UNITED STATES DISTRICT COURT
DISTRICT OF MARYLAND

SEBHIA M. DIBRA, individually and on behalf of all others similarly situated, Plaintiff, v. LAFAYETTE FEDERAL CREDIT UNION, Defendant.	Case No. 8:25-cv-01054 **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Sebhia M. Dibra ("Plaintiff"), individually and on behalf of all others similarly situated ("Class Members"), brings this Class Action Complaint against Defendant Lafayette Federal Credit Union ("Defendant"), alleging as follows based upon personal knowledge, information and belief, and investigation of counsel.

NATURE OF THE ACTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard Plaintiff's and similarly situated Class Members' sensitive personally identifiable information ("PII"),[1] which, as a result, has been wrongfully disclosed to criminal cyberthieves.

2. In February 2025, hackers targeted and accessed Defendant's network systems through and stole Plaintiff's and Class Members' sensitive, confidential PII stored therein, including their full names in combination with their Social Security numbers, financial account numbers, loan account numbers, and other sensitive data, causing widespread injuries to Plaintiff

[1] The Federal Trade Commission ("FTC") defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth. . . .." 17 C.F.R. § 248.201(b)(8).

and Class Members (the "Data Breach").

3. Defendant is a financial institution that operates eight full-service branch locations in the District of Columbia, Maryland and Virginia.

4. Plaintiff and Class Members are current and former customers of Defendant who, in order to obtain services from Defendant, were and are required to entrust Defendant with their sensitive, non-public PII. Defendant could not perform its operations or provide its services without collecting Plaintiff's and Class Members' PII and retains it for many years, at least, even after the customer relationship has ended.

5. Businesses like Defendant that handle PII owe the individuals to whom that data relates a duty to adopt reasonable measures to protect such information from disclosure to unauthorized third parties, and to keep it safe and confidential. This duty arises under contract, statutory and common law, industry standards, representations made to Plaintiff and Class Members, and because it is foreseeable that the exposure of PII to unauthorized persons—and especially hackers with nefarious intentions—will harm the affected individuals, including but not limited to by the invasion of their private financial matters.

6. Defendant breached these duties owed to Plaintiff and Class Members by failing to safeguard their PII it collected and maintained, including by failing to implement industry standards for data security to protect against, detect, and stop cyberattacks, which failures allowed criminal hackers to access and steal at least thousands of consumers' PII from Defendant's care.

7. According to Defendant's notice of the Data Breach provided to Data Breach victims ("Notice Letter"), Defendant determined "that an unknown, unauthorized third party gained access to one LFCU employee email account" on September 16, 2024, which contained sensitive customer PII.

8. Although the Data Breach took place on or before September 16, 2024, Defendant failed to notify affected individuals that their PII was compromised until approximately March 20, 2025—diminishing Plaintiff's and Class Members' ability to timely and thoroughly mitigate and address the increased, imminent risk of identity theft and other harms the Data Breach caused.

9. Defendant failed to adequately protect Plaintiff's and Class Members' PII, and failed to even encrypt or redact this highly sensitive data. This unencrypted, unredacted PII was compromised due to Defendant's negligent and/or careless acts and omissions and its utter failure to protect its customers' sensitive data.

10. Defendant maintained the PII in a reckless manner. In particular, PII was maintained on and/or accessible from Defendant's network in a condition vulnerable to cyberattacks. The mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' PII was a known risk to Defendant, and thus, Defendant knew that failing to take reasonable steps to secure the PII left it in a dangerous condition.

PARTIES

Plaintiff Sebhia Dibra

11. Plaintiff is an adult individual who at all relevant times has been a citizen and resident of the state of New York.

12. Plaintiff is a former customer of Defendant and received financial services from Defendant prior to the Data Breach. Plaintiff provided her PII to Defendant as a condition of and in exchange for obtaining financial and related services from Defendant.

13. Plaintiff greatly values her privacy and is very careful about sharing her sensitive PII. Plaintiff diligently protects her PII and stores any documents containing PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet

or any other unsecured source. Plaintiff would not have provided her PII to Defendant had she known it would be kept using inadequate data security and vulnerable to a cyberattack.

14. At the time of the Data Breach, Defendant retained Plaintiff's PII in its network systems with inadequate data security, causing Plaintiff's PII to be accessed and exfiltrated by cybercriminals in the Data Breach.

15. On or about March 20, 2025, Plaintiff received Defendant's Notice Letter informing that her PII was accessed and exposed to unauthorized hackers in the Data Breach. According to the Notice Letter, the hackers acquired files containing Plaintiff's sensitive PII, including her name, Social Security number, financial account number, and loan account number.

16. Plaintiff has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff now monitors her financial and credit statements multiple times a week and has spent hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities.

17. Plaintiff further anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data Breach, Plaintiff is at a present risk and will continue to be at risk of identity theft and fraud for years.

18. The risk of identity theft is impending and has materialized, as there is evidence that Plaintiff's and Class Members' PII was targeted, accessed, and misused, including through likely publication and dissemination on the dark web. Plaintiff further believes her PII, and that of Class Members, was and will be sold and disseminated on the dark web following the Data Breach as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

19. The Data Breach has also caused Plaintiff to suffer fear, anxiety, and stress about

her PII now being in the hands of cybercriminals, compounded by the fact that Defendant still has not fully informed her of key details about the Data Breach's occurrence or the information stolen.

20. Moreover, since the Data Breach Plaintiff has experienced a spike in spam calls and texts using her PII compromised in the Data Breach, causing additional inconvenience.

PARTIES

21. Plaintiff Sebhia Dibra is a resident and citizen of the state of New York

22. Defendant is a company with its principal place of business located in Rockville, Maryland.

JURISDICTION AND VENUE

23. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). There are at least 100 putative Class Members, the aggregated claims of the individual Class Members exceed the sum or value of $5,000,000 exclusive of interest and costs, and members of the proposed Class, including Plaintiff, are citizens of states different from Defendant.

24. This Court has personal jurisdiction over Defendant because Defendant's principal place of business is in Maryland and Defendant engaged in substantial activity in this state.

25. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1)–(d) because Defendant's principal place of business is located in this District and a substantial part of the events and omissions giving rise to this action occurred in this District.

FACTUAL BACKGROUND

A. Defendant Owed Duties to Adopt Reasonable Data Security Measures for PII.

26. Defendant is a financial institution that operates eight full-service branch locations in the District of Columbia, Maryland and Virginia.

27. Plaintiff and Class Members are current and former customers of Defendant who received financial and related services from Defendant on or prior to September 16, 2024.

28. As a condition of receiving financial and related services from Defendant, Defendants' customers, including Plaintiff and Class Members, were required to entrust Defendant with highly sensitive PII, including their names, Social Security numbers, financial account number, loan account number, and other sensitive data.

29. In exchange for receiving Plaintiff's and Class Members' PII, Defendant promised to safeguard the sensitive, confidential data and use it only for authorized and legitimate purposes, and to delete such information from its systems once there was no longer a need to maintain it.

30. The information Defendant held in its computer networks at the time of the Data Breach included the unencrypted PII of Plaintiff and Class Members.

31. At all relevant times, Defendant knew it was storing and using its networks to store and transmit valuable, sensitive PII belonging to Plaintiff and Class Members, and that as a result, its systems would be attractive targets for cybercriminals.

32. Defendant also knew that any breach of its information technology network and exposure of the data stored therein would result in the increased risk of identity theft and fraud for the individuals whose PII was compromised, as well as intrusion into those individuals' highly private financial matters.

33. Defendant made promises and representations to its customers, including Plaintiff and Class Members, that the PII collected from them as a condition of obtaining financial and services from Defendant would be kept safe and confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it were no longer required to maintain it.

34. Defendant's Privacy Policy, published on Defendant's website and in effect when the Data Breach took place, promises and warrants

> to protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. We maintain physical, electronic, and procedural safeguards that comply with federal regulations to guard your non-public personal information. Lafayette Federal will retain your personal data only for as long as is necessary for the purposes set out in this privacy policy. We will retain and use your personal data to the extent necessary to comply with our legal obligations (for example, if we are required to retain your data to comply with applicable laws), resolve disputes, and enforce our legal agreements and policies.[2]

35. Plaintiff and Class Members relied on these promises from Defendant, a sophisticated financial institution, to implement reasonable practices to keep their sensitive PII confidential and securely maintained, to use this information for necessary purposes only and make only authorized disclosures of this information, and to delete PII from Defendant's systems when no longer necessary for its legitimate business purposes.

36. But for Defendant's promises to keep Plaintiff's and Class Members' PII secure and confidential, Plaintiff and Class Members would not have sought services from or entrusted their PII to Defendant. Consumers in general demand security to safeguard their PII, especially when sensitive financial information is involved.

37. Based on the foregoing representations and warranties and to obtain services from Defendant, Plaintiff and Class Members provided their PII to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its promises and obligations to keep such information confidential and protected against unauthorized access.

B. Defendant Failed to Adequately Safeguard Plaintiff's and Class Member's PII, Causing the Data Breach.

---

[2] *See Lafayette Federal Credit Union*, https://www.lfcu.org/privacy-policy/ (last visited March 28, 2025).

38. On or about March 21, 2025, Defendant began sending Plaintiff and other Data Breach victims Notice Letters informing them of the Data Breach.

39. The Notice Letters generally state as follows, in part:

> **What Happened?** We recently learned that an unknown, unauthorized third party gained access to one LFCU employee email account. Upon discovering the incident, we promptly secured the email account and began an internal investigation. We also engaged a forensic security firm to investigate and confirm the security of our email systems. The investigation determined that an unauthorized third party accessed the email account for a brief period on September 16, 2024, and may have acquired the information contained in the account
>
> **What Information Was Involved?** . . . . we completed our review and determined that the email account contained some of your personal information, including your name in combination with your Social Security number, financial account number, and loan account number.[3]

40. Omitted from the Notice Letter were the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their PII is protected.

41. Thus, Defendant's purported 'disclosure' amounts to no real disclosure at all, as it fails to inform Plaintiff and Class Members of the Data Breach's critical facts with any degree of specificity. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

42. To make matters worse, although the Data Breach occurred on or before September 16, 2024, Defendant waited until March 20, 2025, before it began notifying affected individuals about their PII being compromised, diminishing Plaintiff's and Class Members' ability to timely

[3] *See* Notice Letter sent to Plaintiff from Defendant on March 20, 2025 (attached as **Exhibit A**).

and thoroughly mitigate and address harms resulting from the unauthorized disclosure.

43. Plaintiff's and Class Members' PII was targeted, accessed, and stolen by cybercriminals in the Data Breach. Criminal hackers accessed and acquired confidential files containing Plaintiff's and Class Members' PII from Defendant's network systems, where they were kept without adequate safeguards and in unencrypted form.

44. Defendant could have prevented this Data Breach by properly training personnel, securing account access through measures like phishing-resistant (i.e., non-SMS text based) multi-factor authentication ("MFA") for as many services as possible, training users to recognize and report phishing attempts, implementing recurring forced password resets, and/or securing and encrypting files and file servers containing Plaintiff's and Class Members' PII, but failed to do so.

45. As the Data Breach evidences, Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive PII it collected and maintained from Plaintiff and Class Members, such as phishing-resistant MFA, standard monitoring and altering techniques, encryption, or deletion of information when it is no longer needed. These failures by Defendant allowed and caused cybercriminals to target Defendant's network, access it through Defendant's employee email account, and exfiltrate files containing Plaintiff and Class Member's PII.

46. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing Plaintiff's and Class Members' PII, using controls like limitations on personnel with access to sensitive data and requiring phishing-resistant MFA for access, training its employees on standard cybersecurity practices, and implementing reasonable logging and alerting methods to detect unauthorized access.

47. For example, if Defendant had implemented industry standard logging, monitoring,

and alerting systems—basic technical safeguards that any PHI and/or PII-collecting company is expected to employ—then cybercriminals would not have been able to perpetrate malicious activity in Defendant's network systems for the days-long period it took to carry out the Data Breach, including the reconnaissance necessary to identify where Defendant stored PII, installation of malware or other methods of establishing persistence and creating a path to exfiltrate data, staging data in preparation for exfiltration, and then exfiltrating that data outside of Defendant's system without being caught.

48. Defendant would have recognized the malicious activities detailed in the preceding paragraph if it bothered to implement basic monitoring and detection systems, which then would have stopped the Data Breach or greatly reduced its impact.

49. Further, upon information and belief, had Defendant required phishing-resistant MFA, and/or trained its employees on reasonable and basic cybersecurity topics like common phishing techniques or indicators of a potentially malicious event, cybercriminals would not have been able to gain initial access to Defendant's network to perpetrate this Data Breach.

50. Defendant's tortious conduct and breach of contractual obligations, as detailed herein, are evidenced by its failure to recognize the Data Breach until cybercriminals had already accessed Plaintiff's and Class Members' PII, meaning Defendant had no effective means in place to ensure that cyberattacks were detected and prevented.

C. Defendant Knew of the Risk of a Cyberattack where Businesses in Possession of PII Are Particularly Suspectable.

51. Defendant's negligence in failing to safeguard Plaintiff's and Class Members' PII is exacerbated by the repeated warnings and alerts directed to protecting and securing such data.

52. PII of the kind accessed in the Data Breach is of great value to hackers and cybercriminals as it can be used for a variety of unlawful and nefarious purposes, including

ransomware, fraudulent misuse, and sale on the dark web.

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

54. Data thieves regularly target entities in the financial industry like Defendant due to the highly sensitive information that such entities maintain. Defendant knew and understood that unprotected PII is valuable and highly sought after by criminal parties who seek to illegally monetize that PII through unauthorized access.

55. Data breaches and identity theft have a crippling effect on individuals, and detrimentally impact the economy as a whole.[4]

56. Cyber-attacks against businesses such as Defendant are targeted and frequent. According to Contrast Security's 2023 report *Cyber Bank Heists: Threats to the financial sector*, "Over the past year, attacks have included banking trojans, ransomware, account takeover, theft of client data and cybercrime cartels deploying 'trojanized' finance apps to deliver malware in spear-phishing campaigns."[5]

57. In light of past high profile data breaches at industry-leading companies, including, for example, 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

[4] *Id.*

[5] Contrast Security, "Cyber Bank Heists: Threats to the financial sector," pg. 5, avail. at https://www.contrastsecurity.com/hubfs/Cyber%20Bank%20Heists%20Report%202023.pdf?hsLang=en (last acc. February 9, 2024).

records, May 2020), Defendant knew or, if acting as a reasonable business, should have known that the PII it collected and maintained would be vulnerable to and targeted by cybercriminals.

58. According to the Identity Theft Resource Center's report covering the year 2021, "the overall number of data compromises (1,862) is up more than 68 percent compared to 2020. The new record number of data compromises is 23 percent over the previous all-time high (1,506) set in 2017. The number of data events that involved sensitive information (Ex: Social Security numbers) increased slightly compared to 2020 (83 percent vs. 80 percent)."[6]

59. The increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant itself. According to IBM's 2022 report, "[f]or 83% of companies, it's not if a data breach will happen, but when."[7]

60. As a business in possession of its current and former customers' PII, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to it by Plaintiff and Class Members and of the foreseeable consequences if its data security systems were breached. Such consequences include the significant costs imposed on Plaintiff and Class Members due to a breach. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

61. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being wrongfully disclosed to cybercriminals.

---

[6] *See* "Identity Theft Resource Center's 2021 Annual Data Breach Report Sets New Record for Number of Compromises," Jan. 24, 2022, available at https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data- breach-report-sets-new-record-for-number-of-compromises/ (last accesses Mar. 28, 2025).

[7] IBM, "Cost of a data breach 2022: A million-dollar race to detect and respond," available at https://www.ibm.com/reports/data-breach (last accessed Mar. 28, 2025).

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

63. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on its network server(s), amounting to at least tens of thousands of individuals' detailed PII, and, thus, the significant number of individuals who would be harmed by the exposure of that unencrypted data.

64. Plaintiff and Class Members were the foreseeable and probable victims of Defendant's inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing PII and the critical importance of providing adequate security for that information.

65. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Plaintiff and Class Members especially vulnerable to identity theft, tax fraud, credit and bank fraud, and the like.

D. Defendant Was Required, but Failed to Comply with FTC Rules and Guidance.

66. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

67. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses like Defendant. These 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.[8]

68. The FTC's 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.[9]

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

70. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect third parties' confidential 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 FTC Act. Orders resulting from these actions further clarify the measures business like Defendant must undertake to meet their data security obligations.

71. Such FTC enforcement actions include actions against entities that fail to protect consumer PII like Defendant. *See, e.g., In the Matter of LabMD, Inc*., 2016-2 Trade Cas. (CCH) ¶

[8] *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 accessed Mar. 28, 2025).
[9] *Id.*

79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

72. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect sensitive personal information, like PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

73. The FTC has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis and profit."[10]

74. Defendant failed to properly implement basic data security practices, in violation of its duties under the FTC Act.

75. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' PII or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

E. Defendant was Required, But Failed, to Comply With the GLBA.

76. The GLBA states, "It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect

[10] Statement of FTC Commissioner Pamela Jones Harbour (Remarks Before FTC Exploring Privacy Roundtable), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf.

the security and confidentiality of those customers' nonpublic personal information." 15 U.S.C. § 6801(a).

77. Defendant is a financial institution for purposes of the GLBA, because it is "significantly engaged in financial activities, or significantly engaged in activities incidental to such financial activities," 16 C.F.R. § 314.2(h), by providing financial services.

78. "Nonpublic personal information" means "personally identifiable financial information provided by a consumer to a financial institution; resulting from any transaction with the consumer or any service performed for the consumer; or otherwise obtained by the financial institution." 15 U.S.C. § 6809(4)(A)(i)–(iii).

79. The PII involved in the Data Breach constitutes "nonpublic personal information" for purposes of the GLBA.

80. Defendant collects "nonpublic personal information," as defined by 15 U.S.C. § 6809(4)(A), 16 C.F.R. § 313.3(n) & 12 C.F.R. § 1016.3(p)(1). Accordingly, during the relevant time period, Defendant was subject to the requirements of the GLBA, 15 U.S.C. §§ 6801, *et seq*., and to numerous rules and regulations promulgated under the GLBA.

81. 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: (i) designating one or more employees to coordinate the information security program; (ii) 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; (iii) 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; (iv) overseeing service providers and requiring them by contract to protect the security and confidentiality of customer information; and (v) 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 & 314.4. As alleged herein, Defendant violated the Safeguards Rule.

82. Defendant's conduct resulted in a variety of failures to follow GLBA-mandated rules and regulations, many of which are also industry standard. Among such deficient practices, the Data Breach demonstrates that Defendant failed to implement (or inadequately implemented) information security policies or procedures such as effective employee training, adequate intrusion detection systems, regular reviews of audit logs and records, and other similar measures to protect the confidentiality of the PII it maintained in its information technology systems.

83. Had Defendant implemented data security protocols, the consequences of the Data Breach could have been avoided, or at least significantly reduced as the Data Breach could have been detected earlier, the amount of PII compromised could have been greatly reduced.

F. Defendant Failed to Comply with Industry Standards.

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

85. The Center for Internet Security's (CIS) Critical Security Controls (CSC) recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including Critical Security Controls of Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability

Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security, Incident Response Management, and Penetration Testing.[11]

86. In addition, the NIST recommends certain practices to safeguard systems[12]:

a. Control who logs on to your network and uses your computers and other devices.

b. Use security software to protect data.

c. Encrypt sensitive data, at rest and in transit.

d. Conduct regular backups of data.

e. Update security software regularly, automating those updates if possible.

f. Have formal policies for safely disposing of electronic files and old devices.

g. Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.

87. Further still, the Cybersecurity & Infrastructure Security Agency ("CISA") makes specific recommendations to organizations to guard against cybersecurity attacks, including (a) reducing the likelihood of a damaging cyber intrusion by validating that "remote access to the organization's network and privileged or administrative access requires multi-factor authentication, [e]nsur[ing] that software is up to date, prioritizing updates that address known

[11] *See* Rapid7, "CIS Top 18 Critical Security Controls Solutions," available at https://www.rapid7.com/solutions/compliance/critical-controls/ (last acc. Mar. 28, 2025).

[12] Federal Trade Commission, "Understanding The NIST Cybersecurity Framework," https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist- framework (last acc. Mar. 28, 2025).

exploited vulnerabilities identified by CISA[,] [c]onfirm[ing] that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes," and other steps; (b) taking steps to quickly detect a potential intrusion, including "[e]nsur[ing] that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior [and] [e]nabl[ing] logging in order to better investigate issues or events[;] [c]onfirm[ing] that the organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated," and (c) "[e]nsur[ing] that the organization is prepared to respond if an intrusion occurs," and other steps.[13]

88. Upon information and belief, Defendant failed to implement industry-standard cybersecurity measures, including by failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, and by failing to comply with other industry standards for protecting Plaintiff's and Class Members' PII, resulting in the Data Breach.

G. Defendant Owed Plaintiff and Class Members a Common Law Duty to Safeguard their PII.

89. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant's duty owed to Plaintiff and

[13] Cybersecurity & Infrastructure Security Agency, "Shields Up: Guidance for Organizations," available at https://www.cisa.gov/shields-guidance-organizations (last acc. Mar. 28, 2025).

Class Members obligated it to provide reasonable data security, including consistency with industry standards and requirements, and to ensure its computer systems, networks, and protocols adequately protected Plaintiff's and Class Members' PII.

90. Defendant owed a duty to Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect the PII in its possession, including adequately training its employees and others who accessed PII within its computer systems on how to adequately protect PII.

91. Defendant owed a duty to Plaintiff and Class Members to implement processes that would detect a compromise of PII in a timely manner and act upon data security warnings and alerts in a timely fashion.

92. Defendant owed a duty to Plaintiff and Class Members to disclose in a timely and accurate manner when and how the Data Breach occurred.

93. Defendant owed a duty of care to Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

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

H. Plaintiff and Class Members Suffered Common Injuries and Damages due to Defendant's Conduct.

95. Defendant's failure to implement or maintain adequate data security measures for Plaintiff's and Class Members' PII directly and proximately injured Plaintiff and Class Members by the resulting disclosure of their PII in the Data Breach.

96. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen fraudulent use of that information and

damage to victims may continue for years.

97. Plaintiff and Class Members are also at a continued risk because their Private remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack and are subject to further attack so long as Defendant fails to undertake the necessary and appropriate security and training measures to protect its customers' PII.

98. As a result of Defendant's ineffective and inadequate data security practices, the resulting Data Breach, and the foreseeable consequences of their PII ending up in criminals' possession, the risk of identity theft to Plaintiff and Class Members has materialized and is imminent, and they have all sustained actual injuries and damages, including, without limitation, (a) invasion of privacy; (b) financial 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; (d) financial costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) deprivation of value of their PII; (g) loss of the benefit of their bargain with Defendant; (h) emotional distress including anxiety and stress in dealing with the Data Breach's aftermath; and (i) the continued risk to their sensitive 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 it collects and maintains.

The Risk of Identity Theft to Plaintiff and Class Members Is Present and Ongoing.

99. Plaintiff and Class Members are at a heightened risk of identity theft for years to come because of the Data Breach.

100. The FTC defines identity theft as "a fraud committed or attempted using the

identifying information of another person without authority."[14] 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 "[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."[15]

101. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal individuals' personal data to monetize the information. Criminals monetize the data by selling the stolen information on the internet black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

102. The dark web is an unindexed layer of the internet that requires special software or authentication to access.[16] Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or "surface" web, dark web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[17] This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

103. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs, and frequently, personal and medical information like the PII at

[14] 17 C.F.R. § 248.201 (2013).
[15] *Id.*
[16] *What Is the Dark Web?*, Experian, available at https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.
[17] *Id.*

issue here.[18] The digital character of PII stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the internet and the buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social Security numbers, dates of birth, and medical information.[19] As Microsoft warns "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others."[20]

104. The unencrypted PII of Plaintiff and Class Members will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted and detailed PII may fall into the hands of companies that will use it for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the Plaintiff's and Class Members' PII.

105. Because a person's identity is akin to a puzzle with multiple data points, 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 to track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

Loss of Time to Mitigate the Risk of Identify Theft and Fraud

106. 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 PII was compromised, as in this Data Breach, the

[18] *What is the Dark Web?* – Microsoft 365, available at https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.
[19] *Id.; What Is the Dark Web?*, Experian, available at https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.
[20] *What is the Dark Web?* – Microsoft 365, available at https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.

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 asset of time has been lost.

107. In the event that Plaintiff and Class Members experience actual identity theft and fraud, 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

108. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class Members must monitor their financial accounts for many years to mitigate that harm.

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

110. These efforts are 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.[21]

[21] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited Feb. 26, 2024).

111. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of Defendant's conduct that caused the Data Breach.

Diminished Value of PII

112. Personal data like PII is a valuable property right.[22] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

113. An active and robust legitimate marketplace for personal information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[23] 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.[24, 25] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50 a year.[26]

114. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and black markets, has been damaged and diminished in its value by its unauthorized and likely release onto the dark web, where holds significant value

---

[22] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).
[23] https://www.latimes.com/business/story/2019-11-05/column-data-brokers.
[24] https://datacoup.com/.
[25] https://digi.me/what-is-digime/.
[26] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html.

for the threat actors.

115. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

Future Cost of Credit and Identify Theft Monitoring Is Reasonable and Necessary.

116. To date, Defendant has done little to provide Plaintiff and Class Members with relief for the damages they have suffered due to the Data Breach.

117. Given the type of targeted attack in this case and sophisticated criminal activity, the type of information involved, and the *modus operandi* of cybercriminals, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the dark web for sale and purchase by criminals intending to utilize the PII 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 insurance; or filing false unemployment claims.

118. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her information 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.

119. 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 their cards and request a replacement.[27] The information

[27] *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.

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

120. The retail cost of credit monitoring and identity theft monitoring can cost $200 or more a year per Class Member. This is a reasonable and necessary cost to protect Class Members from the risk of identity theft that arose from Defendant's 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 Defendant's failure to safeguard their PII.

Lost Benefit of the Bargain

121. Furthermore, Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain.

122. When agreeing to provide their PII, which was a condition precedent to obtain financial and related services from Defendant, Plaintiff and Class Members, as customers and consumers, understood and expected that they were, in part, paying for services and data security to protect the PII they were required to provide.

123. In fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received services of a lesser value than what they reasonably expected to receive under the bargains struck with Defendant.

CLASS ACTION ALLEGATIONS

124. Plaintiff brings this nationwide class action individually and on behalf of all other persons similarly situated pursuant to Federal Rule of Civil Procedure 23(a) and 23(b).

125. Plaintiff proposes the following nationwide class definition, subject to amendment as appropriate:

> All individuals residing in the United States whose PII may have been compromised in the Data Breach, including all individuals who received a Notice Letter (the "Class").

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

127. Plaintiff hereby reserves the right to amend or modify the Class definition with greater specificity or division after having had an opportunity to conduct discovery.

128. Numerosity. The members of the Class are so numerous that joinder of all of them is impracticable. According to the breach report submitted to the Office of the Maine Attorney General, approximately 75,545 persons were impacted in the Data Breach. [28]

129. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

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

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

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

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

[28] https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/6c038d1f-41db-4c57-9bdd-c1c7215b7eba.html (last acc. Mar. 28, 2025).

e. Whether Defendant owed a duty to Class Members to safeguard their PII;

f. Whether Defendant breached its duty to Class Members to safeguard their PII;

g. Whether computer hackers 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 Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant breached implied contracts for adequate data security with Class Members;

l. Whether Defendant was unjustly enriched by retention of the monetary benefits conferred on it by Class Members; and

m. Whether Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

130. Typicality. 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.

131. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions.

132. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' PII was stored on the same computer systems 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.

133. Superiority. 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 and party resources, and protects the rights of each Class Member.

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

135. Likewise, particular issues are appropriate for certification pursuant to Federal Rule of Civil Procedure 23(c)(4) 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 the following:

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

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

c. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

d. Whether Defendant failed to take commercially reasonable steps to safeguard customer PII; and

e. Whether adherence to FTC or GLBA data security guidelines and/or measures recommended by data security experts would have reasonably prevented the Data Breach.

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

CAUSES OF ACTION

COUNT I
NEGLIGENCE/NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

137. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 162 above as if fully set forth herein.

138. Defendant required Plaintiff and Class Members to submit sensitive, confidential PII to Defendant as a condition of receiving financial and related services from Defendant.

139. Plaintiff and Class Members provided their PII to Defendant, including their names, Social Security numbers, financial account numbers, loan account numbers, and other sensitive data.

140. Defendant had full knowledge of the sensitivity of the PII to which it was entrusted, and the types of harm that Plaintiff and Class Members could and would suffer if the PII was wrongfully disclosed to unauthorized persons.

141. Defendant owed a duty to Plaintiff and each Class Member to exercise reasonable care in holding, safeguarding, and protecting the PII it collected from them.

142. Plaintiff and Class Members were the foreseeable victims of any inadequate data safety and security practices by Defendant.

143. Plaintiff and Class Members had no ability to protect their PII in Defendant's possession.

144. By collecting, transmitting, and storing Plaintiff's and Class Members' PII Defendant owed Plaintiff and Class Members a duty of care to use reasonable means to secure and safeguard their PII, to prevent the information's unauthorized disclosure, and to safeguard it from theft or exfiltration to cybercriminals. Defendant's duty included the responsibility to implement processes by which it could detect and identify malicious activity or unauthorized access on its networks or servers.

145. Defendant owed a duty of care to Plaintiff and the Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that controls for its networks, servers, and systems, and the personnel responsible for them, adequately protected Plaintiff's and Class Members' PII.

146. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between it and its customers, which is recognized by laws and regulations including but not limited to the FTC Act, the GLBA, and the common law. Defendant was able to ensure its network servers and systems were sufficiently protected against the foreseeable harm a data breach would cause Plaintiff and Class Members, yet it failed to do so.

147. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the FTC 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.

148. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and Class Members' PII;

b. Maintaining and/or transmitting Plaintiff's and Class Members' PII in unencrypted and identifiable form;

c. Failing to implement data security measures, like adequate, phishing-resistant MFA for as many systems as possible, to safeguard against known techniques for initial unauthorized access to network servers and systems;

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

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

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

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

h. Failing to adequately notify Plaintiff and Class Members about the Data Breach so they could take appropriate steps to mitigate damages.

149. But for Defendant's wrongful and negligent breaches of its duties owed to Plaintiff and Class Members, their PII would not have been compromised because the malicious activity would have been prevented, or at least, identified and stopped before criminal hackers had a chance to inventory Defendant's digital assets, stage them, and then exfiltrate them.

150. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiff's and Class Members' PII would injure Plaintiff and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data

breaches in Defendant's industry.

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

152. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer injuries, including but not limited to (a) invasion of privacy; (b) lost or diminished value of their PII; (c) actual identity theft, or the imminent and substantial risk of identity theft or fraud; (d) out-of-pocket and lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (e) loss of benefit of the bargain; (f) anxiety and emotional harm due to their PII's disclosure to cybercriminals; and (g) the continued and certainly increased 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 it.

153. Plaintiff and Class Members are entitled to damages, including compensatory, consequential, punitive, and nominal damages, as proven at trial.

154. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (a) strengthen its data security systems and monitoring procedures; (b) submit to future annual audits of those systems and monitoring procedures; and (c) provide adequate and lifetime credit monitoring to Plaintiff and all Class Members.

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

155. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 162 above as if fully set forth herein.

156. Defendant required Plaintiff and Class Members to provide and entrust their PII to

Defendant as a condition of and in exchange for receiving financial and related services from Defendant.

157. When Plaintiff and Class Members provided their PII to Defendant, they entered into implied contracts with Defendant pursuant to which Defendant agreed to safeguard and protect such PII and to timely and accurately notify Plaintiff and Class Members if and when their PII was breached and compromised.

158. Specifically, Plaintiff and Class Members entered into valid and enforceable implied contracts with Defendant when they agreed to provide their PII to Defendant, and Defendant agreed to reasonably protect it.

159. The implied contracts that Plaintiff and Class Members entered into with Defendant included Defendant's promises to protect PII it collected from Plaintiff and Class Members, or created on its own, from unauthorized disclosures, including those contained in Defendant's Privacy Policy, set forth *supra*. Plaintiff and Class Members provided their PII to Defendant in reliance on its promises.

160. Under the implied contracts, Defendant promised and was obligated to (a) provide financial and related services to Plaintiff and Class Members; and (b) protect Plaintiff's and Class Members' PII provided to obtain such financial services and/or created in connection therewith. In exchange, Plaintiff and Class Members agreed to provide Defendant with their PII.

161. Defendant promised and warranted to Plaintiff and Class Members to maintain the privacy and confidentiality of the PII it collected from them, and to keep such information safeguarded against unauthorized access and disclosure.

162. Defendant's adequate protection of Plaintiff's and Class Members' PII was a material aspect of these implied contracts with Defendant.

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

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

165. Plaintiff and Class Members, who contracted with Defendant for services including reasonable data protection and provided their PII to Defendant, reasonably believed and expected that Defendant would adequately employ adequate data security to protect that PII.

166. A meeting of the minds occurred when Plaintiff and Class Members agreed to, and did, provide their PII to Defendant and agreed Defendant would receive payment for, amongst other things, the protection of their PII.

167. Plaintiff and Class Members performed their obligations under the contracts when they provided their PII and/or payment to Defendant.

168. Defendant materially breached its contractual obligations to protect the PII it required Plaintiff and Class Members to provide when that PII was unauthorizedly disclosed in the Data Breach due to Defendant's inadequate data security measures and procedures.

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

170. Defendant materially breached the terms of its implied contracts, including but not limited to by failing to comply with industry standards or the standards of conduct embodied in statutes or regulations like Section 5 of the FTC Act and the GLBA, and by failing to otherwise

protect Plaintiff's and Class Members' PII, as set forth *supra*.

171. The Data Breach was a reasonably foreseeable consequence of Defendant's breaches of these implied contracts with Plaintiff and Class Members.

172. Due to Defendant's failures to fulfill the data protections promised in these contracts, Plaintiff and Class Members did not receive the full benefit of their bargains with Defendant, and instead received services of a diminished value compared to that described in the implied contracts. Plaintiff and Class Members were therefore damaged in an amount at least equal to the difference in the value of the services with data security protection they paid and provided their PII for, and that which they received.

173. Had Defendant disclosed that its data security procedures were inadequate or that it did not adhere to industry standards for cybersecurity, neither Plaintiffs, Class Members, nor any reasonable person would have contracted with Defendant.

174. Plaintiff and Class Members would not have provided and entrusted their PII to Defendant in the absence of the implied contracts between them and Defendant.

175. Defendant breached the implied contracts it made with Plaintiff and Class Members by failing to safeguard and protect their PII and by failing to provide timely or adequate notice that their PII was compromised in and due to the Data Breach.

176. As a direct and proximate result of Defendant's breach of its implied contracts with Plaintiff and Class Members and the attendant Data Breach, Plaintiff and Class Members have suffered injuries and damages as set forth herein and have been irreparably harmed.

177. Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, to be proven at trial.

COUNT III
UNJUST ENRICHMENT

(On Behalf of Plaintiff and the Class)

178. Plaintiff re-alleges and incorporates by reference all the allegations contained in paragraphs 1 through 162 above, as if fully set forth herein.

179. Plaintiff pleads this claim for unjust enrichment in the alternative to the breach of implied contract count above.

180. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they provided their PII to Defendant, which Defendant used and depended on to operate its business. In exchange, Plaintiff and Class Members should have had their PII protected with adequate data security.

181. Defendant knew Plaintiff and Class Members conferred a benefit upon it, and accepted that benefit by retaining the PII and using it to generate revenue.

182. Defendant failed to secure Plaintiff's and Class Members' PII and, therefore, did not fully compensate Plaintiff or Class Members for the value that their PII provided Defendant.

183. Defendant acquired the PII through inequitable record retention as it failed to investigate and/or disclose the inadequate data security practices previously alleged.

184. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to its own pocket. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant' decision to prioritize its own financial condition over the requisite security and the safety of customers' PII.

185. Under the circumstances, it would be unjust for Defendant to retain the benefits that Plaintiff and Class Members conferred upon it.

186. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injuries and damages as set forth herein.

187. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Sebhia Dibra, individually and on behalf of all others similarly situated, prays for judgment as follows:

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

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

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

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

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

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

G. Awarding pre- and post-judgment interest, as provided by law;

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

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

JURY TRIAL DEMAND

Plaintiff hereby demands a trial by jury of all issues so triable.

Dated: March 31, 2025

Respectfully submitted,

/s/ Thomas A. Pacheco

Thomas A. Pacheco (Bar No. 201712140091)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
900 W Morgan Street
Raleigh, NC 27603
T: (212) 946-9305
tpacheco@milberg.com

Jeff Ostrow (*pro hac vice* forthcoming)
KOPELOWITZ OSTROW P.A.
One West Las Olas Blvd., Suite 500
Fort Lauderdale, FL 33301
Tel: 954-525-4100
ostrow@kolawyers.com

Counsel for Plaintiff and the Putative Class