UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

MOSES A. GALLENS, o*n behalf of himself and those similarly situated*, **Plaintiff,** vs. **HAPPY STATE BANK** **Defendant.**	**Case No. 3:23-cv-01069** **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Plaintiff Moses A. Gallens ("Gallens" or "Plaintiff"), individually and on behalf of all those similarly situated (the "Class" or "Class Members"), brings this Class Action Complaint ("Complaint") against Defendant Happy State Bank ("HSB" or "Defendant") and makes the following allegations upon his personal knowledge as to his own actions and his counsels' investigation, and upon information and belief as to all other matters, and that facts that are a matter of public record.

INTRODUCTION

1. This action stems from Defendant's failure to secure the sensitive personal information, including Social Security numbers, of its current and former customers and other consumers for whom Defendant performed services. HSB was founded in 1908 as the First State Bank. Since then HSB has grown to over 60 locations in more than 40 communities across the Dallas/Fort Worth Metroplex, the Texas Panhandle, South Plains, Austin, and Central Texas.

2. Plaintiff brings this class action against Defendant for its failure to properly secure

and safeguard sensitive personally identifiable information (PHI) provided by and belonging to its customers, including, without limitation, names, Social Security numbers, dates of birth, and financial account information (not including security code, access code, passwords, or PIN) provided by and belonging to HSB customers in connection with their accounts with HSB ("PII" or "Sensitive Information").

3. This class action arises out of the recent targeted cyberattack against HSB that, by Defendant's own admission, allowed unauthorized third-party intruders to remotely access an employee's email account, resulting in the access and exfiltration of highly sensitive personal information belonging to thousands of current and former HSB customers (the "Data Breach").

4. Because of the Data Breach, Plaintiff, and thousands of other victims ("Class Members"), suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses, identity theft, fraud, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack, emotional distress, and the present and certainly imminent risk of future harm caused by the compromise of their sensitive personal information.

5. As part of its services, HSB requires that its customers, including Plaintiff and Class Members, to provide HSB with their PII, including, but not limited to names, Social Security numbers, dates of birth, and financial account information.

6. As a financial institution that collected, stored, and maintained the PII of Plaintiff and Class Members, Defendant owed Plaintiff and Class Members numerous statutory, regulatory, contractual, and common law duties and obligations, including those based on its affirmative representations to keep Plaintiff's and Class Members' PII confidential, safe, secure, and protected from unauthorized disclosure, access, dissemination, or theft.

7. Indeed, during the course of its business operations, Defendant expressly and

impliedly promised to safeguard Plaintiff's and Class Members' PII.

8. Furthermore, by obtaining, collecting, using, retaining, and deriving benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties to Plaintiff and Class Members and knew or should have known that it was responsible for safeguarding and protecting Plaintiff's and Class Members' PII from unauthorized disclosure access, dissemination, or theft.

9. Plaintiff and Class Members provided their PII to HSB with the reasonable expectation of privacy and mutual understanding that HSB would comply with its legal duties, obligations, and representations to keep such information confidential, safe, secure.

10. Plaintiff and Class Members reasonably expected and relied upon HSB to maintain adequate data security and retention systems.

11. Plaintiff and Class Members further reasonably expected and relied upon Defendant to only use their PII for business purposes, implement reasonable retention and data destruction policies, and to make only authorized disclosures of this information.

12. Plaintiff and Class Members would not have paid the amounts of money they paid for HSB's services, or surrendered their PII, had they known their information would be stored using inadequate data security and retention systems.

13. Defendant's data security obligations were particularly important given the substantial increase in data breaches preceding the date of the Data Breach.

14. Defendant breached its duties, promises, and obligations, and Defendant's failures to honor its obligations increased the risk that Plaintiff's and Class Members' PII would be compromised in the event of a likely cyberattack.

15. Beginning on or about March 16, 2023, HSB notified state Attorneys General

and/or many of its customers about a data breach involving the sensitive PII of thousands of individual financial services customers ("Notice Letter").[1] On April 27, 2023, HSB sent a further notice informing state Attorneys General about additional customers it had identified as being impacted by the Data Breach, bringing to total number of affected persons reported, thus far, to 17,317.[2] HSB explained through its Notice Letter that it became aware of unusual activity in an email account of an employee who was no longer employed by HSB, but whose email account was, inexplicably and in violation of adequate data security practices, still active. HSB determined that the former employee had been "subject to a phishing email scam" and in the time between that phishing scam, the employee's termination, and July 28, 2022, HSB had failed to secure that email. As such, HSB discovered that the email account was "accessed without authorization between July 28th and 29th, 2022." HSB, in the eight to nine months since this incident occurred, determined that the data for certain of its customers (at least 17,317) was stored in that email and potentially accessed and exfiltrated by these unknown unauthorized third parties.[3]

16. Presaging the harm that Defendant knew would befall victims of the Data Breach, the Notice Letter also advised Plaintiff and Class Members "to remain vigilant against incidents of identity theft and fraud . . . over the next 12 to 24 months." Moreover, recognizing that each Class Member is now subject to the present and continuing risk of identity theft and fraud, Defendant offered Plaintiff and Class Members identity theft protection for 12-24 months through Equifax.

---

[1] https://apps.web.maine.gov/online/aeviewer/ME/40/fe93a1a4-6d7c-4833-b110-bc795599b539/de6ebbba-bcd7-4f17-b764-7a7ce02ab3de/document.html March 16, 2023, letter from Mikel Williamson, HSB's President, ("March 16, 2023, Letter") (last visited May 9, 2023).

[2] https://apps.web.maine.gov/online/aeviewer/ME/40/4494fd68-72e6-48aa-a9a1-d52b44904a60.shtml (last visited May 9, 2023).

[3] March 16, 2023, Letter.

17. Notably, even though the Data Breach occurred on July 28 and 29, 2022, and HSB "became aware of unusual activity" on the impacted email account in July 2022, HSB did not notify Plaintiff and Class Members until March 16 or April 27, 2023, failing to promptly notify the impacted individuals until eight or nine months later, an unreasonable amount of time from any objective measure.

18. At this phase of litigation, the full extent of the types of sensitive personal information, the number of impacted persons, the scope of the breach, and the root cause of the Data Breach are all within the exclusive control of Defendant and its agents, counsel, and forensic security vendors.

19. Upon information and belief, Defendant is responsible for allowing this Data Breach because of multiple acts of negligence, including but not limited to: its failure to design, implement, and maintain reasonable data security systems and safeguards; and/or failure to exercise reasonable care in the hiring, supervision, training, and monitoring of its employees; and/or failure to comply with industry-standard data security practices; and/or failure to comply with federal and state laws and regulations that govern data security and privacy practices and are intended to protect the type of Sensitive Information at issue in this action; and/or failure to design, implement and execute reasonable data retention and destruction policies.

20. In this era of frequent data security attacks and data breaches, particularly in the financial industry, Defendant's failures leading to the Data Breach are particularly egregious, as this Data Breach was highly foreseeable.

21. Until notified of the breach, Plaintiff and Class Members were not aware that their PII had been compromised in the Data Breach and that they were, and continue to be, at significant risk of identity theft and various of forms of personal, social, and financial harm. This risk will

remain for the rest of their lives.

22. As HSB instructed, advised, and warned in its Notice Letters, Plaintiff and the Class Members must now closely monitor their financial accounts to guard against future identity theft and fraud. Plaintiff's and Class Members' have heeded such warnings to mitigate against the imminent risk of future identity theft and financial loss. Such mitigation efforts included and will include into the future: reviewing financial statements, changing passwords, and signing up for credit and identity theft monitoring services. The loss of time and other mitigation costs are tied directly to guarding against and mitigating against the imminent risk of identity theft.

23. Plaintiff and Class Members have suffered actual and present injuries as a direct result of the Data Breach, including: (a) theft of their PII; (b) costs associated with the detection and prevention of identity theft for their respective lifetimes; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the consequences of the Data Breach; (d) invasion of privacy; (e) the emotional distress, stress, nuisance, and annoyance of responding to, and resulting from, the Data Breach; (f) the present and/or imminent injury arising from actual and/or potential fraud and identity theft posed by their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (g) damages to and diminution in value of their personal data entrusted to Defendant on the mutual understanding that Defendant would safeguard their PII against theft and not allow access to and misuse of their personal data by others; and (h) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further injurious breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII. Plaintiff and Class Members, at the very least, are entitled to damages and injunctive relief tailored to address the vulnerabilities exploited in the breach, and designed to

protect Plaintiff's and Class Members' PII, as well as an order from the Court directing the destruction and deletion of all PII for which Defendant cannot demonstrate a reasonable and legitimate purpose for continuing to maintain possession of such PII.

24. Defendant understands the need to protect the privacy of their customers and use security measures to protect their customers' information from unauthorized disclosure.[4] As a sophisticated financial entity who maintains private and sensitive consumer information, Defendant further understood the importance of safeguarding PII. Yet Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff and Class members' PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiff and Class Members was compromised through access to and exfiltration by an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they are entitled to injunctive and other equitable relief.

25. Plaintiff seeks to remedy these harms, and to prevent the future occurrence of an additional data breach, on behalf of himself and all similarly situated persons whose PII was compromised as a result of the Data Breach. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement for loss of time, reimbursement of opportunity costs, out-of-pocket costs, price premium damages, and injunctive relief including improvements to Defendant's data security systems and protocols, future annual audits, and adequate credit monitoring services funded by the Defendant.

[4] See https://www.my100bank.com/privacy-policy/ (last visited May 9, 2023).

PARTIES

26. Plaintiff Moses A. Gallens is a citizen of the state of Texas. Plaintiff Gallens is a consumer and former customer of HSB. Plaintiff Gallens provided his personal information and PII to HSB. HSB notified Plaintiff Gallens of the Data Breach and the unauthorized access of his PII by sending him a Notice of Data Breach letter, dated April 27, 2023.

27. Defendant Happy State Bank is a Texas corporation and maintains a location, and does a substantial portion of its business, at 16633 Dallas Parkway, STE 350, Addison, Texas, 75001.

28. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

29. All of Plaintiff's claims stated herein are asserted against HSB and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

JURISDICTION AND VENUE

30. 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, and there are more than 100 members in the proposed class. The minimal diversity requirement is met as at least one Class Member and Defendant are citizens of different states.

31. This Court has personal jurisdiction over HSB because HSB is incorporated and has its principal place of business in the Northern District of Texas; conducts substantial business in this District through its headquarters, offices, and affiliates; engaged in the conduct at issue here

in this District; and otherwise has substantial contacts with this District, and purposely availed themselves to the Courts in this District.

32. Venue is proper in the Northern District of Texas under 28 U.S.C. §§ 1391(a)(2), 1391(b)(1), 1391(b)(2), and 1391(c)(2) as a substantial part of the events giving rise to the claims emanated from activities within this district, and Defendant HSB's principal place of business is in this district. Further, on information and belief, decisions regarding the management of the information security of Plaintiff's and Class Members' PII were made by Defendant within this district.

BACKGROUND

33. HSB is a full-service bank which operates over 60 locations in over 40 communities across the Dallas/Fort Worth Metroplex, the Texas Panhandle, South Plains, Austin, and Central Texas and has assets in the billions.[5]

34. HSB has acknowledged the sensitive and confidential nature of the PII it collects from its customers.

35. Collecting, maintaining, retaining, and protecting PII is vital to many of HSB's business purposes.[6] Furthermore, HSB has acknowledged through conduct and statements that the PII should only be used for a legitimate business purpose, that the misuse or inadvertent access, disclosure or unauthorized dissemination of PII can pose major privacy and financial risks to impacted individuals, and that they may not disclose and must take reasonable steps to protect PII from improper release or disclosure.[7]

[5] https://www.happybank.com/about (last visited May 9, 2023)
[6] See *Id.*
[7] See https://www.my100bank.com/privacy-policy/ (last visited May 9, 2023).

36. As a sophisticated financing institution, HSB knew, or should have known, that Plaintiff's and Class Members' PII, that HSB collected and maintained, was a target of data thieves and that they had a duty to protect Plaintiff's and Class Members' PII from unauthorized access.

37. Plaintiff and Class Members relied on HSB's express and implied promises and on this sophisticated Defendant to keep their sensitive PII confidential and securely maintained, to use this information for business purposes only, to implement reasonable retention policies, to limit access to authorized individuals, and to make only authorized disclosures of this information.

38. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties to these individuals to safeguard and protect the PII from unauthorized access.

THE DATA BREACH AND DEFENDANT'S RESPONSE

39. Before July 28, 2022, a now former employee of HSB was the subject of a phishing email scam which compromised that employee's email.[8] That email address remained active even after the employee stopped working for HSB and between July 28 and 29, 2022 unauthorized third parties accessed that email account. The PII of thousands of HSB's customers was stored in that email account and potentially accessed and exfiltrated by those unauthorized third parties.[9]

40. Beginning on or about March 16, 2023 and continuing on April 27, 2023, HSB reported the Data Breach to the various Attorneys General offices, including Texas, Indiana, Maine, Massachusetts, Montana, among others. On those same dates, HSB also began notifying Plaintiff and Class Members of the Data Breach.

41. The PII that was accessed without authorization included names along with data

[8] March 16, 2023 Letter
[9] *Id.*

elements including Social Security numbers, dates of birth, and financial account information.

42. Upon information and belief, the PII was not encrypted or was not adequately encrypted prior to the data breach.

43. Even though HSB became aware of "unusual activity" in July 2022, HSB took between eight and nine months to notify state Attorneys General and Class Members about the Data Breach. Even then, HSB did not fully disclose the scope of the Data Breach but opted to issue a vague letter leaving Plaintiff and Class Members without a full understanding of how the breach occurred or what happened to their PII once it was accessed.

Defendant Acquires, Collects, and Stores Plaintiff's and Class Members' PII

44. Defendant acquired, collected, and stored the PII of Plaintiff and Class Members.

45. In the course and scope of its banking business, HSB collects massive amounts of highly sensitive PII, including but not limited to, names, Social Security numbers, dates of birth, and financial account information.

46. By obtaining, collecting, and storing Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

47. Plaintiff and Class Members entrusted their PII to HSB on the premise and with the understanding that HSB would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties, and/or only retain PII for necessary business purposes and for a reasonable amount of time.

Securing PII

48. Defendant could have prevented this Data Breach by properly securing and encrypting Plaintiff's and Class Members' PII. Additionally, Defendant could have destroyed data, including old data that Defendant had no legal right or responsibility to retain.

49. Defendant knew that the PII it maintained was a target of data thieves and that it had a duty to protect Plaintiff's and Class Members' PII from unauthorized access.

50. In its notice letter, HSB issued an express warning and advised Plaintiff and Class Members of the seriousness of the attack, and that they should "remain vigilant" and immediately sign up for identity theft protection. The Notice Letter further instructed customers to:

- Remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors over the next 12 to 24 months;
- Enroll in Equifax Credit Watch Gold credit monitoring service.

51. These warnings and instructions are an acknowledgment by HSB that it is not only plausible that the criminals acquired the PII for criminal purposes, thereby placing the impacted customers at an imminent threat of identity theft and financial fraud – but that the theft and dissemination and misuse of the PII is the highly probable result of this type of cyberattack and a present threat to all Class Members.

52. Without the likelihood of dissemination and misuse, and materialization of identity theft, the warnings and instructions to mitigate the risk would be unnecessary and would cause more harm than good, and Defendant would not have advised such actions that would cost Plaintiff and Class Members time and money.

53. As an additional line of protection, HSB paid for a program that offered identity theft protection to Class Members. Absent an actual, materialized, and imminent threat to the Plaintiff and Class Members, such a program would also have been unnecessary and a waste of

Defendant's time and money. HSB would not have spent resources offering such a program without the likelihood that the Class Member PII was exfiltrated and disseminated in the attack, and that a materialized and imminent risk of identity theft was present for all Class Members.

54. What is evident and indisputable is that the Data Breach resulted in the unauthorized access of HSB's systems and files, and that those compromised files contained the PII of Plaintiff and thousands of Class Members including their names, Social Security numbers, dates of birth, and financial account information.

55. Upon information and belief, the cyberattack targeted HSB due to HSB's status as a multi-billion-dollar bank that collects valuable personal and financial data on its many customers, including Plaintiff and Class Members.

56. Upon information and belief, the cyberattack was expressly designed to gain access to and steal the private and confidential data, including (among other things) the PII of Plaintiff and the Class Members.

57. As a result of the Data Breach, the risk of identity theft has materialized, and Plaintiff and Class Members are at an imminent risk of identity theft.

THE DATA BREACH WAS FORESEEABLE

58. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the financial industry and other industries holding significant amounts of PII preceding the date of the breach.

59. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion

records, May 2020), HSB knew or should have known that its systems would be targeted by cybercriminals.

60. Indeed, cyberattacks against the financial industry have been common for over a decade with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[10]

61. As a sophisticated financial institution that collects, uses, and stores particularly sensitive PII, Defendant was and is at all times fully aware of the increasing risks of cyber-attacks targeting the PII it controls, and its obligations to protect the PII of Plaintiff and Class Members.

62. Plaintiff and Class Members now currently face a lifetime of constant surveillance and monitoring of their financial and personal records and loss of rights. Plaintiff and Class Members are incurring, and will continue to incur, such damages in addition to any fraudulent use of their PII.

63. The injuries to Plaintiff and Class Members are directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members, and such as encrypting the data so unauthorized third parties could not see the PII.

DEFENDANT FAILED TO PROTECT PLAINTIFF'S AND CLASS MEMBERS' PII

64. Despite the prevalence of public announcements of data breach and data security compromises, and despite Defendant's own acknowledgment of its duties to keep PII private and

10 Gordon M. Snow, Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit, FBI (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector.

secure, Defendant failed to take appropriate steps to protect the PII of Plaintiff and the Class from being compromised.

65. Defendant did not use reasonable security procedures and practices appropriate to the nature of the Sensitive Information it was maintaining for Plaintiff and Class Members, causing the exposure of Plaintiff and Class Members' PII.

A. Defendant Failed to Properly Comply with Federal Trade Commission Data Security Standards

66. 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.

67. The FTC has brought well publicized enforcement actions against businesses for failing to adequately and reasonably protect consumer 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. This includes the FTC's enforcement action against Equifax following a massive data breach involving the personal and financial information of 147 million Americans.

68. In 2016, the FTC updated its publication, "Protecting Personal Information: A Guide for Business," which established cyber-security guidelines for businesses that Defendant did not adequately employ. The FTC advised that businesses like Defendant should protect the PII that they keep by following some minimum standards related to data security, including, among others:

(a) Encrypting information stored on computer networks;

(b) Identifying network vulnerabilities;

(c) Implementing policies to update and correct any security problems;

(d) Utilizing an intrusion detection systems;

(e) Monitor all incoming traffic for suspicious activity indicating someone is attempting to hack the system;

(f) Watching for large amounts of data being transmitted from the system;

(g) Developing a response plan ready in the event of a breach;

(h) Limiting employee and vendor access to sensitive data;

(i) Requiting complex passwords to be used on networks;

(j) Utilizing industry-tested methods for security;

(k) Verifying that third-party service providers have implemented reasonable security measures;

(l) Educating and training employees on data security practices;

(m) Implementing multi-layer security including firewalls, anti-virus, and anti-malware software;

(n) Implementing multi-factor authentication.

69. In particular, the FTC further advised that companies not maintain PII longer than is needed for authorization of a transaction: "If you don't have a legitimate business need for sensitive personally identifying information, don't keep it."[11]

70. Upon information and belief, HSB failed to implement or adequately implement at least one of these fundamental data security practices.

71. Defendant could have prevented this Data Breach by properly following FTC guidelines by adequately encrypting or otherwise protecting its equipment and computer files

[11] FTC, Protecting Personal Information: A Guide for Business (Oct. 2016), https://www/ftc.gov/business-guidance/resources/protecting-personal-information-guide-business.

containing PII.

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

B. Defendant Failed to Comply with Industry Standards

73. The financial industry also routinely incorporates these cybersecurity practices that are standard in the financial industry, and that Defendant did not adequately employ. These minimum standards include but are not limited to:

(o) Maintaining a secure firewall configuration;

(p) Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;

(q) Monitoring for suspicious or irregular traffic to servers;

(r) Monitoring for suspicious credentials used to access servers;

(s) Monitoring for suspicious or irregular activity by known users;

(t) Monitoring for suspicious or unknown users;

(u) Monitoring for suspicious or irregular server requests;

(v) Monitoring for server requests for PII;

(w) Monitoring for server requests from VPNs; and

(x) Monitoring for server requests from Tor exit nodes.

74. Upon information and belief, Defendant failed to comply with at least one of these minimal industry standards, thereby opening the door to and causing the Data Breach.

75. Defendant could have prevented this Data Breach by properly following industry data security standards by adequately encrypting or otherwise protecting their equipment and computer files containing PII.

76. Defendant could also have prevented the scale of the Data Breach simply by

designing and implementing data retention practices to delete PII that is no longer needed for an ongoing business purpose.

77. Defendant had the resources necessary, and reasonable data security alternatives were known and available to HSB that would have prevented the Data Breach, but Defendant neglected to adequately evaluate its systems, and invest in adequate security measures, despite its obligation to protect its systems and Plaintiff's and Class Members' PII.

C. HSB Failed to Comply with Gramm-Leach-Bliley Act

78. HSB 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.

79. 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).

80. HSB 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 period Defendant was 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. The GLBA Privacy Rule became effective on July 1, 2001. *See* 16 C.F.R. § 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.

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

82. 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(a) and 313.5(a)(1); 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(a)(1) and 313.5(a)(1); 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(a); 12 C.F.R. § 1016.9. As alleged herein, HSB violated the Privacy Rule and Regulation P.

83. Upon information and belief, HSB failed to provide annual privacy notices to customers after the customer relationship ended, despite retaining these customers' PII and storing and/or sharing that PII on its network.

84. HSB failed to adequately inform its customers that it was storing and/or sharing, or would store and/or share, the customers' PII on its inadequately secured network and would do so after the customer relationship ended.

85. 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: (a) designating

one or more employees to coordinate the information security program; (b) 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; (c) 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; (d) overseeing service providers and requiring them by contract to protect the security and confidentiality of customer information; and (e) 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. As alleged herein, Defendant violated the Safeguard Rule.

86. HSB failed to assess reasonably foreseeable risks to its networks, and the security, confidentiality, and integrity of PII in its custody or control.

87. HSB failed to design and implement information safeguards to control the risks identified through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

88. HSB failed to evaluate and adjust its information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances.

THE VALUE OF PII

89. There is both a healthy black market and a legitimate market for the type of PII that was compromised in this action. PII is such a valuable commodity to criminal networks that once the information has been compromised, criminals often trade the information on the "cyber black market" for years.

90. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the Dark Web. Numerous sources cite Dark Web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[12]

91. 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 value of $40, and stolen online banking logins with a minimum of $2,000 on the account have an average market value of $120.[13] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[14]

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

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, when 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

[12] Anita George, Your personal data is for sale on the dark web. Here's how much it costs, Digital Trends (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.

[13] Zachary Ignoffo, Dark Web Price Index 2021, Privacy Affairs (Mar. 8, 2021), https://www.privacyaffairs.com/dark-web-price-index-2021/.

[14] In the Dark, VPNOverview (2019), https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/.

lot of problems.[15]

93. The Social Security Administration has further warned that identity thieves can use an individual's Social Security number to apply for additional 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, apply for a job using a false identity, open bank accounts, and apply for other government documents such as driver's license and birth certificates.

94. 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 not typically discovered until an individual's authentic tax return is rejected.

95. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

96. 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."[16]

97. This data, as one would expect, demands a much higher price on the black market.

---

[15] Social Security Administration, Identity Theft and Your Social Security Number (June 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf.

[16] Brian 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-millions-worrying-about-identity-theft.

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 in price on the black market."[17]

PLAINTIFF AND CLASS MEMBERS SUFFERED FORESEEABLE CONCRETE HARMS

98. As a result of Defendant's ineffective and inadequate data security and retention measures, the Data Breach, and the foreseeable consequences of the PII ending up in the possession of criminals, the risk of identity theft is materialized and imminent.

99. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII 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 PII for identity theft crimes, such as opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; or file false unemployment claims.

100. 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.[18] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

101. There may be a time lag between when harm occurs versus when it is discovered,

---

[17] Tim Greene, Anthem hack: Personal data stolen sells for 10x price of stolen credit card numbers, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[18] *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.

and also between when PII is stolen and when it is used. The fraudulent activity resulting from the Data Breach may not become evident for years.

102. Indeed, "[t]he risk level is growing for anyone whose information is stolen in a data breach."[19] Javelin Strategy & Research, a leading provider of quantitative and qualitative research, notes that "[t]he theft of SSNs places consumers at a substantial risk of fraud."[20] Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that have not yet been exploited by cybercriminals bears a high risk that the cybercriminals who now possess Class Members' PII will do so at a later date or re-sell it.

103. To date, Defendant has done little to adequately protect Plaintiff and Class Members, or to compensate them for their injuries sustained in this data breach. The complimentary Credit monitoring service offered by HSB is wholly inadequate as the service is only offered for 12-24 months and it places the burden squarely on Plaintiff and Class Members by requiring them to expend time signing up for that service, as opposed to automatically enrolling all victims of this cybercrime.

104. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class Members must, in HSB's words, "remain vigilant" and monitor their financial accounts for many years to mitigate the risk of identity theft.

105. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as placing "freezes" and "alerts" with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing

---

[19] Susan Ladika, Study: Data Breaches Pose a Greater Risk, Fox Business (Mar. 6, 2016), https://www.foxbusiness.com/features/study-data-breaches-pose-a-greater-risk.

[20] The Consumer Data Insecurity Report: Examining The Data Breach- Identity Fraud Paradigm In Four Major Metropolitan Areas, Al Pascal, 2014), https://www.it.northwestern.edu/bin/docs/TheConsumerDataInsecurityReport_byNCL.pdf.

passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports, which may take years to discover and detect.

106. 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."[21]

107. 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.[22]

108. Furthermore, Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to pay HSB or its clients for services, Plaintiff and other reasonable consumers understood and expected that they were paying for services and data security, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received services that were of a lesser value than what they reasonably expected.

109. As a result of Defendant's ineffective and inadequate data security and retention measures, the Data Breach, and the ongoing and imminent risk of identity theft, Plaintiff and Class

---

[21] See United States 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.

[22] See Federal Trade Commission, Identity Theft.gov, https://www.identitytheft.gov/Steps (last visited July 7, 2022).

Members have suffered numerous actual and concrete injuries, including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) the loss of benefit of the bargain (price premium damages); (h) deprivation of value of their PII; and (i) the continued risk to their PII, 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' Sensitive Information.

PLAINTIFF'S EXPERIENCES

Plaintiff Moses A. Gallens's Experience

110. Plaintiff Moses A. Gallens is a resident and citizen of Texas.

111. Prior to the Data Breach, Plaintiff Gallens used HSB's services, maintaining a bank account with HSB until he closed it in January 2023.

112. By virtue of Plaintiff Gallens's maintaining a bank account with HSB, HSB acquired significant personal, income, and financial information of Plaintiff Gallens.

113. Plaintiff Gallens greatly values his privacy and Sensitive Information, especially when receiving financial services. Plaintiff Gallens has taken reasonable steps to maintain the confidentiality of his PII, and he has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

114. Plaintiff Gallens stores any and all documents containing PII in a secure location and destroys any documents he receives in the mail that contain any PII or that may contain any

information that could otherwise be used to compromise his identity and financial accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts. In addition, he does not release his birthdate or other PII on social media sites, *etc.*, as a precautionary measure from identity fraud.

115. Plaintiff Gallens received a Notice Letter from HSB, dated April 27, 2023, informing him that his full name, Social Security number, and financial account information were acquired by unauthorized third parties.

116. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Gallens faces, Defendant HSB encouraged Plaintiff Gallens to sign-up for a complimentary one-year membership to credit monitoring services offered by Defendant HSB. This offer is inadequate because data breach victims whose Social Security number is involved commonly face a lifetime of ongoing identity theft.

117. As a result of the Data Breach, Plaintiff Gallens has suffered a loss of time and has spent, and continues to spend, a considerable amount of time on issues related to mitigating the impact of the Data Breach.

118. Plaintiff Gallens expected and reasonably relied upon Defendant as part of its services to provide adequate data security to protect the sensitive PII that he entrusted to HSB. If Plaintiff Gallens had known that HSB would not adequately protect his PII, he would not have allowed HSB access to this PII and would not have engaged in business with HSB.

119. As a result of the Data Breach and the directives that he received in the Notice Letter, Plaintiff Gallens has already spent precious hours dealing with the consequences of the Data Breach (*e.g.*, self-monitoring his bank and credit accounts), as well as his time spent verifying the legitimacy of the Notice of Data Breach, communicating with his bank, and researching

multiple forms of security protection services. This time has been lost forever and cannot be recaptured.

120. Moreover, Plaintiff Gallens spent this time at Defendant's direction. The notice letter Plaintiff Gallens received from HSB directed him to spend time mitigating his losses and to "remain vigilant" by closely monitoring his accounts over the next 12 to 24 months."

121. Plaintiff Gallens has suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (a) damage to and deprivation in the value of his PII, a form of property that Defendant obtained from the Plaintiff; (b) violation of his privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

122. Plaintiff Gallens also lost the benefit of the bargain and price premium damages for the services he paid for. Had he known that HSB would have inadequate data security practices, he would not have entered into a business transaction, paid for the services, or provided his PII.

123. Plaintiff Gallens has suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

124. Plaintiff Gallens has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his stolen PII, especially his Social Security number, combined with his name and financial account information, being placed in the hands of unauthorized third-party intruders and possibly criminals.

125. As a result of the Data Breach, Plaintiff Gallens has experienced a substantial increase in suspicious emails and telephone calls.

126. Plaintiff Gallens has recently received an email from American Express indicating that someone attempted to log into his credit card account and access it and has been locked out

of his credit card account while American Express investigates. Upon information and belief, this attempt to access his accounts was committed as a result of the Data Breach

127. Plaintiff Gallens has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

128. Plaintiff, pursuant to Fed. R. Civ. P. 23(a), 23(b)(1), 23(b)(2), 23(b)(3), 23(c)(4) and/or 23(c)(5), brings this Action on behalf of himself and on behalf of all other persons similarly situated. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> All individuals residing in the United States whose PII was accessed or exfiltrated during the Data Breach announced by HSB in 2023 (the "Nationwide Class").

129. Excluded from the Class are Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and agents; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and 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. Also excluded from the Class are any judicial officers presiding over this matter, members of their immediate family, and members of their judicial staff.

130. Plaintiff reserves the right to modify or amend the definitions of the proposed Class before the Court determines whether certification is appropriate.

131. 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 Class consists of, at least 17,317

individuals whose sensitive data was compromised in the Data Breach. The number and identities of Class Members can be ascertained through Defendant's records.

132. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): 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 breached a duty to Class Members to safeguard their PII;

(b) Whether Defendant expressly or impliedly promised to safeguard the PII of Plaintiff and Class Members;

(c) Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;

(d) 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;

(e) Whether Defendant's data security systems prior to, during, and after the Data Breach complied with the applicable FTC data security laws and regulations;

(f) Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards, as applicable;

(g) Whether unauthorized third parties accessed or obtained Class Members PII in the Data Breach;

(h) Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

(i) Whether the Plaintiff and Class Members suffered legally cognizable injuries as a result of Defendant's misconduct;

(j) Whether Defendant's conduct was negligent;

(k) Whether Defendant breached expressed or implied contractual obligations;

(l) Whether Defendant violated state consumer protections statutes;

(m) Whether Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class Members;

(n) Whether Defendant failed to provide notice of the Data Breach in a timely manner;

(o) Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

(p) Whether Plaintiff and Class Members are entitled to damages, restitution, and/or civil penalties; and

(q) Whether Defendant violated state statutes as alleged herein;

133. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of every other Class Member, was compromised in the Data Breach due to Defendant's misfeasance, and their claims arise under the same legal doctrines.

134. Adequacy of Representation, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff's counsel are competent and experienced in litigating complex class actions and data breach cases, and they intend to prosecute this actions vigorously.

135. 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 of Plaintiff's and Class Members' data was stored on the same computer system and unlawfully accessed 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.

136. Superiority, Fed. R. Civ. P. 23(b)(3): A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent

a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

137. Manageability, Fed. R. Civ. P. 23(b)(3): The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

138. Conduct Generally Applicable to the Class, Fed. R. Civ. P. 23(b)(2): Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate. Unless a class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

139. 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. The particular issues include, but are not limited to:

(a) Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

(b) Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

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

(d) Whether an implied contracts existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of those implied contracts;

(e) Whether Defendant breached the implied contracts;

(f) Whether Defendant adequately, and accurately informed Plaintiff and Class Members that their PII had been compromised;

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

(h) Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members; and

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

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

140. Plaintiff re-alleges and incorporates by reference paragraphs 1-139 as if fully set forth herein.

141. Plaintiff brings this Count on behalf of himself and Class.

142. As a condition of receiving their financial services from Defendant or its partners or affiliates, Plaintiff and the Class were obligated to provide and entrust it with certain PII, including their name, birthdate, Social Security number, and financial account information provided in connection with financial services.

143. Plaintiff and the Class entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

144. By undertaking the duty to maintain and secure this data, sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their systems and networks—and Plaintiff and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from cyber theft.

145. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed or obtained by unauthorized parties.

146. Defendant knew or reasonably should have known that its failure to exercise due care in the collecting, storing, and using of consumers' PII involved an unreasonable risk of harm to Plaintiff and the Class, including harm that foreseeably could occur through the criminal acts of a third party.

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

148. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former customers' PII that it was no longer required to retain pursuant to regulations.

149. Defendant had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's and the Class's PII, and to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and the Class.

150. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII, a mandatory step in receiving services from Defendant. While this special relationship exists independent from any contract, it is recognized by Defendant's Privacy Policies, as well as applicable laws and regulations. Specifically, Defendant actively solicited and gathered PII as part of their businesses and were solely responsible for and in the position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Plaintiff, Class and Subclass members from a resulting data breach.

151. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff and the Class, to maintain adequate data security.

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

153. Defendant also had a common law duty to prevent foreseeable harm to others. Plaintiff and the Class 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 the PII of Plaintiff and the Class, the critical importance of adequately safeguarding that PII, and the necessity of encrypting PII stored on Defendant's systems. It was foreseeable that Plaintiff and Class Members would be harmed by the failure to protect their personal information because hackers are known to routinely attempt to steal such information and use it for nefarious purposes.

154. Defendant's conduct created a foreseeable risk of harm to Plaintiff and the Class. Defendant's wrongful conduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included their decision not to comply with industry standards for the safekeeping of Plaintiff's and the Class's PII, including basic encryption techniques available to Defendant.

155. Plaintiff and the Class had and have no ability to protect their PII that was in, and remains in, Defendant's possession.

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

157. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiff and the Class within Defendant's possession was 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 PII by third parties.

158. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully accessed by unauthorized third persons as a result of the Data Breach.

159. Defendant, through its actions and inaction, unlawfully breached its duties to Plaintiff and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiff and the Class when the PII was within Defendant's possession or control.

160. Defendant improperly and inadequately safeguarded the PII of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

161. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect its current and former customers' PII in the face of increased risk of theft.

162. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and the Class by failing to have appropriate procedures in place to detect and prevent dissemination of its current and former customers' PII.

163. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove consumers' PII it was no longer required to retain pursuant to regulations.

164. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and the Class the existence and scope of the Data Breach.

165. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the PII of Plaintiff and the Class would not have been compromised.

166. There is a close causal connection between (a) Defendant's failure to implement security measures to protect the PII of Plaintiff and the Class and (b) the harm or risk of imminent harm suffered by Plaintiff and the Class. Plaintiff's and the Class's PII was accessed and exfiltrated as the direct and proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

167. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of businesses, such as Defendant, of failing to implement reasonable measures to protect PII. The FTC Act and related authorities form part of the basis of Defendant's duty in this regard.

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

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

170. Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect.

171. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

172. Defendant failed to provide Plaintiff and Class Members privacy notices that "accurately reflect[ed] [the financial institution's] privacy policies and practices." in violation of

16 C.F.R. § 313.4(a)(1) and 313.5(a)(1); 12 C.F.R. §§ 1016.4 and 1016.5, and therefore violated Regulation P (12 C.F.R. § 1016) under the GLBA.

173. Defendant also failed to follow Section 501(b) of the GLBA, 15 U.S.C. § 6801(b), by not protecting the security, confidentiality, and integrity of customer information by failing to develop a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including failing to do one or more of the following: (a) designating one or more employees to coordinate the information security program; (b) 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; (c) 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; (d) overseeing service providers and requiring them by contract to protect the security and confidentiality of customer information; and (e) 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. Consequently, Defendant violated the Safeguard Rule of the GLBA.

174. Defendant's violations of Regulation P and the Safeguard Rule of the GLBA constitutes negligence per se.

175. Plaintiff and the Class are within the class of persons that Regulation P and the Safeguard Rule were intended to protect.

176. The harm that occurred as a result of the Data Breach is the type of harm Regulation P and the Safeguard Rule of the GLBA were intended to guard against.

177. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to control how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII for Plaintiff's and Class Members' respective lifetimes; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the 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 other identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the current and former customers' PII in their continued possession; and (viii) present and future costs in the form of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the compromise of PII as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class Members.

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

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

180. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff and the Class are now at an increased risk of identity theft or fraud.

181. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff and the Class are entitled to and demand actual, consequential, and nominal damages and injunctive relief to be determined at trial.

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

182. Plaintiff re-alleges and incorporates by reference paragraphs 1-139 as if fully set forth herein.

183. Plaintiff brings this Count on behalf of himself and the Class.

184. Defendant intentionally intruded into Plaintiff's and Class Members' seclusion by failing to keep their PII secure.

185. By failing to keep Plaintiff's and Class Members' PII secure, and allowing for access and disclosing of the PII to unauthorized parties for unauthorized use, Defendant unlawfully invaded Plaintiff's and Class Members' privacy right to seclusion by, *inter alia*:

(a) intruding into their private affairs in a manner that would be highly offensive to a reasonable persons;

(b) invading their privacy by improperly using their PII properly obtained for a specific purpose for another purpose, or disclosing it to unauthorized persons;

(c) failing to adequately secure their PII from disclosure to unauthorized

persons; and

(d) enabling the disclosure of their PII without consent.

186. The PII that was publicized during the Data Breach was highly sensitive, private, and confidential, as it included private financial, employment, and personal information.

187. As a direct and proximate result of Defendant's intrusion upon seclusion, Plaintiff and Class Members suffered injury and sustained actual losses and damages as alleged herein. Plaintiff and Class Members alternatively seek an award of nominal damages.

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

188. Plaintiff re-alleges and incorporates by reference paragraphs 1-139 as if fully set forth herein.

189. Plaintiff brings this Count on behalf of himself and the Class.

190. For years and continuing to today, Defendant's business model has depended upon it being entrusted with customers' PII. Trust and confidence are critical and central to the services provided by Defendant in the financing industry. Unbeknownst to Plaintiff and absent Class Members, however, Defendant did not secure, safeguard, or protect its customers' and employees' data and employed deficient security procedures and protocols to prevent unauthorized access to customers' PII. Defendant's deficiencies described herein were contrary to its security messaging.

191. Plaintiff and absent Class Members received services from Defendant, and Defendant were provided with, and allowed to collect and store, their PII on the mistaken belief that Defendant complied with its duties to safeguard and protect its customers' and employees' PII. Upon information and belief, putting its short-term profit ahead of safeguarding PII, and unbeknownst to Plaintiff and absent Class Members, Defendant knowingly sacrificed data security to save money.

192. Upon information and belief, Defendant knew that the manner in which it maintained and transmitted customer PII violated industry standards and their fundamental duties to Plaintiff and absent Class Members by neglecting well-accepted security measures to ensure confidential information was not accessible to unauthorized access. Defendant had knowledge of methods for designing safeguards against unauthorized access and eliminating the threat of exploit, but it did not use such methods.

193. Defendant had within its exclusive knowledge, and never disclosed, that it had failed to safeguard and protect Plaintiff's and absent Class Members' PII. This information was not available to Plaintiff, absent Class Members, or the public at large.

194. Defendant also knew that Plaintiff and Class Members expected security against known risks and that it was required to adhere to state and federal standards for the protection of confidential personally identifying, financial, and other personal information.

195. Plaintiff and absent Class Members did not expect that Defendant would knowingly insecurely maintain and hold their PII when that data was no longer needed to facilitate a business transaction or other legitimate business reason. Likewise, Plaintiff and absent Class Members did not know or expect that Defendant would employ substantially deficient data security systems and fail to undertake any required monitoring or supervision of the entrusted PII.

196. Had Plaintiff and absent Class Members known about Defendant's efforts to deficiencies and efforts to hide its ineffective and substandard data security systems, Plaintiff and absent Class Members would not have entered business dealings with Defendant.

197. By withholding the facts concerning the defective security and protection of customer PII, Defendant put its own interests ahead of the very customers who placed their trust and confidence in Defendant and benefitted itself to the detriment of Plaintiff and absent Class

Members.

198. As a result of its conduct as alleged herein, Defendant sold more services than it otherwise would have, and was able to charge Plaintiff and Class Members more for financial services than it otherwise could have. Defendant was unjustly enriched by charging for and collecting for those services that it would not have obtained to the detriment of Plaintiff and absent Class Members.

199. It would be inequitable, unfair, and unjust for Defendant to retain these wrongfully obtained fees and benefits. Defendant's retention of wrongfully obtained monies would violate fundamental principles of justice, equity, and good conscience.

200. Defendant's unfair and deceptive conduct to not disclose those defects have, among other things, caused Plaintiff and Class Members to enter a business arrangement that was deceptive and dangerous to their identities.

201. As a result, Plaintiff and Class Members paid for services that they would not have paid for had Defendant disclosed the inadequacy of its data security practices.

202. Plaintiff and each Member of the proposed Class are each entitled to restitution and non-restitutionary disgorgement in the amount by which Defendant was unjustly enriched, to be determined at trial.

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

203. Plaintiff re-alleges and incorporates by reference paragraphs 1-139 as if fully set forth herein.

204. Plaintiff brings this Count on behalf of himself and the Class.

205. HSB solicited and invited prospective customers to provide their PII as part of its regular business practices. HSB acquired and maintained the PII of Plaintiff and the Class, including names, birthdates, Social Security numbers, and financial account information provided in connection with entering into a relationship to receive financial services.

206. When Plaintiff and Class Members paid money and provided their PII to HSB in exchange for goods or services, they entered into implied contracts with HSB and its vendors, pursuant to which HSB agreed to safeguard and protect such information and to timely and accurately notify them if their data had been breached and compromised.

207. HSB solicited and invited prospective customers to provide their PII as part of its regular business practices. As a condition of receiving services, HSB required Plaintiff and Class Members to provide their PII, including names, Social Security numbers, dates of birth, financial account numbers, and other information.

208. Pursuant to FTC guidelines and standard practice in the financial industry, HSB was obligated to take reasonable steps to maintain the security of Plaintiff's and Class Members' PII. As a result, by requesting that Plaintiff and Class Members provide their PII as part of their doing business with HSB, HSB implicitly promised to adhere to these industry standards.

209. Plaintiff and Class Members each accepted HSB's offers and provided their PII to HSB. In entering into such implied contracts, Plaintiff and the Class reasonably believed that HSB's data security practices and policies, were reasonable and consistent with industry standards, and that HSB would use part of the fees received from Plaintiff and the Class to pay for adequate and reasonable data security practices to safeguard the PII.

210. Plaintiff and Class Members accepted HSB offers and provided their PII to Defendant. Defendant accepted the PII, and there was a meeting of the minds that Defendant would secure, protect, and keep the PII confidential.

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

212. Plaintiff and Class Members would not have entered into transactions with Defendant if Plaintiff and Class Members had known that Defendant would not protect their PII.

213. Plaintiff and the Class would not have provided and entrusted their PII to HSB in the absence of the implied contract between them and HSB to keep the information secure.

214. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

215. Defendant breached its implied contracts with Plaintiff and the Class by failing to safeguard and protect their PII and by failing to provide timely and accurate notice that their PII was compromised as a result of the Data Breach.

216. As a direct and proximate result of Defendant's breaches of their implied contracts, Plaintiff and the Class sustained actual losses and damages as described herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

A. For an Order certifying the Class, and appointing Plaintiff and his counsel to represent the certified Class and/or Classes;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and the Class Members' PII, and from refusing to issue prompt, complete, any accurate

disclosures to Plaintiff and Class Members;

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

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

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

iii. requiring Defendant to delete, destroy, and purge the 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 the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff's and Class Members' personal identifying information;

v. prohibiting Defendant from maintaining Plaintiff's and Class Members' on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on

Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

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

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

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

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

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

xii. requiring Defendant 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 Defendant to implement a system of tests to assess its respective

employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting PII;

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

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

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

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

D. For an award of damages, including a sum of money sufficient to provide to Plaintiff and Class Members identity theft protection services for their respective

lifetimes.

E. For an award of damages, including actual, statutory, nominal, and consequential damages, as allowed by law in an amount to be determined;

F. For an award of punitive damages;

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

H. For prejudgment interest on all amounts awarded; and

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

JURY TRIAL DEMAND

A jury trial is demanded by Plaintiff and the putative Class Members as to all issues so triable.

Dated: May 10, 2023

Respectfully submitted,

/s/ Joe Kendall

JOE KENDALL
Texas Bar No. 11260700
KENDALL LAW GROUP, PLLC
3811 Turtle Creek Blvd., Suite 1450
Dallas, Texas 75219
214-744-3000 / 214-744-3015 (Facsimile)
jkendall@kendalllawgroup.com

M. Anderson Berry, Esq.*
Gregory Haroutunian, Esq.*
CLAYEO C. ARNOLD, A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Phone: (916) 239-4778
Fax: (916) 924-1829
aberry@justice4you.com
gharoutunian@justice4you.com
*pro hac vice forthcoming

Attorneys for Plaintiff and the Proposed Class

ClassAction.org
