UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA

KYLIE MEYER, individually and on behalf of all others similarly situated, Plaintiff, v. NCB MANAGEMENT SERVICES, INC. and BANK OF AMERICA CORPORATION, Defendants.	Case No. 2:23-cv-1340 **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

Plaintiff Kylie Meyer ("Plaintiff"), individually and on behalf of all others similarly situated, brings this Class Action Complaint against Defendants NCB Management Services ("NCB") and Bank of America Corporation ("BOA" and collectively with NCB, "Defendants"), based upon personal knowledge with respect to Plaintiff and upon information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters, and alleges the following:

NATURE OF THE ACTION

1. Plaintiff brings this class action on behalf of herself and all other similarly situated individuals ("Class members") who had their sensitive personal information ("PII") disclosed to in a data breach of NCB's system starting on or about February 1, 2023 (the "Data Breach").

2. On or about March 24, 2023, NCB sent letters to 494,969 individuals notifying them of the Data Breach and informing them that their sensitive PII was accessed by unauthorized hackers (the "Notice").[1] Specifically, the Notice claimed that "NCB discovered on February 4 that

[1] https://apps.web.maine.gov/online/aeviewer/ME/40/65d544dc-79b0-437c-a7f8-757ffec624af.shtml (last visited April 6, 2023).

an unauthorized party gained access to NCB's systems on February 1, 2023" and NCB "confirmed on March 8 that [impacted individuals'] client information previously connected with [their] Bank of America credit card account[s] was potentially obtained by the unauthorized party."[2]

3. The Notice informed Plaintiff and other impacted individuals that the hackers gained access to the following highly sensitive financial information and other PII through the hackers' unauthorized access of NCB's system:

a. first and last name,

b. address,

c. phone number,

d. email address,

e. date of birth,

f. employment position,

g. pay amount,

h. driver's license number,

i. Social Security number,

j. account number,

k. credit card number,

l. routing number,

m. account balance, and/or

n. account status.

4. In the ordinary course of its business, NCB purchases debt from lending institutions, such as BOA.[3] Through such debt purchases, NCB receives and stores the PII of the

[2] *Id*.

[3] https://therecord.media/debt-buyer-cyberattack-data-breach (last visited April 6, 2023).

customers/clients of the companies from which NCB purchases debt—such as the PII and other information listed above that was compromised in the Data Breach.[4]

5. One such company that NCB purchased debt from is BOA.[5] NCB's Notice explains that the Data Breach involved PII of individuals who "formerly had [a credit card account] with Bank of America."[6] By virtue of the Data Breach, BOA negligently sold and transferred Plaintiff's and Class members' past due BOA accounts to NCB without ensuring that NCB had adequate security safeguards in place to prevent and protect against the Data Breach and other cybersecurity risks. Through that transfer of data and information to NCB, BOA facilitated the Data Breach.

6. Thus, the Data Breach resulted from NCB's and BOA's failure to securely exchange Plaintiff's and Class members' PII and/or adequately protect and safeguard it from unauthorized access and other cybersecurity incidents such as the Data Breach.

7. Despite learning of the Data Breach on February 1, 2023, Defendants waited nearly two months before finally notifying impacted individuals on or about March 24, 2023, that their highly sensitive PII had been compromised in the Data Breach.

8. Defendants owed a duty to Plaintiff and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII against unauthorized access and disclosure. Defendants breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect individuals' PII from unauthorized access and disclosure.

9. As a direct and proximate result of Defendants' inadequate security and breach of

---

[4] *Id.*
[5] *Id.*
[6] https://apps.web.maine.gov/online/aeviewer/ME/40/65d544dc-79b0-437c-a7f8-757ffec624af.shtml (last visited April 6, 2023).

their duties and obligations, the Data Breach occurred, and Plaintiff's and Class members' PII was accessed and disclosed by an unauthorized actor. This action seeks to remedy these failings and their consequences. Plaintiff brings this action on behalf of herself and all similarly situated individuals whose PII was exposed as a result of the Data Breach, which Defendants learned of on or about February 1, 2023, but did not publicly disclose until on or after March 24, 2023.

10. Plaintiff, on behalf of herself and all other Class members, asserts claims for negligence, negligence per se, breach of fiduciary duty, unjust enrichment, breach of implied contract, declaratory relief, and violation of the New York General Business Law § 349, and seeks declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

Plaintiff Kylie Meyer

11. Plaintiff Kylie Meyer is an adult resident and citizen of the State of New York who resides in Rhinebeck, New York.

12. In or about April 2019, Plaintiff opened a credit card account with Defendant BOA.

13. In or about November 2021, Plaintiff closed her credit card account with BOA.

14. In or about December 2022, Plaintiff opened a checking account with Citizens Bank ("Citizens Account").

15. On or about April 5, 2023, Plaintiff received a letter in the mail from Defendant NCB—dated March 24, 2023—stating that her PII was compromised in the Data Breach.

16. In the letter, Defendant NCB stated that Plaintiff's PII compromised in the Data Breach "may have included details about a credit card account that you formerly had with Bank of America," including her "first and last name, address, phone number, email address, date of birth, employment position, pay amount, driver's license number, Social Security number, account

number, credit card number, routing number, account balance, and/or account status."

17. In the letter, Defendant NCB stated further that "an unauthorized party gained access to NCB's systems on February 1, 2023." Only nine short days thereafter, Plaintiff discovered a fraudulent transaction on her Citizens Account in the amount of $10 (on or about February 13, 2023). Upon information and belief, Plaintiff believes that this fraudulent transaction was conducted using her PII obtained through the Data Breach.

18. As a direct and proximate result of Defendants' failure to safeguard her PII and otherwise prevent the Data Breach, Plaintiff has spent approximately an hour detecting the fraudulent transaction on her Citizens Account, contacting Citizens to dispute it, filing a dispute with Citizens, and then subsequent to receiving the letter notifying her of the Data Breach, monitoring her accounts for further fraudulent activity. Plaintiff will continue to expend further time doing monitoring her accounts for fraudulent activity in the days, weeks, and months following the filing of this complaint.

19. As a direct and proximate result of Defendants' failure to safeguard her PII and otherwise prevent the Data Breach, Plaintiff suffered actual damages including, without limitation, time and expenses related to monitoring her financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, the lost value of her personal information, and other economic and non-economic harm. Plaintiff and Class members will now be forced to expend additional time to review their credit reports and monitor their financial accounts and medical records for fraud or identify theft – particularly since the compromised information may include Social Security numbers.

Defendants

20. Defendant NCB Management Services is a provider of Accounts Receivable

Management and Call Center Management solutions, as well as a national debt buyer, with its principal place of business and headquarters at 1 Allied Drive, Trevose, Pennsylvania 19053.[7]

21. Defendant Bank of America Corporation is an American multinational investment bank and financial services holding company, with its principal place of business and headquarters located at 100 North Tryon Street, Charlotte, North Carolina 28255.[8]

JURISDICTION AND VENUE

22. This Court has subject matter jurisdiction over this controversy pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, because at least one member of the Class is a citizen of a different state than Defendants, there are more than 100 Members of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interests and costs. Plaintiff is a resident of the State of New York, Defendant NCB is a resident of the Commonwealth of Pennsylvania by virtue of maintaining its headquarters in Trevose, Pennsylvania, and Defendant BOA is a resident of the State of North Carolina by virtue of maintaining its headquarters in Charlotte, North Carolina.

23. This Court has personal jurisdiction over NCB because NCB maintains its principal place of business in Pennsylvania and conducts substantial business in Pennsylvania and in this district through its principal place of business, engaged in the conduct at issue herein from and within this District, and otherwise has substantial contacts with this District and purposely availed itself of the Courts in this District.

24. This Court has personal jurisdiction over BOA because it is authorized to and does conduct substantial business in this District, engaged in the conduct at issue herein and giving rise to Plaintiff's claims from and within this District, and otherwise has substantial contacts with this

[7] https://www.ncbi.com/ (last visited April 6, 2023).
[8] https://about.bankofamerica.com/en (last visited April 6, 2023).

District—including but not limited to, by maintaining and operating approximately 50 retail banking locations and hundreds of ATM machines in this judicial district—and purposely availed itself of the Courts in this District.

25. Venue is proper under 28 U.S.C. §§ 1391(b)(1) and (2) because NCB resides in this district, and this district is where a substantial part of the acts, omissions, and events giving rise to Plaintiff's claims occurred. Further, venue is proper for BOA because this district is where a substantial part of the acts, omissions, and events giving rise to Plaintiff's claims occurred.

FACTUAL ALLEGATIONS

26. Plaintiff and the proposed Class members are individuals who previously maintained accounts with BOA, whose PII BOA subsequently sold and transferred to NCB. Thus, Plaintiff and all Class members are consumers of both Defendants and entrusted their highly sensitive PII to both Defendants.

27. Prior to transferring Plaintiff's and Class members' sensitive PII to NCB, BOA failed to assess and ensure that NCB had ample protections in place to safely and securely store, maintain, use, or otherwise possess Plaintiff's and Class members' sensitive PII. Instead, BOA negligently sold and transferred Plaintiff's and Class members' sensitive PII to NCB.

28. Likewise, at all times relevant hereto, NCB failed to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard against unauthorized access and disclosure of the sensitive PII Plaintiff and Class members entrusted to it.

29. Thus, Plaintiff brings this class action against Defendants for both of their failures to properly secure and safeguard PII, for failing to comply with industry standards to protect and safeguard PII, and for failing to provide timely, accurate, and adequate notice to Plaintiff and other Class members that such PII had been compromised in the Data Breach.

A. Both Defendants Advertise and Market Their Services to Consumers as Being Secure and Safe

30. BOA's website has numerous advertisement statements assuring its customers that its services are safe and secure. For instance, BOA's website tells consumers: "your security is our top priority."[9]

31. Likewise, the first line of BOA's Privacy Notice states: "Your privacy is important to us."[10] BOA further assures consumers such as Plaintiff and Class members that BOA "abide by rigorous privacy standards to ensure personal information we collect, use and share is protected."[11]

32. BOA assures consumers that it will timely notify them of a data breach in the event one occurs: "In the event of a data breach, we provide timely notification."[12]

33. Not only does BOA assure consumers that its own services are safe, but it also advertises on its website that it takes steps to ensure that third-party companies with which BOA works to provide its services are also protecting consumers' information: "Bank of America works with third-party providers who are contractually obligated to comply with our policies to protect information."[13]

34. Thus, BOA's website stresses that it ensures consumers' personal information is safe and secure, even when that information is accessed or provided to third-party companies such as NCB:

> Protecting your personal information
> To protect personal information from unauthorized access and use, we use security measures that comply with applicable federal and state laws. These measures may include device safeguards and secured files and buildings **as well as oversight of our third-party providers to ensure personal information remains confidential**

[9] https://www.bankofamerica.com/security-center/overview/ (last visited April 6, 2023).
[10] https://www.bankofamerica.com/security-center/online-privacy-notice/ (last visited April 6, 2023).
[11] *Id*.
[12] *Id*.
[13] *Id*.

> **and secure** …. Third-party providers are contractually obligated to comply with our policies to protect information we share with them or they collect on our behalf.[14]

One such third-party with which BOA shares consumers' PII is NCB. Thus, BOA's website comments above apply to its relationship with NCB and tell consumers that BOA takes steps to ensure NCB protects information BOA shares with it, such as Plaintiff's and Class members' PII.

35. NCB describes itself as "a twenty-five-year-old provider of Accounts Receivable Management (ARM) and Call Center Management (CCM) solutions, as well as a respected national debt buyer" that is "an industry leader since 1994 in providing clients with a full-spectrum of Accounts Receivable Management (ARM) Solutions."[15]

36. NCB advertises that it provides the foregoing services to its clients—such as BOA—using "the latest in new information systems and communication technology."[16]

37. Like BOA, NCB advertises that consumers' PII in its possession is safe because NCB utilizes "leading-edge data security" backed by "flexible proprietary technology."[17] Furthermore, NCB's website tells consumers that when it collects data from its business customers—as it did from BOA—its collection practices are safe and secure because NCB conducts such data transfers "using a fully automated, state of the art collection system, the latest technology advancements, apply[ing] the highest in security standards and employ[ing] a well-trained, highly effective staff."[18]

38. Based on the foregoing advertisements and website representations made by both Defendants—stressing data privacy and security measures both Defendants were purportedly

---

[14] *Id*.
[15] https://www.ncbi.com/Clients (last visited April 6, 2023).
[16] https://www.ncbi.com/About (last visited April 6, 2023).
[17] https://www.ncbi.com/Clients (last visited April 6, 2023).
[18] https://www.ncbi.com/Financial (last visited April 6, 2023).

taking to ensure consumers' PII was safe and protected—Plaintiff and Class members had the impression that Defendants had adequate measures to safeguard their sensitive PII and Plaintiff and Class members entrusted their PII to both Defendants based on those representations.

B. The Data Breach

39. Contrary to the foregoing representations, however, both Defendants lacked adequate practices, policies, procedures, security, and other safeguards to ensure Plaintiff's and Class members' PII was protected from cybersecurity threats.

40. As admitted in NCB's Notice, "an unauthorized party gained access to NCB's systems" on February 1, 2023 that NCB purportedly discovered on February 4, 2023.[19] NCB's Notice states further that it consulted with "federal law enforcement authorities" to assist its investigation of the Data Breach, but notably omitted from its Notice any change to its data security or retention policies.

41. Contrary to BOA's website statement assuring consumers that it would timely notify them of any data breach it—or any third-parties with which it shares consumers' PII—suffers, both Defendants waited nearly two months after learning of the Data Breach before notifying impacted individuals of its occurrence.

42. Based on their own statements assuring consumers that their data was secure, as well as industry best practices for data security, Defendants owed a duty to Plaintiff and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII against unauthorized access and disclosure. Defendants breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect its consumers' PII from unauthorized access and disclosure.

[19] https://apps.web.maine.gov/online/aeviewer/ME/40/65d544dc-79b0-437c-a7f8-757ffec624af.shtml (last visited April 6, 2023).

C. Defendants Knew that Criminals Target PII

43. At all relevant times, Defendants knew, or should have known, its customers' Plaintiff's, and all other Class members' PII was a target for malicious actors. Despite such knowledge, Defendants failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class members' PII from cyber-attacks that Defendants should have anticipated and guarded against.

44. PII is a valuable property right.[20] The value of PII as a commodity is measurable.[21] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[22] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[23] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

45. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, SSNs, PII and other sensitive information directly on various Internet websites making the information publicly available. This

---

[20] *See* Marc van Lieshout, *The Value of Personal Data*, 457 International Federation for Information Processing 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible…"), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data

[21] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE.COM (April 28, 2014), http://www.medscape.com/viewarticle/824192.

[22] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD ILIBRARY (April 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[23] IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

46. Consumers place a high value on the privacy of their PII. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[24]

47. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

D. Theft of PII Has Grave and Lasting Consequences for Victims

48. Theft of PII is serious. The FTC warns consumers that identity thieves use PII to exhaust financial accounts, start new utility accounts, and incur charges and credit in a person's name.[25]

49. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[26] According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is

---

[24] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior*, *An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

[25] *See* Federal Trade Commission, *What to Know About Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Nov. 15, 2021).

[26] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number. *Id*.

valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[27]

50. With access to an individual's PII, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and SSN to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[28]

51. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[29]

52. Theft of SSNs also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of her SSN, and a new SSN will not be provided until

---

[27] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN (Sept. 1, 2017), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[28] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, IDENTITYTHEFT.GOV https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last accessed Nov. 15, 2021).

[29] Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RESOURCE CENTER (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/ (last accessed Nov. 15, 2021).

after the harm has already been suffered by the victim.

53. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[30]

54. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used and it takes some individuals up to three years to learn that information.[31]

55. It is within this harsh and dangerous reality that Plaintiff and all other Class members must now live with the knowledge that their PII is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

E. Damages Sustained by Plaintiff and the Other Class Members

56. As a direct and proximate result of Defendants' failures, Plaintiff and Class members are at substantial risk of suffering identity theft and fraud or misuse of their PII.

57. Plaintiff and the Class suffered actual injury from having PII compromised as a result of Defendants' negligent data management and resulting Data Breach including, but not limited to (a) damage to and diminution in the value of their PII, a form of property that Defendants

[30] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (August 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.
[31] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 Journal of Systemics, Cybernetics and Informatics 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

obtained from Plaintiff; (b) violation of their privacy rights; and (c) present and increased risk arising from the identity theft and fraud.

58. For the reasons mentioned above, Defendants' conduct, which directly and proximately caused the Data Breach, caused Plaintiff and members of the Class these significant injuries and harm.

59. Plaintiff brings this class action against Defendants for their failure to: (1) properly secure and safeguard PII; (2) ensure that proper security measures were in place to protect PII; and (3) provide timely, accurate, and adequate notice to Plaintiff and other class members that their PII had been compromised.

60. Plaintiff, individually and on behalf of all other similarly situated individuals impacted by the Data Breach, alleges claims for negligence, negligence per se, breach of fiduciary duty, unjust enrichment, breach of implied contract, declaratory relief, and violation of the New York General Business Law § 349.

CLASS ALLEGATIONS

61. Plaintiff brings this action on behalf of himself and the following classes:

> Nationwide Class: All residents of the United States who were notified by Defendants that their PII may have been compromised as a result of the Data Breach.
>
> New York Subclass: All residents of New York who were notified by Defendants that their PII may have been compromised as a result of the Data Breach.

The foregoing classes are referred to herein, collectively, as the "Class."

62. Excluded from the Class are: (1) the Judges presiding over the Action, Class Counsel, and members of their families; (2) the Defendant, its subsidiaries, parent companies, successors, predecessors, and any entity in which Defendants or their parents, have a controlling interest, and their current or former officers and directors; (3) Persons who properly opt out; and

(4) the successors or assigns of any such excluded Persons.

63. **Numerosity**: Members of the class are so numerous that their individual joinder is impracticable, as the proposed class includes at least 494,969 members who are geographically dispersed.

64. **Typicality**: Plaintiff's claims are typical of class members' claims. Plaintiff and all class members were injured through Defendants' uniform misconduct, and Plaintiff's claims are identical to the claims of the class members she seeks to represent because she, like all Class members, received Defendants' Notice informing them that their PII was compromised in the Data Breach. Accordingly, Plaintiff's claims are typical of class members' claims.

65. **Adequacy**: Plaintiff's interests are aligned with the class she seeks to represent and Plaintiff has retained counsel with significant experience prosecuting complex class action cases, including cases involving alleged privacy and data security violations. Plaintiff and her counsel intend to prosecute this action vigorously. The class's interests are well-represented by Plaintiff and undersigned counsel.

66. **Superiority**: A class action is the superior—and only realistic—mechanism to fairly and efficiently adjudicate Plaintiff's and other class member's claims. The injury suffered by each individual class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for class members individually to effectively redress Defendants' wrongdoing. Even if class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer

management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

67. **Commonality and Predominance:** The following questions common to all class members predominate over any potential questions affecting individual class members:

a. Whether Defendants had duties to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and Class members' PII from unauthorized access and disclosure;

b. Whether Defendants failed to exercise reasonable care to secure and safeguard Plaintiff's and Class members' PII;

c. Whether Defendants breached their duties to protect Plaintiff's and Class members' PII; and

d. Whether Plaintiff and all other members of the Class are entitled to damages and the measure of such damages and relief.

68. Given that Defendants engaged in a common course of conduct as to Plaintiff and the Class, similar or identical injuries and common law and statutory violations are involved, and common questions outweigh any potential individual questions.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the New York Subclass)

69. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

70. Defendants owed a duty to Plaintiff and all other Class members to exercise reasonable care in safeguarding and protecting their PII in their possession, custody, or control.

71. Defendants knew the risks of collecting and storing Plaintiff's and all other Class members' PII and the importance of maintaining secure systems.

72. Given the nature of Defendants' business, the sensitivity and value of the PII they maintain, and the resources at their disposal, Defendants should have identified the vulnerabilities to their systems and prevented the Data Breach from occurring.

73. Defendants breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII entrusted to them—including Plaintiff's and Class members' PII.

74. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class members' PII to unauthorized individuals.

75. But for Defendants' negligent conduct or breach of the above-described duties owed to Plaintiff and Class members, their PII would not have been compromised.

76. As a result of Defendants' above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and all other Class members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii)

improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; and/or (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

COUNT II
NEGLIGENCE PER SE
(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the New York Subclass)

77. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

78. BOA's duties arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as BOA, of failing to employ reasonable measures to protect and secure PII.

79. BOA violated Section 5 of the FTCA by failing to use reasonable measures in choosing a vendor to sell Plaintiff and all other Class members' debts to without ensuring that NCB had adequate security safeguards in place to prevent and protect against a data breach, which included their PII, and not complying with applicable industry standards. BOA's conduct was particularly unreasonable given the nature and amount of PII it sold, and the foreseeable consequences of a data breach involving PII including, specifically, the substantial damages that would result to Plaintiff and other Class members.

80. BOA's violations of Section 5 of the FTCA constitutes negligence *per se*.

81. NCB's duties arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as NCB, of failing to employ reasonable

measures to protect and secure PII.

82. NCB violated Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and all other Class members' PII and not complying with applicable industry standards. NCB's conduct was particularly unreasonable given the nature and amount of PII it obtains and stores, and the foreseeable consequences of a data breach involving PII including, specifically, the substantial damages that would result to Plaintiff and the other Class members.

83. NCB's violations of Section 5 of the FTCA constitutes negligence per se.

84. Plaintiff and Class members are within the class of persons that Section 5 of the FTCA was intended to protect.

85. The harm occurring as a result of the Data Breach is the type of harm Section 5 of the FTCA was intended to guard against.

86. It was reasonably foreseeable to Defendants that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class members' PII to unauthorized individuals.

87. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of Defendants' violations of Section 5 of the FTCA. Plaintiff and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of

the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vi) actual or attempted fraud.

COUNT III
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the New York Subclass)

88. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

89. Plaintiff and Class members either directly or indirectly gave Defendants their PII in confidence, believing that both Defendants would protect that information, based on the substantial number of statements on both Defendants' websites promising to do so.

90. Plaintiff and Class members would not have provided Defendants with their sensitive PII had they known it would not be adequately protected.

91. Defendants' acceptance and storage of Plaintiff's and Class members' PII created a fiduciary relationship between Defendants and Plaintiff and Class members. In light of this relationship, Defendants were obligated to act primarily for the benefit of consumers who entrusted their sensitive PII to them, which includes safeguarding and protecting Plaintiff's and Class members' PII.

92. Defendants have a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of their relationship. Defendants breached that duty by failing to properly protect the integrity of the system containing Plaintiff's and Class members' PII, failing to comply with the data security guidelines set forth by Section 5 of the FTCA, and otherwise failing to safeguard the PII of Plaintiff and Class members it collected.

93. As a direct and proximate result of Defendants' breaches of its fiduciary duties, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII compromised as a result of the Data Breach; and (vii) actual or attempted fraud.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the New York Subclass)

94. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

95. Plaintiff and Class members have both a legal and equitable interest in their PII that was collected, stored, and maintained by Defendants—thus conferring a benefit upon Defendants—that was ultimately compromised by the Data Breach.

96. Defendants accepted or had knowledge of the benefits conferred upon them by Plaintiff and Class members. Defendants also benefitted from the receipt of Plaintiff's and Class members' PII.

97. As a result of Defendants' failure to safeguard and protect Plaintiff's PII, conduct, Plaintiff and Class members suffered actual damages.

98. Defendants should not be permitted to retain the benefit belonging to Plaintiff and Class members because Defendants failed to adequately implement the data privacy and security

procedures for itself that were mandated by federal, state, and local laws and industry standards.

99. Defendants should be compelled to provide for the benefit of Plaintiff and Class members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

COUNT V
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the New York Subclass)

100. Plaintiff realleges and incorporates by reference all allegations of the preceding factual allegations as though fully set forth herein.

101. Defendants required Plaintiff and Class members to provide, or authorize the transfer of, their PII in order for Defendants to provide services. In exchange, Defendants entered into implied contracts with Plaintiff and Class members in which Defendants agreed to comply with its statutory and common law duties to protect Plaintiff's and Class members' PII and to timely notify them in the event of a data breach.

102. Plaintiff and Class members would not have provided their PII to Defendants had they known that Defendants would not safeguard their PII, as promised, or provide timely notice of a data breach.

103. Plaintiff and Class members fully performed their obligations under their implied contracts with Defendants.

104. Defendants breached the implied contracts by failing to safeguard Plaintiff's and Class members' PII and by failing to provide them with timely and accurate notice of the Data Breach.

105. The losses and damages Plaintiff and Class members sustained (as described above) were the direct and proximate result of Defendants' breach of its implied contracts with Plaintiff and Class members.

COUNT VI
DECLARATORY RELIEF
(28 U.S.C. § 2201)
(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the New York Subclass)

106. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

107. An actual controversy has arisen and exists between Plaintiff and members of the Class, on the one hand, and Defendants, on the other hand, concerning the Data Breach and Defendants' failure to protect Plaintiff's and class members' PII, including with respect to the issue of whether Defendants took adequate measures to protect that information. Plaintiff and Class members are entitled to judicial determination as to whether Defendants have performed and are adhering to all data privacy obligations as required by law or otherwise to protect Plaintiff's and class members PII from unauthorized access, disclosure, and use.

108. A judicial determination of the rights and responsibilities of the parties regarding Defendants' privacy policies and whether they failed to adequately protect PII is necessary and appropriate to determine with certainty the rights of Plaintiff and the Class members, and so that there is clarity between the parties as to Defendants' data security obligations with respect to PII going forward, in view of the ongoing relationships between the parties.

COUNT VII
VIOLATION OF THE NEW YORK GENERAL BUSINESS LAW
N.Y. Gen. Bus. Law §§ 349, *et seq*.
(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the New York Subclass)

109. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

110. Defendants engaged in deceptive acts or practices in the conduct of their business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff, Class members, and New York Subclass members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff, Class members, and New York Subclass members' PII, including duties imposed by the FTC Act, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff, Class members, and New York Subclass members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff, Class members, and New York Subclass members' PII, including duties imposed by the FTC Act;

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff, Class members, and New York Subclass members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff, Class members, and New York Subclass members' PII, including duties imposed by the FTC Act.

111. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

112. Defendants acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregarded Plaintiff, Class members, and New York Subclass members' rights. Data breaches within Defendants' business industries put them on notice that their security and privacy protections were inadequate.

113. As a direct and proximate result of Defendants' deceptive and unlawful acts and practices, Plaintiff, Class members, and New York Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants as they would not have paid for their services or would have paid less for them but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity

protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

114. Defendants' deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the myriad New Yorkers affected by the Data Breach.

115. The above deceptive and unlawful practices and acts by Defendants caused substantial injury to Plaintiff, Class members, and New York Subclass members that they could not reasonably avoid.

116. Plaintiff, Class members, and New York Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages, restitution, injunctive relief, and attorney's fees and costs.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of the class members, by and through undersigned counsel, respectfully request that the Court grant the following relief:

A. Certify this case as a class action pursuant to Fed. R. Civ. P. 23, and appoint Plaintiff as class representative and undersigned counsel as class counsel;

B. Award Plaintiff and class members actual and statutory damages, punitive damages, and monetary damages to the maximum extent allowable;

C. Award declaratory and injunctive relief as permitted by law or equity to assure that class members have an effective remedy, including enjoining Defendants from continuing the unlawful practices as set forth above;

D. Award Plaintiff and class members pre-judgment and post-judgment interest to the

maximum extent allowable;

E. Award Plaintiff and class members reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Award Plaintiff and Class members such other favorable relief as allowable under law or at equity.

JURY TRIAL DEMANDED

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

Dated: April 6, 2023

Respectfully submitted,

By: */s/ Mark B. DeSanto*

Joseph B. Kenney (316557)
Mark B. DeSanto (320310)
SAUDER SCHELKOPF LLC
1109 Lancaster Avenue
Berwyn, PA 19312
Telephone: (888) 711-9975
Facsimile: (610) 421-1326
jbk@sstriallawyers.com
mbd@sstriallawyers.com

Attorneys for Plaintiff