutions, hospitals, doctors and health insurance companies."[14] Bankers Life further advised affected customers to contact IDX, and informed them of their abilities to place fraud alerts with the three (3) credit bureaus, and to place a security freeze on their credit reports.[15]

43. Bankers Life offered victims of the Data Breach identity theft protection services through IDX, including either 12 or 24 months of credit monitoring and identity theft recovery services.[16]

44. Bankers Life waited until January 26, 2024, to report the Data Breach

---

[13] *Id.*
[14] *Id.*
[15] *Id.*
[16] *Id.*

to the Maine Attorney General and other necessary consumer agencies, reporting that it involved an "external system breach (hacking)"; that the breach occurred on November 28, 2023, that it was discovered on November 29, 2023; and that 45,842 persons were affected.[17]

45. As a result of the Data Breach, its victims face a lifetime risk of identity theft, as it includes sensitive information that cannot be changed, like their dates of birth and Social Security numbers. Accordingly, Bankers Life's identity theft protection and credit monitoring through IDX is wholly insufficient to compensate Plaintiff and the Class Members for their damages caused by the Data Breach.

46. Indeed, as a result of the Data Breach which Defendant permitted to occur by virtue of its inadequate data security practices, Plaintiff and the proposed Class Members have suffered injury and damages, including identity theft and fraudulent charges, being forced to expend significant time and effort to remediate the consequences of the breach, as well as anxiety and emotional distress.

C. Plaintiff's Experience

47. Plaintiff is a customer of Bankers Life who purchased a long-term care insurance policy from Defendant.

48. As a material condition of receiving or applying to receive a policy from Bankers Life, Plaintiff was required to provide Defendant with her PII, including her full name, address, social security number, date of birth, and health history.

---

[17] *See*: Bankers Life's Data Breach Notification to Maine Attorney General, avail. at https://apps.web.maine.gov/online/aeviewer/ME/40/1c0e29fa-a97f-4b3e-bd73-4f20e205b77f.shtml (last acc. Feb. 9, 2024).

49. On or about February 6, 2024, Plaintiff received Bankers Life's Data Breach Notice, informing her that her PII, her name, Social Security Number, date of birth, and policy number, were compromised and unauthorizedly disclosed in the Data Breach.

50. As a direct result of the Data Breach, Plaintiff has spent considerable time and effort attempting to remediate the harmful effects of the Data Breach, including seeking legal advice as to what action to take in response to the Data Breach, and to prevent further fraudulent withdraws and damages, as well as time and effort to monitor her accounts to protect herself from additional identity theft.

51. Plaintiff fears for her personal financial security and uncertainty over the information compromised in the Data Breach. She is experiencing feelings of anxiety, sleep disruption, stress, and fear because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

52. Plaintiff was highly disturbed by the Data Breach's nature and the thought of cybercriminals accessing her highly sensitive PII and the harm caused by the Data Breach.

53. As a result of Bankers Life's Data Breach, Plaintiff faces a lifetime risk of additional identity theft, as it includes sensitive information that cannot be changed, like her date of birth and Social Security number.

D. This Data Breach was Foreseeable by Bankers Life.

54. Plaintiff and the proposed Class Members provided their PII to Bankers

Life with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access. By failing to do so, Defendant put all Class Members at risk of identity theft, financial fraud, and other harms.

55. Defendant tortiously failed to take the necessary precautions required to safeguard and protect the PII of Plaintiff and the Class Members from unauthorized disclosure. Defendant's actions represent a flagrant disregard of Plaintiff's and the other Class Members' rights.

56. Plaintiff and Class members were the foreseeable and probable victims of Defendant's inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing PII and the critical importance of providing adequate security for that information. Indeed, Bankers Life has already experienced a large data breach in 2018.[18]

57. Cyber-attacks against financial institutions such as Defendant are targeted and frequent. According to Contrast Security's 2023 report, "Cyber Bank Heists: Threats to the financial sector," "[o]ver the past year, attacks have included banking trojans, ransomware, account takeover, theft of customer data and cybercrime cartels deploying 'trojanized' finance apps to deliver malware in spear-phishing campaigns."[19] In fact, "40% [of financial institutions] have been victimized

[18] https://www.ibj.com/articles/71110-data-breach-at-bankers-life-under-investigation-by-state-insurance-department ; https://www.bankinfosecurity.com/bankers-life-hack-affects-more-than-566000-a-11691

[19] Contrast Security, "Cyber Bank Heists: Threats to the financial sector," pg. 5, avail. at

by a ransomware attack."[20]

58. According to the Identity Theft Resource Center's January 24, 2022 report for 2021, "the overall number of data compromises (1,862) is up more than 68 percent compared to 2020. The new record number of data compromises is 23 percent over the previous all-time high (1,506) set in 2017. The number of data events that involved sensitive information (Ex: Social Security numbers) increased slightly compared to 2020 (83 percent vs. 80 percent)."[21]

59. The increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Bankers Life. According to IBM's 2022 report, "[f]or 83% of companies, it's not if a data breach will happen, but when."[22]

60. Based on data from the Maine Attorney General, as of August 2022, "…at least 79 financial service companies have reported data breaches affecting 1,000 or more consumers, and the total number of consumers affected by these breaches could be as high as 9.4 million."[23]

---

https://www.contrastsecurity.com/hubfs/Cyber%20Bank%20Heists%20Report%202023.pdf?hsLang=en (last acc. February 9, 2024).

[20] *Id.,* pg. 15.

[21] *See* "Identity Theft Resource Center's 2021 Annual Data Breach Report Sets New Record for Number of Compromises," Jan. 24, 2022, available at https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/ (last acc. Feb. 9, 2024).

[22] IBM, "Cost of a data breach 2022: A million-dollar race to detect and respond," available at https://www.ibm.com/reports/data-breach (last acc. Feb. 9, 2024).

[23] Carter Pape, "Breach data from Maine shows scope of bank, credit union exposures," American Banker, August 24, 2022, available at https://www.americanbanker.com/news/breach-data-from-maine-shows-scope-of-bank-credit-union-exposures

61. PII is of great value to hackers and cybercriminals, and the data compromised in the Data Breach can be used for a variety of unlawful and nefarious purposes, including ransomware and fraudulent misuse, and sale on the Dark Web.

62. PII can be used to distinguish, identify, or trace an individual's identity, such as their name, Social Security number, and financial records. This can be accomplished alone, or in combination with other personal or identifying information that is connected, or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.

63. Given the nature of the Data Breach, it was foreseeable that the compromised PII could be used by hackers and cybercriminals in a variety of different injurious ways. Indeed, the cybercriminals who possess Plaintiff's and the Class Members' PII can easily obtain their tax returns or open fraudulent credit card accounts in the Class Members' names.

E. Bankers Life Failed to Comply with FTC Guidelines

64. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

65. In 2016, the FTC updated its publication, *Protecting PII: A Guide for Business*, which establishes cyber-security guidelines for businesses. The guidelines

note that businesses should protect the personal customer information that they keep; properly dispose of PII that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[24]

66. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[25]

67. 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

---

[24] *See* Federal Trade Commission, October 2016, "Protecting Private information: A Guide for Business," available at https://www.bulkorder.ftc.gov/system/files/publications/2_9-00006_716a_protectingpersinfo-508.pdf (last acc. Feb. 9, 2024).

[25] *See id*.

obligations.

68. These FTC enforcement actions include actions against entities failing to safeguard PII such as Defendant. *See, e.g., In the Matter of LabMD, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

69. Bankers Life failed to properly implement basic data security practices widely known throughout the industry. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customer PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

70. Defendant was at all times fully aware of its obligations to protect the PII of its customers. Bankers Life was also aware of the significant repercussions that would result from its failure to do so.

F. Bankers Life Fails to Comply with Industry Standards

71. A number of industry and national best practices have been published and are widely used as a go-to resource when developing an institution's cybersecurity standards.

72. The Center for Internet Security's (CIS) Critical Security Controls (CSC) recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including 18 Critical Security Controls of Inventory and

Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security, Incident Response Management, and Penetration Testing.[26]

73. In addition, the National Institute of Standards and Technology (NIST) recommends certain practices to safeguard systems, *infra,* such as:

- Control who logs on to your network and uses your computers and other devices.
- Use security software to protect data.
- Encrypt sensitive data, at rest and in transit.
- Conduct regular backups of data.
- Update security software regularly, automating those updates if possible.
- Have formal policies for safely disposing of electronic files and old devices.
- Train everyone who uses your computers, devices, and network

[26] *See* Rapid7, "CIS Top 18 Critical Security Controls Solutions," available at https://www.rapid7.com/solutions/compliance/critical-controls/ (last acc. Feb. 9, 2024).

about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.[27]

74. Further still, the Cybersecurity & Infrastructure Security Agency makes specific recommendations to organizations to guard against cybersecurity attacks, including (1) reducing the likelihood of a damaging cyber intrusion by validating that "remote access to the organization's network and privileged or administrative access requires multi-factor authentication, [e]nsur[ing] that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA[,] [c]onfirm[ing] that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes," and other steps; (2) taking steps to quickly detect a potential intrusion, including "[e]nsur[ing] that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior [and] [e]nabl[ing] logging in order to better investigate issues or events[;] [c]onfirm[ing] that the organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated," and (3) "[e]nsur[ing] that the organization is prepared to respond if an intrusion occurs," and other steps.[28]

75. Upon information and belief, Bankers Life failed to implement industry-

---

[27] Federal Trade Commission, "Understanding The NIST Cybersecurity Framework," https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework (last acc. Feb. 9, 2024).

[28] Cybersecurity & Infrastructure Security Agency, "Shields Up: Guidance for Organizations," available at https://www.cisa.gov/shields-guidance-organizations (last acc. Feb. 9, 2024).

standard cybersecurity measures, including failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, as well as failing to comply with other industry standards for protecting Plaintiff's and the proposed Class Members' PII, resulting in the Data Breach.

G. The Data Breach Caused Plaintiff and the Class Members Injury and Damages

76. Plaintiff and members of the proposed Class have suffered injury and damages from the misuse of their PII that can be directly traced to Bankers Life, that has occurred, is ongoing, and/or imminently will occur.

77. As stated prior, in the Data Breach, unauthorized cybercriminals were able to access the Plaintiff's and the proposed Class Members' PII, which is now being used for fraudulent purposes and/or has been sold for such purposes, causing widespread injury and damages.

78. The ramifications of Bankers Life's failure to keep Plaintiff's and the Class's PII secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, or other information, such as addresses, without permission, to commit fraud or other crimes.

79. Because Bankers Life failed to prevent the Data Breach, Plaintiff and

the proposed Class Members have suffered, will imminently suffer, and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. Plaintiff and the Class Members have suffered, will imminently suffer, or are at an increased risk of suffering:

a. Fraudulent misuse of PII, fraudulent charges, and fraudulent loan applications;

b. The loss of the opportunity to control how PII is used;

c. The diminution in value of their PII;

d. The compromise and continuing publication of their PII;

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

f. Lost opportunity costs and lost wages associated with the time and effort expended addressing and trying 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;

g. Delay in receipt of tax refund monies;

h. Unauthorized use of stolen PII; and

i. The continued risk to their PII, which remains in the possession of Bankers Life and is subject to further breaches so long as Bankers Life fails to undertake the appropriate measures to protect the PII in its possession.

80. Furthermore, the Data Breach has placed Plaintiff and the proposed Class Members at an increased risk of fraud and identity theft.

81. There are myriad dangers which affect victims of identity theft, including: cybercriminals opening new financial accounts, credit cards, and loans in victim's names; victim's losing health care benefits (medical identity theft); hackers taking over email and other accounts; time and effort to repair credit scores; losing home due to mortgage and deed fraud; theft of tax refunds; hackers posting embarrassing posts on victim's social media accounts; victims spending large amounts of time and money to recover their identities; experiencing psychological harm and emotional distress; victims becoming further victimized by repeat instances of identity theft and fraud; cybercriminals committing crimes in victim's names; victims' personal data circulating the Dark Web forever; victims receiving increased spam telephone calls and emails; victims' children or elderly parents having their identities stolen.[29]

82. The FTC recommends that identity theft victims take time and effort intensive or costly steps to protect their personal and financial information after a data breach, including contacting the company where the fraud occurred and asking them to close or freeze accounts and changing login information; contacting one of the credit bureaus to place a fraud alert on credit files (consider an extended fraud alert

[29] *See* Gaetano DiNardi, Aura.com, "How Bad Is Identity Theft? Is It Serious?" (December 14, 2022) available at https://www.aura.com/learn/dangers-of-identity-theft#:~:text=Fraudsters%20can%20open%20new%20accounts,to%20repair%20your%20credit%20score (last acc. Feb. 9, 2024).

that lasts for 7 years if someone steals their identity); reviewing their credit reports; seeking a credit freeze; correcting their credit reports; and other steps such as contacting law enforcement and reporting the identity theft to the FTC.[30]

83. Identity thieves use stolen PII such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

84. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information.

85. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive other services in the victim's name, and may even give the victim's PII to police during an arrest—resulting in an arrest warrant being issued in the victim's name. That can be even more problematic and difficult to remedy for someone who already has a criminal record.

86. Further, according to the Identity Theft Resource Center's 2021 Consumer Aftermath Report, identity theft victims suffer "staggering" emotional tolls: For example, nearly 30% of victims have been the victim of a previous identity crime; an all-time high number of victims say they have contemplated suicide. 35% reported not having enough money to pay for food and utilities, while 14% were

[30] *See* Federal Trade Commission, available at https://www.identitytheft.gov/Steps (last acc. Feb. 9, 2024).

evicted because they couldn't pay rent or their mortgage. 54% percent reported feelings of being violated. [31]

87. What's more, theft of PII is also gravely serious outside of the traditional risks of identity theft. In the last two decades, as more and more of our lives become interconnected through the lens of massively complex cloud computing, PII/PHI is a valuable property right.[32]

88. The value of sensitive information is axiomatic; one need only consider the value of Big Data in corporate America, or that the consequences of cyber theft include heavy prison sentences. Even the obvious risk to reward analysis of cybercrime illustrates beyond doubt that PII has considerable market value.

89. It must also be noted there may be a substantial time lag–measured in years–between when harm occurs versus when it is discovered, and also between when PII and/or financial information is stolen and when it is used.

90. PII and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

---

[31] Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (June 11, 2021), avail. at https://www.creditcards.com/statistics/credit-card-security-id-theft-fraud-statistics-1276/ citing Identity Theft Resource Center, "2021 Consumer Aftermath Report," May 26, 2021 available at https://www.idtheftcenter.org/post/the-identity-theft-resource-centers-2021-consumer-aftermath-report-reveals-impacts-on-covid-19-identity-crime-victims/ (last acc. Feb. 9, 2024).

[32] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("Private information") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("Private information, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

91. Where the most PII belonging to Plaintiff and Class Members was accessible from Bankers Life's network, there is a strong probability that entire batches of stolen information have been dumped on the black market, and are yet to be dumped on the black market, meaning Plaintiff and the Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and the Class Members must vigilantly monitor their financial accounts for many years to come.

92. While credit card information can sell for as little as $1-$2 on the black market, other more sensitive information can sell for as much as $363, according to the Infosec Institute. PII is particularly valuable because criminals can use it to target victims with frauds and scams, posing as medical personnel through the use of otherwise sacrosanct information. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

93. Social Security numbers are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud.[33]

94. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional

[33] *See* U.S. Social Security Administration, "Identity Theft and Your Social Security Number," Publication No. 05-10064, July 2021, available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last acc. Feb. 9, 2024).

credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[34] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

102. Moreover, it is not an easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[35]

103. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[36]

---

[34] *See id.*

[35] *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR, Brian Naylor, Feb. 9, 2015, http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited February 12, 2024).

[36] *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, Tim Greene, Feb. 6, 2015,

104. Accordingly, the Data Breach has caused Plaintiff and the proposed Class Members a greatly increased risk of identity theft and fraud, in addition to the other injuries and damages set forth herein, specifically the criminal fraudulent activity, fraudulent charges, theft of monies, and attendant costs, lost time and efforts in remediating the impact of the Data Breach, and other injury and damages as set forth in the preceding paragraphs.

105. Bankers Life knew or should have known of these harms which would be caused by the Data Breach they permitted to occur, and strengthened its data systems accordingly.

CLASS ALLEGATIONS

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

115. Plaintiff brings this nationwide class action individually and on behalf of all other persons similarly situated ("the Nationwide Class") pursuant to Rule 23(a) of the Federal Rules of Civil Procedure, and Fed. R. Civ. P. 23(b)(3).

116. Plaintiff proposes the following Class definition(s), subject to amendment based on information obtained through discovery:

> **All persons whose PII was compromised as a result of the Data Breach experienced by Bankers Life beginning on November 28, 2023 as announced by Bankers Life, including all persons who received the Data Breach Notice.**

---

https://www.networkworld.com/article/935334/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited February 12, 2024).

117. Excluded from the Class are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

118. Plaintiff reserves the right to amend the definition of the Class or add a class or subclass if further information and discovery indicate that the definition of the Class should be narrowed, expanded, or otherwise modified.

119. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of Class Members' 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 for each Class Member.

120. This action satisfies the requirements for a class action under Fed. R. Civ. P. 23(a)(1)-(3) and Fed. R. Civ. P. 23(b)(2), including requirements of numerosity, commonality, typicality, adequacy, predominance, and superiority.

121. **Numerosity, Fed. R. Civ. P. 23(a)(1):** The members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the PII of approximately 45,842 customers of Defendant was compromised in the Data Breach. Such information is readily ascertainable from Defendant's records.

122. **Commonality, Fed. R. Civ. P. 23(a)(2):** There are questions of law and fact common to the Class, which predominate over any questions affecting only

individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;

b. 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;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, *e.g.*, the FTC Act;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether SIM card hackers obtained Class Members' PII in the Data Breach;

f. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

g. Whether Plaintiff and the Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

h. Whether Defendant breached the covenant of good faith and fair dealing implied in its contracts with Plaintiff and Class Members;

i. Whether Defendant's acts violated Illinois law, and;

j. Whether Plaintiff and the Class Members are entitled to

damages, civil penalties, punitive damages, and/or injunctive relief.

123. **Typicality, Fed. R. Civ. P. 23(a)(3):** The claims or defenses of Plaintiff are typical of the claims or defenses of the proposed Class because Plaintiff's claims are based upon the same legal theories and same violations of law. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' PII, like that of every other Class Member, was compromised in the Data Breach.

124. **Adequacy, Fed. R. Civ. P. 23(a)(4):** Plaintiff will fairly and adequately represent and protect the interests of the members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions.

125. **Predominance, Fed. R. Civ. P. 23(b)(3):** Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data—PII—was stored on the same computer systems and unlawfully exposed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

126. **Superiority, Fed. R. Civ. P. 23(b)(3):** A class action is a superior method for the fair and efficient adjudication of this controversy because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy, and joinder of the Class Members is otherwise impracticable. Class treatment presents a superior mechanism for fairly resolving

similar issues and claims without repetitious and wasteful litigation for many reasons, including the following:

a. It would be a substantial hardship for most individual members of the Class if they were forced to prosecute individual actions. Many members of the Class are not in the position to incur the expense and hardship of retaining their own counsel to prosecute individual actions, which in any event might cause inconsistent results.

b. When the liability of Defendant has been adjudicated, the Court will be able to determine the claims of all members of the Class. This will promote global relief and judicial efficiency in that the liability of Defendant to all Class Members, in terms of money damages due and in terms of equitable relief, can be determined in this single proceeding rather than in multiple, individual proceedings where there will be a risk of inconsistent and varying results.

c. A class action will permit an orderly and expeditious administration of the Class claims, foster economies of time, effort, and expense, and ensure uniformity of decisions. If Class Members are forced to bring individual suits, the transactional costs, including those incurred by Defendant, will increase dramatically, and the courts will be clogged with a multiplicity of

lawsuits concerning the very same subject matter, with identical fact patterns and the same legal issues. A class action will promote a global resolution and will promote uniformity of relief as to the Class Members and as to Defendant.

d. This lawsuit presents no difficulties that would impede its management by the Court as a class action. The class certification issues can be easily determined because the Class includes only Bankers Life's customers, the legal and factual issues are narrow and easily defined, and the Class membership is limited. The Class does not contain so many persons that would make the Class notice procedures unworkable or overly expensive. The identity of the Class Members can be identified from Defendant's records, such that direct notice to the Class Members would be appropriate.

127. In addition, Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

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

a. Whether Defendant failed to timely and adequately notify the

public of the Data Breach;

b. Whether Bankers Life owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;

c. Whether Bankers Life's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Bankers Life's failure to institute adequate protective security measures amounted to negligence;

e. Whether Bankers Life failed to take commercially reasonable steps to safeguard consumer PII; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

129. Finally, all members of the proposed Class are readily ascertainable. Bankers Life has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

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

130. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

131. Defendant required Plaintiff and the Class Members to submit private, confidential PII to it, as a condition of applying for and receiving financial and/or insurance services.

132. Plaintiff and the Class Members are individuals who provided certain PII to Defendant including their names, addresses, social security numbers, dates of birth, health information, and other private information.

133. Defendant had full knowledge of the sensitivity of the PII to which it was entrusted, and the types of harm that Plaintiff and the Class Members could and would suffer if the PII was wrongfully disclosed to unauthorized persons. Defendant had a duty to Plaintiff and each Class Member to exercise reasonable care in holding, safeguarding, and protecting that information.

134. Plaintiff and the Class Members were the foreseeable victims of any inadequate safety and security practices. Plaintiff and the Class Members had no ability to protect their data in Defendant's possession.

135. By collecting and storing this data in its computer systems, Defendant had a duty of care to use reasonable means to secure and safeguard it, to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect if that PII was exposed to the internet and to give prompt notice to those affected in the case of a data breach.

136. Defendant owed a duty of care to Plaintiff and the Class Members to provide data security consistent with industry standards and other requirements

discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the PII.

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

138. In addition, Defendant had a 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.

139. Defendant's duty to use reasonable care in protecting confidential data and PII 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 PII.

140. Defendant breached its duties, and was negligent, by acts of omission or commission, by failing to use reasonable measures to protect the Plaintiff's and Class Members' PII. 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 Plaintiff's and Class Members' PII;

b. Failing to adequately train employees on proper cybersecurity protocols;

c. Failing to adequately monitor the security of its networks and systems;

d. Failure to periodically ensure that its network system had plans in place to maintain reasonable data security safeguards;

e. Allowing unauthorized access to Plaintiff's and Class Members' PII;

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

141. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiff's and Class Members' PII would result in injury to Plaintiff and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyber-attacks and data breaches in the industry.

142. It was therefore foreseeable that the failure to adequately safeguard Plaintiff's and Class Members' PII would result in one or more types of injuries to them.

143. As a direct and proximate result of Defendant's negligence set forth in the preceding paragraphs, Plaintiff and Class Members have suffered injury and damages as set forth herein, including monetary damages, fraudulent misuse of their PII and fraudulent charges; loss of the opportunity to control how their PII is used;

diminution in value of their PII; compromise and continuing publication of their PII; and are entitled to compensatory, consequential, and incidental damages as a result of the Data Breach.

144. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen their 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
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

145. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

146. Through their course of conduct, Defendant, Plaintiff, and Class Members entered into implied contracts for financial and/or insurance services, and that Defendant would deal with them fairly and in good faith, 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' PII entrusted to Defendant.

147. Specifically, Plaintiff and the Class Members entered into valid and enforceable implied contracts with Defendant when they first applied to receive or received Defendant's financial services.

148. The valid and enforceable implied contracts that Plaintiff and Class Members entered into with Defendant included Defendant's promise to protect

nonpublic PII given to Defendant, or that Defendant created on its own, from unauthorized disclosures. Plaintiff and Class Members provided this PII in reliance of that promise.

149. Defendant solicited and invited Plaintiff and Class Members to provide their PII as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their PII to Defendant.

150. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with industry standards and relevant laws and regulations, including the FTC Act.

151. Plaintiff and Class Members who paid money to Defendant for financial services in the form of premiums, interest and/or fees, and who provided their PII to Defendant, reasonably believed and expected that Defendant would adequately employ adequate data security to protect that PII. Defendant failed to do so.

152. Under the implied contracts, Defendant promised and was obligated to: (a) provide financial services to Plaintiff and Class Members; and (b) protect Plaintiff's and the Class Members' PII: (i) provided to obtain such services and/or (ii) created in connection therewith. In exchange, Plaintiff and Class Members agreed to pay money for these services and to turn over their PII.

153. Both the provision of financial services, and the protection of Plaintiff's and Class Members' PII, were material aspects of these implied contracts.

154. The implied contracts for the rendering of financial services—contracts that include the contractual obligations to maintain the privacy of Plaintiff's and

Class Members' PII—are also acknowledged, memorialized, and embodied in multiple documents, including Defendant's Privacy Policy as described in the preceding paragraphs.

155. Defendant's representations, including, but not limited to those found in its Privacy Policy, described in the preceding paragraphs, memorialize and embody an implied contractual obligation requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' PII.

156. Plaintiff and the Class Members as customers of Defendant value their privacy, the privacy of their dependents, and the ability to keep their PII private. To customers such as Plaintiff and the Class Members, Defendant's practices that do not adhere to industry-standard data security protocols to protect PII render the financial services fundamentally less useful and less valuable than those which adhere to industry-standard data security.

157. Plaintiff and Class Members would not have entrusted their PII to Defendant and entered into these implied contracts with Defendant without an understanding that their PII would be safeguarded and protected, or entrusted their PII to Defendant, directly or indirectly, in the absence of its implied promise to monitor its computer systems and networks to ensure that PII was not disclosed to unauthorized parties and exposed to the public as occurred in the Data Breach.

158. A meeting of the minds occurred when Plaintiff and the Class Members agreed to, and did, provide their PII to Defendant and paid for financial services for, amongst other things, (a) the provision of such services and (b) the protection of their

PII.

159. Plaintiff and the Class Members performed their obligations under the contracts when they paid for financial services in the form of fees and interest and provided their PII to Defendant.

160. Defendant materially breached its contractual obligations to protect the nonpublic PII of Plaintiff and the Class Members which Defendant required and gathered when the information was unauthorizedly disclosed in the Data Breach.

161. Defendant materially breached its contractual obligations to deal fairly and in good faith with Plaintiff and the Class Members when it failed to take adequate precautions to prevent the Data Breach and failed to promptly notify them of the Data Breach.

162. Defendant materially breached the terms of its implied contracts, including, but not limited to, the terms stated in the relevant Privacy Policy. Defendant did not maintain the privacy of Plaintiff's and the Class Members' PII. Specifically, Defendant did not comply with industry standards, the standards of conduct embodied in statutes like Section 5 of the FTC Act, or otherwise protect Plaintiff's and the Class Members' PII, as set forth above.

163. The Data Breach was a reasonably foreseeable consequence of Defendant's conduct, by acts of omission or commission, in breach of these contracts.

164. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiff and Class Members did not receive the full benefit of their bargains, and instead received financial services that were of a

diminished value compared to those described in the contracts. Plaintiff and Class Members were therefore damaged in an amount at least equal to the difference in the value of the services with data security protection they paid for and that which they received.

165. Had Defendant disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiff, the Class Members, nor any reasonable person would have purchased financial services from Defendant.

166. As a direct and proximate result of the Data Breach, Plaintiff and the Class Members have suffered injury and damages as set forth herein and have been irreparably harmed, as well as suffering and the loss of the benefit of the bargain they had struck with Defendant.

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

168. Plaintiff and the 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 III
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

169. Plaintiff re-alleges and incorporates by reference all paragraphs above

as if fully set forth herein.

170. This claim is pleaded in the alternative to the claim of breach of implied contract (Count II).

171. Plaintiff and members of the Class conferred benefits upon Defendant in the form of payments for financial services. Also, Defendant received additional benefits from receiving the PII of Plaintiff and members of the Class—such data is used to facilitate both payment and the provision of services.

172. Defendant appreciated or knew of these benefits that it received. And under principles of equity and good conscience, this court should not allow Defendant to retain the full value of these benefits—specifically, the payments and PII of Plaintiff and members of the Class.

173. After all, Defendant failed to adequately protect Plaintiff's and Class Members' PII. And if such inadequacies were known, then Plaintiff and the members of the Class would never have conferred payment to Defendant, nor disclosed their PII.

174. Defendant should be compelled to disgorge into a common fund—for the benefit of Plaintiff and members of the Class—all funds that were unlawfully or inequitably gained despite Defendant's misconduct and the resulting Data Breach.

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

175. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

176. At all times during Plaintiff's and Class Members' interactions with Defendant and/or its agents, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' PII.

177. Defendant's relationship with Plaintiff and Class Members was governed by terms and expectations that Plaintiff's and Class Members' PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized parties.

178. Plaintiff and Class Members provided their PII to Defendant and/or its agents with the explicit and implicit understandings that Defendant would protect and not permit the PII to be disseminated to any unauthorized parties.

179. Plaintiff and Class Members also provided their PII to Defendant and/or its agents with the explicit and implicit understandings that Defendant would take precautions to protect such PII from unauthorized disclosure.

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

181. Due to Defendant's failure to prevent, detect, or avoid the Data Breach from occurring by, inter alia, following industry standard information security practices to secure Plaintiff's and Class Members' PII, Plaintiff's and Class Members' PII was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

182. As a direct and proximate result of Defendant's acts and/or omissions,

Plaintiff and Class Members have suffered damages.

183. But for Defendant's disclosure of Plaintiff's and Class Members' PII in violation of the parties' understanding of confidence, their protected PII 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' protected PII, as well as the resulting damages.

184. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff' and Class Members' PII.

185. As a direct and proximate result of Defendant's breach of confidence, Plaintiff and Class Members have suffered and will suffer injury and damages as set forth herein, including monetary damages, fraudulent misuse of their PII and fraudulent charges; loss of the opportunity to control how their PII is used; diminution in value of their PII; compromise and continuing publication of their PII; and are entitled to compensatory, consequential, and incidental damages as a result of the Data Breach.

186. As a direct and proximate result of Defendant's breach of confidence, Plaintiff and Class Members have suffered and will continue to suffer injury and/or harm.

COUNT V
INVASION OF PRIVACY—INTRUSION UPON SECLUSION
(On Behalf of Plaintiff and the Class)

187. Plaintiff re-alleges and incorporates by reference all paragraphs above

as if fully set forth herein.

188. Plaintiff and the Class had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

189. Defendant owed a duty to its customers, including Plaintiff and the Class Members, to keep their PII confidential.

190. Defendant failed to protect said PII and exposed the PII of Plaintiff and the Class Members to unauthorized persons which is now publicly available, including on the dark web, and being fraudulently misused.

191. Defendant allowed unauthorized third parties access to and examination of the PII of Plaintiff and the Class Members, by way of Defendant's failure to protect the PII.

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

193. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and the Class Members disclosed their PII to Defendant as a condition of receiving financial services, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and the Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

194. The Data Breach constitutes an intentional or reckless interference by

Defendant with Plaintiff's and the Class Members' interests in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

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

196. Defendant acted with reckless disregard for Plaintiff's and Class Members' privacy when they allowed improper access to its systems containing Plaintiff's and Class Members' PII.

197. Defendant was aware of the potential of a data breach and failed to adequately safeguard their systems and implement appropriate policies to prevent the unauthorized release of Plaintiff's and Class Members' PII.

198. Because Defendant acted with this knowing state of mind, they had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and the Class Members.

199. As a proximate result of the above acts and omissions of Defendant, the PII of Plaintiff and the Class Members was disclosed to third parties without authorization, causing Plaintiff and the Class Members to suffer injury and damages as set forth herein, including monetary damages, fraudulent misuse of their PII and fraudulent charges; loss of the opportunity to control how their PII is used; diminution in value of their PII; compromise and continuing publication of their PII; and are entitled to compensatory, consequential, and incidental damages as a result

of the Data Breach.

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

COUNT VI
BAILMENT
(On Behalf of Plaintiff and the Class)

201. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

202. Plaintiff, the Class Members, and Defendant contemplated a mutual benefit bailment when the Plaintiff and putative members of the Class transmitted their PII to Defendant solely for the purpose of obtaining financial services.

203. Plaintiff and the Class entrusted their PII to Defendant for a specific purpose—to obtain financial services—with an implied contract that the trust was to be faithfully executed, and the PII was to be accounted for when the special purpose was accomplished.

204. Defendant accepted the Plaintiff's and the Class's PII for the specific purpose of obtaining financial services.

205. Defendant was duty bound under the law to exercise ordinary care and

diligence in safeguarding Plaintiff's and the Class's PII.

206. Plaintiff and the Class's PII was used for a different purpose than the Plaintiff and the Class intended, for a longer time period and/or in a different manner or place than Plaintiff and the Class intended.

207. As set forth in the preceding paragraphs, Plaintiff and the Class Members were damaged thereby.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, RENAE ALISON, on behalf of herself, and all others similarly situated, prays for judgment as follows:

A. Trial by jury pursuant to Fed. R. Civ. Proc. 38(b) on all claims so triable;

B. An Order certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing her counsel to represent the Class;

C. Awarding Plaintiff and the Class damages that include applicable compensatory, actual, exemplary, and punitive damages, as allowed by law;

D. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

E. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

F. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

G. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the transmitted PII;

H. Awarding attorneys' fees and costs, as allowed by law,

I. Awarding prejudgment and post-judgment interest, as provided by law;

J. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and,

K. Any and all such relief to which Plaintiff and the Class are entitled.

Dated: February 12, 2024 Respectfully submitted,

/s/ Lynn A. Toops

Lynn A. Toops (No. 63337-43)
Amina A. Thomas*
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, Indiana 46204
(317) 636-6481
ltoops@cohenandmalad.com
athomas@cohenandmalad.com

J. Gerard Stranch, IV *
Andrew E. Mize*
STRANCH, JENNINGS & GARVEY, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
(615) 254-8801
(615) 255-5419 (facsimile)
gstranch@stranchlaw.com
amize@stranchlaw.com

*Motion for *Pro Hac Vice* Admission forthcoming

Counsel for Plaintiff and the Proposed Class