UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NORTH CAROLINA

Robert Hamilton, *individually and on behalf of all others similarly situated*, Plaintiff, **v.** **Ally Financial Inc. and Ally Bank,** Defendants.	**Case No.** **CLASS ACTION COMPLAINT** **JURY DEMAND ENDORSED HEREIN**

CLASS ACTION COMPLAINT

Plaintiff Robert Hamilton, individually and on behalf of all similarly situated persons, alleges the following against Ally Financial Inc. ("Ally Financial") and Ally Bank ("Ally Bank" (collectively "Ally" and "Defendants") based on personal knowledge with respect to himself and on information and belief derived from, among other things, investigation by his counsel and review of public documents, as to all other matters:

SUMMARY OF THE CASE

1. This class action arises out of the cyberattack and data breach that occurred, at an undisclosed point in time, after an unauthorized third party gained access to a vendor's system (the "Data Breach"). The cyberattack and ensuing data breach were the result of Defendants' failure to implement reasonable and industry-standard data security practices. Defendants became aware of the cyberattack and data breach on August 1, 2024.

2. An investigation by Defendants revealed that the Data Breach resulted in the exposure of Plaintiff and Class Members' personal information.

3. Plaintiff brings this class action against Defendants for their failure to properly

secure and safeguard Personally Identifiable Information ("PII") and Protected Health Information ("PHI," together with PII "Private Information") provided by its clients, including, without limitation, full names, Social Security numbers, dates of birth, and addresses, drivers' license numbers, email addresses, and phone numbers.

4. Defendants failed to implement reasonable industry standard security practices, which would have prevented this attack from being successful. Considering the particularly sensitive Private Information that Defendants maintain in their regular course of business, as well as the prevalence of data security incidents within the banking and financial sector, Defendants' conduct is especially egregious.

5. By procuring, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendants assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

6. Hackers can access and then list for sale to criminals unencrypted and unredacted Prviate Information. The exposed Private Information belonging to Plaintiff and Class Members can likewise be sold on the dark web. Accordingly, Plaintiff and Class Members face a present and indefinite risk of identity theft; one that is particularly heightened given the exposure of Social Security numbers.

7. Plaintiff brings this class action lawsuit on behalf all those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access by an unknown third party and precisely what specific type of information was accessed.

8. Plaintiff and Class Members have suffered injuries deriving from Defendants'

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

9. Defendants disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, and/or negligently failing to implement and maintain adequate and reasonable measures to ensure that the Private Information of Plaintiff and Class Members was safeguarded, failing to take appropriate and reasonable steps to prevent the unauthorized disclosure of this data, and failing to adhere to applicable, required, and proper protocols, policies, and procedures regarding the encryption of data, even for internal use. Consequently, Plaintiff's and Class Members' Private Information was compromised, and Plaintiff and Class Members have a continuing interest in ensuring that their Private Information is and remains safe, and they are accordingly entitled to injunctive and other equitable relief.

THE PARTIES

Plaintiff Robert Hamilton

10. Plaintiff Robert Hamilton is, and at all times relevant has been, a resident and citizen of Odessa, Texas. Plaintiff received a Notice of Data Breach letter (the "Notice Letter") dated August 30, 2024, on or about that date. The letter notified Plaintiff that, on an unspecified

date, an unauthorized actor was able to access Plaintiff's Private Information through a vendor's system. The type of data and information at issue included Plaintiff's name, Social Security number, date of birth, address, driver's license number, email address, and phone number. The Notice Letter directed Plaintiff to the vendor's website[1] for more information.

Defendant Ally Financial Inc.

11. Defendant Ally Financial Inc. is a Delaware corporation with its headquarters located at 500 Woodward Avenue, Detroit, Michigan 48226. Ally Financial Inc. operates out of its Corporate Center located in Charlotte, North Carolina.

Defendant Ally Bank

12. Defendant Ally Bank is a subsidiary of Ally Financial. Ally Bank is a Utah corporation with its headquarters located at 200 West Civic Center Drive, Sandy, Utah 84070. Ally Bank operates out of its Corporate Center located in Charlotte, North Carolina.

JURISDICTION AND VENUE

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

14. The Court has personal jurisdiction over Defendants named in this action because Defendants principal place of business, the Ally Bank and Ally Financial Corporate Center, is located within this District, and Defendants conduct substantial business in this state and District through its numerous locations and Corporate Center.

[1] https://www.fbcs-inc.com/cyber-incident/ (last accessed September 4, 2024).

15. Venue is proper in this District under 28 U.S.C. § 1391(b) because Defendants operate out of their Corporate Center in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District including, upon information and belief, that the servers and computer systems relevant to this Data Breach are located in this District. When Defendants disclosed this Data Breach to the Maine Attorney General, it listed its Raleigh, North Carolina Corporate Center as the location of the Data Breach.

FACTUAL ALLEGATIONS

16. Plaintiff and Class Members, as current and/or former customers of Defendants, reasonably relied, whether directly or indirectly, on Defendants to keep their sensitive Private Information confidential; to maintain its system security; to use this information for business purposes only; and to make only authorized disclosures of their Private Information. It flows logically that customers expect reasonable security when entrusting companies, particularly financial institutions, with highly sensitive Private Information including Social Security numbers.

17. Defendants had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' Private Information from involuntary disclosure to third parties.

The Data Breach

18. On or about August 30, 2024, Defendants began notifying certain Class Members of the Data Breach.

19. In its Notice Letters to Plaintiff and Class Members, Defendants recognized the substantial risk of imminent harm presented by the Data Breach, informing victims that it had ceased working with the affected vendor and offering to provide victims with identity theft monitoring services. However, this is inadequate to compensate Plaintiff and Class Members, who now face a substantial risk of harm for the rest of their lives.

Securing Private Information and Preventing Breaches

20. Defendants could have prevented this Data Breach by properly encrypting or otherwise protecting its systems and those it utilizes containing Private Information.

21. By offering victims identity theft services in its Notice Letter, Defendants have acknowledged the sensitive nature of the Private Information implicated in the Data Breach. Undeniably, collecting, maintaining, and protecting Private Information is vital to Defendants' business practices as financial institutions. Through Defendants' conduct and statements, Defendants have acknowledged that the misuse or disclosure of Private Information can pose serious privacy and financial risks to victims.

22. Indeed, Defendant provides on its website that: "[w]e restrict access to the personal information obtained from our website to only those employees, agents and contractors who need it to do their jobs. We maintain administrative, technical, and physical safeguards designed to protect your personal information."[2]

23. Defendants had a duty to adopt and maintain reasonable measures to protect and secure Plaintiff's and Class Members' Private Information from involuntary disclosure to third parties.

The Cyber Attack and Data Breach were Foreseeable Risks of Which Defendants were on Notice

24. It is widely acknowledged that Private Information, especially that involving Social Security numbers, is an invaluable commodity and a frequent target of hackers.

[2] https://www.ally.com/privacy/

25. According to the *2023 Annual Data Breach Report*, the number of data compromises in 2023 (3,205) increased by 78 percentage points compared to 2022 (1,801).[3] The ITRC set a new record for the number of data compromises tracked in a year, up 72 percentage points from the previous all-time high in 2021 (1,860).[4]

26. In light of recent high profile data breaches at other industry leading companies, including T-Mobile, USA (37 million records, February-March 2023), 23andMe, Inc. (20 million records, October 2023), Wilton Reassurance Company (1.4 million records, June 2023), NCB Management Services, Inc. (1 million records, February 2023), Defendant knew or should have known that the PII that they collected and maintained would be targeted by cybercriminals.

27. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack.

28. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite their own acknowledgment of its duties to keep Private Information private and secure, Defendant failed to take appropriate steps to protect the Private Information of Plaintiffs and the proposed Class from being compromised.

At All Relevant Times Defendants Had a Duty to Plaintiff and Class Members to Properly Secure Their Private Information

29. At all relevant times, Defendants had a duty to Plaintiff and Class Members to properly secure their Private Information, encrypt and maintain such information using industry standard methods, train its employees, utilize available technology to defend its systems from

[3] https://www.idtheftcenter.org/publication/2023-data-breach-report/
[4] *Id.*

invasion, act reasonably to prevent foreseeable harm to Plaintiff and Class Members, and to promptly notify Plaintiff and Class Members when it became aware that their Private Information may have been compromised.

30. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between Defendants, on the one hand, and Plaintiff and the Class Members, on the other hand. The special relationship arose because Plaintiff and Class Members entrusted Defendants with their Private Information when they were their customers.

31. Defendants had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite its obligation to protect such information. Accordingly, Defendants breached its common law, statutory, and other duties owed to Plaintiff and Class Members.

32. Security standards commonly accepted among businesses that store Private Information using the internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;

c. Monitoring for suspicious or irregular traffic to servers;

d. Monitoring for suspicious credentials used to access servers;

e. Monitoring for suspicious or irregular activity by known users;

f. Monitoring for suspicious or unknown users;

g. Monitoring for suspicious or irregular server requests;

h. Monitoring for server requests for Private Information;

i. Monitoring for server requests from VPNs; and j. Monitoring for server requests from Tor exit nodes.

33. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R. § 248.201 (2013). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id.*

34. The ramifications of Defendants' failure to keep its Class Members' Private Information secure are long-lasting and severe. Once PII is stolen, particularly financial information, fraudulent use of that information and damage to victims is likely to continue for years.

The Value of Private Information

35. PII of data breach victims remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[5] According to the Dark Web Price Index for 2021, payment card details for an account balance up to $1,000 have an average market value of $150, credit card details with an account balance up to $5,000 have an average market value of $240, stolen online banking logins with a minimum of $100 on the account have an average market

[5] Your personal data is for sale on the dark web. Here's how much it costs, Digital Trends, Oct. 16, 2019, available at: https://www.digitaltrends.com/computing/personal-data-sold-on-thedark-web-how-much-it-costs/ (last accessed September 4, 2024).

value of $40, and stolen online banking logins with a minimum of $2,000 on the account have an average market value of $120.[6]

36. 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."[7]

37. PII can be used to distinguish, identify, or trace an individual's identity, such as their name and Social Security number. 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.[8]

38. Given the nature of Defendant's Data Breach, as well as the long delay in notification to Class Members, it is foreseeable that the compromised PII has been or will be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Plaintiffs' and Class Members' PII may easily obtain Plaintiffs' and Class Members' tax returns or open fraudulent credit card accounts in Class Members' names.

39. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, basic credit card information in a retailer data breach, because credit card victims can cancel or close credit and debit card accounts.[9]

---

[6] Dark Web Price Index 2021, Zachary Ignoffo, March 8, 2021, available at: https://www.privacyaffairs.com/dark-web-price-index-2021/ (last accessed September 4, 2024).
[7] https://www.networkworld.com/article/935334/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed September 4, 2024).
[8] See OFFICE OF MGMT. & BUDGET, OMB MEMORANDUM M-07-16 n. 1.
[9] See Jesse Damiani, Your Social Security Number Costs $4 On The Dark Web, New Report Finds, Forbes, Mar 25, 2020, available at https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4- on-the-dark-web-new-report-finds/?sh=6a44b6d513f1 (last accessed Sept. 21, 2023).

40. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

41. To date, Defendants have only offered its Class Members basic identity theft services even with the delay from their discovery of the Data Breach to the production of the notice letters. The advice offered to victims in the notice letters is inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the PII at issue here. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the Class Members.

Defendant Failed to Comply with the Gramm-Leach-Bliley Act

42. Defendant is a financial institution, as that term is defined by Section 509(3)(A) of the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. § 6809(3)(A), and thus is subject to the GLBA.

43. The GLBA defines a financial institution as "any institution the business of which is engaging in financial activities as described in Section 1843(k) of Title 12 [The Bank Holding Company Act of 1956]." 15 U.S.C. § 6809(3)(A).

44. Defendant collects nonpublic personal information, as defined by 15 U.S.C. § 6809(4)(A), 16 C.F.R. § 313.3(n) and 12 C.F.R. § 1016.3(p)(1). Accordingly, during the relevant time period Defendant were subject to the requirements of the GLBA, 15 U.S.C. §§ 6801.1, *et seq*., and is subject to numerous rules and regulations promulgated on the GLBA statutes.

45. The GLBA Privacy Rule became effective on July 1, 2001. *See* 16 C.F.R. Part 313. Since the enactment of the Dodd-Frank Act on July 21, 2010, the CFPB became responsible for implementing the Privacy Rule. In December 2011, the CFPB restated the implementing regulations in an interim final rule that established the Privacy of Consumer Financial Information,

Regulation P, 12 C.F.R. § 1016 ("Regulation P"), with the final version becoming effective on October 28, 2014.

46. Accordingly, Defendant's conduct is governed by the Privacy Rule prior to December 30, 2011 and by Regulation P after that date.

47. Both the Privacy Rule and Regulation P require financial institutions to provide customers with an initial and annual privacy notice. These privacy notices must be "clear and conspicuous." 16 C.F.R. §§ 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. "Clear and conspicuous means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice." 16 C.F.R. § 313.3(b)(1); 12 C.F.R. § 1016.3(b)(1). These privacy notices must "accurately reflect[] [the financial institution's] privacy policies and practices." 16 C.F.R. § 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. They must include specified elements, including the categories of nonpublic personal information the financial institution collects and discloses, the categories of third parties to whom the financial institution discloses the information, and the financial institution's security and confidentiality policies and practices for nonpublic personal information. 16 C.F.R. § 313.6; 12 C.F.R. § 1016.6. These privacy notices must be provided "so that each consumer can reasonably be expected to receive actual notice." 16 C.F.R. § 313.9; 12 C.F.R. § 1016.9. As alleged herein, Defendant violated the Privacy Rule and Regulation P.

48. Upon information and belief, Defendant failed to provide annual privacy notices to customers after the customer relationship ended, despite retaining these customers' PII and storing that PII on Defendant's network systems.

49. Defendant failed to adequately inform their customers that they were storing and/or sharing, or would store and/or share, the customers' PII on an insecure platform, accessible to unauthorized parties from the internet, and would do so after the customer relationship ended.

50. The Safeguards Rule, which implements Section 501(b) of the GLBA, 15 U.S.C. § 6801(b), requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (1) designating one or more employees to coordinate the information security program; (2) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks; (3) designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (4) overseeing service providers and requiring them by contract to protect the security and confidentiality of customer information; and (5) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§ 314.3 and 314.4.

51. As alleged herein, Defendant violated the Safeguard Rule.

52. Defendant failed to assess reasonably foreseeable risks to the security, confidentiality, and integrity of customer information and failed to monitor the systems of its IT partners or verify the integrity of those systems.

53. Defendant violated the GLBA and its own policies and procedures by sharing the PII of Plaintiff and Class Members with a non-affiliated third party without providing Plaintiff and Class Members (a) an opt-out notice and (b) a reasonable opportunity to opt out of such disclosure.

Defendants Failed to Comply with FTC Guidelines

54. 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.

55. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[10] 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.[11]

56. The FTC further recommends that companies not maintain Private Information 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.

57. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and

[10] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Jan. 19, 2024).
[11] *Id.*

appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

58. Defendant failed to properly implement basic data security practices.

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

60. Defendant was at all times fully aware of its obligation to protect the Private Information obtained from its customers. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendants Failed to Comply with Industry Standards

61. As discussed above, experts studying cyber security routinely identify entities operating in banking as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

62. Several best practices have been identified that a minimum should be implemented by entities like Defendants, including, but not limited to, the following: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data, and; limiting which employees can access sensitive data.

63. Other best cybersecurity practices that are standard in the legal industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as

firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

64. Defendants failed to meet the minimum standards of any of the following frameworks: 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 all established standards in reasonable cybersecurity readiness.

65. These foregoing frameworks are existing and applicable industry standards in the banking industry, and Defendants failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the data breach.

Plaintiff and Class Members Face a Substantial Risk of Increased Harm

66. Victims of all data breaches are exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim.

67. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to

manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

68. Here, the cybercriminals targeted and successfully exfiltrated Social Security numbers, which are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult, if not impossible, for an individual to change. Identity thieves use Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. Identity thieves 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. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

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

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[12]

70. It is incredibly difficult to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and

[12] Social Security Administration, *Identity Theft and Your Social Security Number* (July 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Jan. 19, 2024).

evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

71. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[13]

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

73. Criminals are also able to piece together bits and pieces of compromised Private Information for develop what are called "Fullz" packages.[14]

---

[13] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited Jan. 19, 2024).

[14] "Fullz" is fraudster-speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm/ (last visited on Jan. 19, 2024).

74. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

75. The development of "Fullz" packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

76. The existence and prevalence of "Fullz" packages means that the Private Information stolen from the data breach can easily be linked to the unregulated data of Plaintiff and Class Members. Cybercriminals can then use this information to misrepresent their identity to gain access to financial and other accounts by providing verifying information compiled from unique sources.

77. Thus, even if certain information was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

78. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to identity thieves and other criminals (like illegal and scam telemarketers).

79. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone

steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[15]

80. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[16]

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

82. According to the U.S. Government Accountability Office, 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.

See GAO Report, at p. 29.

83. Plaintiff and Class Members must vigilantly monitor their financial and other accounts for many years to come. Yet, to date, Defendants have only offered Plaintiff and Class Members temporary, non-automatic identity theft protection despite Plaintiff and Class Members being forced to face a lifetime of risk of their financial information being compromised as a result of their sensitive, Private Information being exfiltrated in the Data Breach. Defendants' offer of

---

[15] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited Jan. 19, 2024).

[16] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007), https://www.gao.gov/new.items/d07737.pdf (last visited Jan. 19, 2024).

identity theft monitoring indicates that even they understand that Plaintiff and Class Members now face a present and increased risk of harm due to their Private Information being exfiltrated from Defendants' vendor's systems by criminal threat actors.

Common Injuries & Damages

84. As a result of Defendants' ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their Private Information; and (e) the continued risk to their Private Information, which remains in the possession of Defendant, and which 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.

Loss of Time to Mitigate Risk of Identity Theft and Fraud

85. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm—yet, the resource and asset of time has been lost.

86. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class Members must monitor their financial accounts indefinitely to mitigate the risk of identity theft.

87. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as contacting their banks to ensure their financial accounts are secured.

88. Plaintiff's mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[17]

89. Plaintiff's mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[18]

Diminution Value of Private Information

90. PII and PHI are valuable property rights.[19] Their value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison

---

[17] *See* U.S. Government Accountability Office, GAO-07-737, *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/new.items/d07737.pdf.

[18] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited Aug. 28, 2024).

[19] *See, e.g.*, Randall 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

sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

91. An active and robust legitimate marketplace for Private Information exists. In 2019, the data brokering industry was worth roughly $200 billion.[20]

92. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[21]

93. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[22]

94. Conversely sensitive PII can sell for as much as $363 per record on the dark web according to the Infosec Institute.[23]

95. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, Private Information is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

---

quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[20] https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited Aug. 28, 2024).

[21] https://datacoup.com/ (last visited Aug. 28, 2024).

[22] Nielsen Computer & Mobile Panel, Frequently Asked Questions, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited Aug. 28, 2024).

[23] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Aug. 28, 2024).

96. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is static and impossible to "close" and difficult, if not impossible, to change, *e.g.*, names, Social Security numbers, dates of birth.

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

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

99. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members, and of the foreseeable consequences that would occur if Defendants' data security system or that of their vendors was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

100. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants' network and that of their vendors, amounting to, upon information and belief, thousands to tens of thousands of individuals' detailed personal information, upon information and belief, and thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

101. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members across its systems and that of its vendors.

Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary

102. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information involved, and the volume of data obtained in the Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes—*e.g.,* opening bank accounts in the victims' names to make purchases or to launder money; filing false tax returns; taking out loans or lines of credit; or filing false unemployment claims.

103. Such fraud may go undetected until debt collection calls commence months, or even years, later. 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.

104. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.[24] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

105. Consequently, Plaintiff and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

[24] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/ 25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1.

106. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is a reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendants' Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear but for Defendants' failure to safeguard their Private Information.

Plaintiff's Experience

107. Plaintiff Robet Hamilton is an adult individual who at all relevant times has been a citizen and resident of the State of Texas.

108. Plaintiff is a former customer of Defendants', whose services he used to finance two of his vehicles.

109. As Defendants' customer, Plaintiff was required to provide his Private Information, including his Social Security number, to Defendants, as part of their banking relationship.

110. Plaintiff is not aware of any data breaches other than this one that exposed his Private Information and is concerned that it and other Private Information has now been exposed to bad actors.

111. Plaintiff suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of Private Information, a form of property that Defendants obtained from Plaintiff; (b) violation of privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

112. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a

result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

113. Plaintiff greatly values his privacy, and would not have provided his Private Information, undertaken the services and paid the amounts that he did if he had known that his Private Information would be maintained using inadequate data security systems.

CLASS ACTION ALLEGATIONS

114. Plaintiff brings the following nationwide class action on behalf of himself and all others similarly situated:

> **All persons residing in the United States whose Private Information was compromised in the Data Breach announced by Ally Financial Inc. and Ally Bank in its August 31, 2024 Notice Letter (the "Class").**

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

116. Plaintiff reserves the right to modify or amend the definition of the proposed class and any future subclass before the Court determines whether certification is appropriate.

117. Numerosity, Fed R. Civ. P. 23(a)(1): Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are thousands of individuals whose Private Information may have been improperly accessed in the Data Breach, and each Class is apparently identifiable within Defendant's records.

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

a. Whether and to what extent Defendants had a duty to protect Plaintiff's and Class Members' Private Information;

b. Whether Defendants had duties not to disclose the Plaintiff's and Class Members' Private Information to unauthorized third parties;

c. Whether Defendants had duties not to use Plaintiff's and Class Members' Private Information for non-business purposes;

d. Whether Defendants failed to adequately safeguard Plaintiff's and Class Members' Private Information;

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

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

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

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

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

j. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiff's and Class Members' Private Information;

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

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

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

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

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

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

121. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiffs have suffered are typical of other Class Members. Plaintiff has also retained

counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

122. Predominance, Fed. R. Civ. P. 23(b)(3): Defendants have engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendants' 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.

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

124. The nature of this action and the laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs

of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

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

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

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

128. Further, Defendants have acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

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

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

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

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

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

e. Whether Defendants breached the contract;

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

g. Whether Defendants breached the implied contract;

h. Whether Defendants adequately and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

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

j. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiff's and Class Members' Private Information;

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

CAUSES OF ACTION

COUNT 1
Negligence
(On Behalf of Plaintiff and the Class)

130. Plaintiff restates and realleges facts set forth above as if fully alleged herein.

131. Defendants collect the Private Information of its current and former customers, including that of Plaintiff and Class Members, in the ordinary course of providing its business services As a condition of receiving services from Defendants, their current and former customers were obligated to provide Defendants with their Private Information or the Private Information of their employees, including, but not limited to Social Security numbers, drivers' license numbers, and financial account information..

132. Plaintiff and Class Members entrusted Defendants with their Private Information, directly or indirectly, with the understanding that Defendant would safeguard their information.

133. Defendants 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 the Private Information were wrongfully disclosed.

134. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' Private Information held within 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 they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

135. 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.

136. Defendant's duty to use reasonable security measures also arose under the GLBA, under which they were required to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards.

137. 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 its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

138. Defendant's duty of care to use reasonable security measures arose as a result of the relationship that existed between Defendant and Plaintiff and Class Members. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential Private Information, a necessary part of being customers of Defendants'.

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

140. Plaintiff and the Class had no ability to protect their Private Information that was in, and possibly remains in, Defendants' possession. Defendants were in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

141. Defendants had and continue to have a duty to adequately disclose that the Private Information of Plaintiff and the Class within its 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.

142. Defendants had a duty to employ proper procedures to prevent the unauthorized dissemination of the Private Information of Plaintiff and the Class.

143. Defendants have admitted that the Private Information of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

144. Moreover, Defendants had a duty to promptly and adequately notify Plaintiff and the Class of the Data Breach.

145. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of 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 Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information of Plaintiff and the Class; and (viii) 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 the Class.

COUNT II

Unjust Enrichment

(On Behalf of Plaintiff and the Class)

146. Plaintiff restates and realleges the facts set forth above as if fully alleged herein.

147. Plaintiff brings this claim in the alternative to the breach of implied contract claim below.

148. Defendants benefited from receiving Plaintiff and Class Members' Private Information by its ability to retain and use that information for its own benefit. Defendants understood this benefit.

149. Defendants also understood and appreciated that Plaintiff and Class Members' Private Information was private and confidential, and its value depended upon Defendants maintaining the privacy and confidentiality of that information.

150. Defendants were also enriched by the fees it was paid for its services which, in part, should have been used for adequate data security.

151. Plaintiff and Class Members were required to provide Defendants or Defendants' vendors with their Private Information. In exchange, Plaintiff and Class Members should have received adequate protection and data security for such Private Information held by Defendants.

152. Defendants knew Plaintiff and Class Members conferred a benefit, which Defendants accepted. Defendants profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

153. Defendants failed to provide reasonable security, safeguards, and protections to the Private Information of Plaintiff and Class Members.

154. Under the principles of equity and good conscience, Defendants should not be permitted to retain money or the value of benefits belonging to Plaintiff and Class Members, because Defendants failed to implement appropriate data management and security measures mandated by industry standard.

155. Defendants wrongfully accepted and retained these benefits to the detriment of Plaintiff and Class Members.

156. Defendants' enrichment at the expense of Plaintiff and Class Members is and was unjust.

157. As a result of Defendants' wrongful conduct, as alleged above, Plaintiff and Class Members are entitled to restitution and disgorgement of all profits, benefits, and other compensation obtained by Defendants, plus attorneys' fees, costs, and interest thereon.

COUNT III

Breach of Implied Contract

(On Behalf of Plaintiff and the Class)

158. Plaintiff restates and realleges the facts set forth above as if fully alleged herein.

159. When Plaintiff and Class Members provided their Private Information to Defendants in exchange for their financial and banking services, they entered into implied contracts with Defendants pursuant to which Defendants agreed to reasonably protect such

information. Such agreement exists anytime there is an exchange of highly sensitive Private Information, such as a combination of names, financial account information, medical information, and Social Security numbers.

160. Defendants solicited and invited Class Members to provide their Private Information Private Information as part of Defendants' regular business practices. Plaintiff and Class Members accepted Defendants' offers and provided their Private Information to Defendant.

161. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendants' data security practices complied with relevant laws and regulations and were consistent with industry standards. Plaintiff and Class Members further understood that Defendants' employees and third party vendors would not use the Private Information to commit crimes against them.

162. Class Members who paid money to Defendants or otherwise used their services reasonably believed and expected that Defendants would use part of those funds to obtain adequate data security. Defendants failed to do so.

163. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure. Plaintiff and Class Members would not have entrusted their Private Information to Defendants in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

164. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

165. Defendants breached its implied contracts with Plaintiff and Class Members by failing to safeguard and protect their Private Information.

166. As a direct and proximate result of Defendant's breaches of the implied contracts, Plaintiff and Class Members sustained damages as alleged herein.

167. Plaintiff and Class Members lost the benefit of their bargain.

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

169. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT IV

Breach of Fiduciary Duty

(On Behalf of Plaintiff and the Class)

170. Plaintiff restates and realleges the facts set forth above as if fully alleged herein.

171. In light of the special relationship between Defendants and Plaintiff and Class Members, whereby Defendants became guardians of Plaintiff and Class Members' Private Information, Defendants became a fiduciary by their undertaking and guardianship of the Private Information, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff and Class Members' Private Information; (2) to timely notify Plaintiff and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendants did and does store.

172. Defendants have a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of Defendants' relationship with its customers, in particular, to keep secure their Private Information.

173. Defendants breached its fiduciary duties to Plaintiff and Class Members by failing to diligently discovery, investigate, and give notice of the Data Breach in a reasonable and practicable period.

174. Defendants breached its fiduciary duties to Plaintiff and Class Members by failing to encrypt or otherwise protect the integrity of the systems containing Plaintiff's and Class Members' Private Information.

175. Defendants breached its fiduciary duties owed to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach.

176. Defendants breached its fiduciary duties to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' Private Information.

177. As a direct and proximate result of Defendants' breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, as alleged herein.

178. As a direct and proximate result of Defendants' breach of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT V

Declaratory and Injunctive Relief

(On Behalf of Plaintiff and the Class)

179. Plaintiff restates and realleges the facts set forth above as if fully alleged herein.

180. Plaintiff pursues this claim under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

181. Defendants owe a duty of care to Plaintiff and Class Members that requires it to adequately secure Plaintiff and Class Members' Private Information.

182. Defendants failed to fulfill its duty of care to safeguard Plaintiff and Class Members' Private Information.

183. As described above, actual harm has arisen in the wake of the Data Breach regarding Defendants' contractual obligations and duties of care to provide security measures to Plaintiff and Class Members.

184. Further, Plaintiff and Class Members are at risk of additional or further harm due to the exposure of their Private Information and Defendants' failure to address the security failings that led to such exposure.

185. There is no reason to believe that Defendant's security measures are any more adequate now than they were before the breach to meet Defendants' contractual obligations and legal duties.

186. Plaintiff therefore, seeks a declaration (1) that Defendants' existing data security measures do not comply with its contractual obligations and duties of care to provide adequate data security, and (2) that to comply with its contractual obligations and duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to, the following:

a. Ordering that Defendants engage internal security personnel to conduct testing, including audits on Defendants' systems, on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third party security auditors;

b. Ordering that Defendants engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendants audit, test, and train its security personnel and employees regarding any new or modified data security policies and procedures;

d. Ordering that Defendants purge, delete, and destroy, in a reasonably secure manner, any Private Information not necessary for its provision of services;

e. Ordering that Defendants conduct regular database scanning and security checks; and

f. Ordering that Defendants routinely and continually conduct internal training and education to inform internal security personnel and employees how to safely share and maintain highly sensitive personal information, including but not limited to, customers' and employees' Private Information.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and Class Members, requests judgment against Defendant and that the Court grants the following:

1. For an order certifying the Class, as defined herein, and appointing Plaintiff and his Counsel to represent the Class;

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

3. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect Plaintiff and Class Members' interests, including but not limited to an order:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

xvi. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xvii. for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

4. For an award of damages, including actual, statutory, nominal, and consequential damages, as allowed by law;

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

6. For prejudgment and post-judgment interest on all amounts awarded; and

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

DEMAND FOR JURY TRIAL

Plaintiff, individually and on behalf of the Class, hereby demands a trial by jury on all issues so triable.

DATED: September 10, 2024

Respectfully submitted,

/s/ Scott C. Harris

Scott C. Harris (SBN 35328)
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC
900 W. Morgan Street
Raleigh, North Carolina 27603
Phone: (919) 600-5000
sharris@milberg.com

Terence R. Coates*
Dylan J. Gould*
Isabel C. DeMarco*
MARKOVITS, STOCK & DEMARCO, LLC
119 East Court Street, Suite 530
Cincinnati, OH 45202
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com

David K. Lietz*
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Avenue NW
Washington, D.C. 20015-2052
Telephone: (866) 252-0878
Facsimile: (202) 686-2877
dlietz@milberg.com

Counsel for Plaintiff and the Proposed Class

**Pro Hac Vice forthcoming*