IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

In re: NCB Management Services, Inc. Data Breach Litigation	Case No. 23-1236-KNS **This Document Applies To:** **ALL ACTIONS** **CLASS ACTION** **JURY TRIAL DEMANDED**

PLAINTIFFS AMENDED CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Joseph Lindquist, Lillian Mardikian, Howard Suh, Ernesto Medina, Benedict Lozada, Edward Del Hierro, Tobi Patterson, Jude-Law Palmer, Kevin Bliss, Michael Teixeira, Diane Ross, Jacqueline O'Brien, Kelly Matts, Micael Martin, Bryan Woodlow and Christine Neubauer (collectively, "Plaintiffs"), individually and on behalf of all others similarly situated, assert the following against Defendant NCB Management Services, Inc. ("NCB") ("Defendant"), based upon personal knowledge, where applicable, information and belief, and the investigation of counsel.

INTRODUCTION

1. NCB is a national debt collection and accounts receivable management company based in Trevose, Pennsylvania. It provides account services to companies, such as Bank of America ("BOA") and Pathward, among other financial institutions and lenders.

2. During the course of its operations, the Defendant acquired, collected, stored, utilized, and derived a benefit from Plaintiffs' and Class Members' first and last names, addresses, phone numbers, email addresses, dates of birth, employment positions, pay amounts, driver's license numbers, Social Security numbers, account numbers, credit card numbers, routing

numbers, account balances, and/or account statuses (collectively the "Personally Identifiable Information" or "PII").

3. Defendant, therefore, owed and otherwise assumed non-delegable statutory, regulatory, contractual, and common law duties and obligations, including to keep Plaintiffs' and Class Members' PII confidential, safe, secure, and protected from the type of unauthorized access, disclosure, and theft that occurred in this matter.

4. Defendant's data security obligations and risks of storing sensitive PII in a vulnerable state, were upon information and belief known and recognized by Defendant given the public and financial industry awareness in high frequency of targeted data breaches. Indeed, during the course if its business operations, Defendant expressly and impliedly promised to safeguard Plaintiffs' and Class Members' PII.

5. Furthermore, Plaintiffs and Class Members each provided their PII to Defendant with a reasonable expectation of privacy that Defendant would comply with their respective duties, obligations, and representations, and that their PII would be adequately safeguarded and protected against unauthorized access, disclosure and exfiltration.

6. Despite notice of the risk of a data breach, Defendant breached its duties to Plaintiffs and Class Members as described in detail herein.

7. On February 4, 2023, NCB discovered that an unauthorized third party gained access to its systems on February 1, 2023, that stored Plaintiffs' and Class Members' highly sensitive information (the "Data Breach"). NCB first publicly announced the Data Breach on or around March 24, 2023.[1]

[1] According to NCB, "confidential client account information maintained by NCB was accessed by an unauthorized party." At the time, NCB indicated that the Data Breach impacted 494,969 people. *See* Office of the Maine Attorney General, Data Breach Notifications, NCB Management Services, Inc., Mar. 24, 2023, *available at*

8. However, the Data Breach was much larger than NCB initially disclosed and was in fact a part of a companywide ransomware attack affecting NCB's systems and servers. On or around May 23, 2023, NCB issued an additional public announcement that the number of people affected by the Data Breach was approximately 1,087,842 – more than double the initial estimate.[2] NCB followed up with additional public announcements. However, the full extent of the Data Breach is not yet known.

9. Given the type of business in which Defendant operated and the types of PII routinely acquired and stored, the Data Breach was significantly impactful and dangerous to the impacted consumers.

10. Indeed, several Plaintiffs have already experienced identity theft or fraud that, likely, is likely attributable to the Data Breach.

11. Currently, the full extent of the types of sensitive PII, the scope of the Data Breach, and the root cause of the Data Breach are all within the exclusive control of Defendant and its agents, counsel, and forensic security vendors at this phase of litigation.

12. Upon information and belief, Defendant is responsible for allowing this Data Breach because of multiple acts of negligence, including but not limited to: (i) their failure to design, implement, and maintain reasonable data security systems and safeguards; (ii) and/or failure to exercise reasonable care in the hiring, supervision, training, and monitoring of its employees and agents and vendors; (iii) and/or failure to comply with industry-standard data security practices; (iv) and/or failure to comply with federal and state laws and regulations that

https://apps.web.maine.gov/online/aeviewer/ME/40/65d544dc-79b0-437c-a7f8-757ffec624af.shtml (last visited July 20, 2023).

[2] *See* Office of the Maine Attorney General, Data Breach Notifications, NCB Management Services, Inc., May 19, 2023, *available at* https://apps.web.maine.gov/online/aeviewer/ME/40/fcafcce5-ef56-4784-a86a-820c6b1aa127.shtml (last visited July 20, 2023).

govern data security and privacy practices and are intended to protect the type of PII at issue in this action; (v) and/or failure to design, implement and execute reasonable data retention and destruction policies.

13. Upon information and belief, despite its role in managing so much sensitive PII, NCB failed to take basic security measures such as adequately encrypting its data or following industry security standards to destroy PII that was no longer necessary for the intended business purpose.

14. Moreover, NCB failed to recognize and detect that unauthorized third parties had accessed its network in a timely manner to mitigate the harm. NCB further failed to recognize that substantial amounts of data had been compromised, and more likely than not, had been exfiltrated and stolen. Had NCB not committed the acts of negligence described herein, it would have discovered the Data Breach sooner – and/or prevented the invasion and theft altogether.

15. Upon information and belief, based on the type of sophisticated and malicious criminal activity, the type of PII targeted, NCB's admission that the PII was accessed, NCB's admission that Plaintiffs' and Class Member's PII was in the files that were accessed, and reports of criminal misuse of Plaintiffs' and Class Members' PII, Plaintiffs' and Class Members' PII was likely accessed, disclosed, exfiltrated, stolen, disseminated, and used by a criminal third party.

16. Moreover, as a result of the Data Breach, given the criminal targeting of the PII, the sensitivity of the information, the likelihood of exfiltration, and reports of actual fraud following the Data Breach, Plaintiffs and Class Members are now experiencing a current, imminent, and ongoing risk of fraud and identity theft. The risk of identity theft is not speculative or hypothetical but is impending and has materialized.

17. Plaintiffs have suffered several categories of related and actual harm: (i) invasion of privacy, (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud and/or unauthorized use of their PII, (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, (iv) lost or diminished value of PII, (v) loss of benefit of the bargain, (vi) future costs of ongoing credit and identity theft monitoring, (vii) statutory damages, (viii), nominal damages, (ix) and the ongoing future risk of harm as long as Defendant maintains Plaintiffs and Class Members PII with inadequate security practices.

18. Plaintiffs and Class Members would not have provided their PII, engaged in a consumer relationship, or paid any banking, debt collection, servicing, transactional or other fees for Defendant's services, had they known their information would be maintained using inadequate data security and retention systems.

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

20. Plaintiffs, on behalf of themselves, and all others similarly situated, bring claims for negligence, negligence *per se*, breach of implied contract, unjust enrichment, violations of state consumer protection and data privacy statutes, the Driver's Privacy Protection Act ("DPPA"), declaratory and injunctive relief, and breach of contract to which Plaintiffs and Class Members were intended third party beneficiaries.

21. Plaintiffs seek actual, compensatory, consequential, incidental, punitive, nominal and statutory damages, in an amount to be proven at trial. Plaintiff also seek future compensatory damage to provide adequate credit and identity theft monitoring. And Plaintiffs seek declaratory

and injunctive relief related to the ongoing and future risk of identity theft requiring Defendant to adopt reasonably sufficient practices to safeguard the PII that remains in Defendant's custody and control in order to prevent incidents like the Data Breach from reoccurring in the future.

JURISDICTION AND VENUE

22. The Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 as it arises under the laws of the United States, including the Driver's Privacy Protection Act, 18 U.S.C. §§ 2721, *et seq.*

23. This Court also has jurisdiction over the subject matter of this action pursuant to 28 U.S.C § 1332(d), because the amount in controversy for the Class exceeds $5,000,000, exclusive of interest and costs, there are more than 100 putative Members of the Class defined below, and a significant portion of putative Class Members are citizens of a different state than Defendant.

24. The Court also has supplemental jurisdiction over Plaintiffs' state law claims pursuant to 28 U.S.C. § 1367(a) because they are related to claims in the action within such original jurisdiction, and they form part of the same case or controversy under Article III of the United States Constitution.

25. This Court has general personal jurisdiction over Defendant because NCB is incorporated in the Commonwealth of Pennsylvania and maintains its principal place of business in this District.

26. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District. Trevose, Pennsylvania is the principal place of business operations for NCB where policies and decisions were made related to the data security systems and management at issue in this matter.

PARTIES

I. Plaintiffs

Plaintiff Joseph Lindquist

27. Plaintiff Joseph Lindquist ("Plaintiff Lindquist") is a citizen and resident of the State of Florida. Plaintiff Lindquist was a customer of BOA prior to the Data Breach.

Plaintiff Lillian Mardikian

28. Plaintiff Lillian Mardikian ("Plaintiff Mardikian") is a citizen and resident of the State of California. Plaintiff Mardikian was a customer of BOA prior to the Data Breach.

Plaintiff Howard Suh

29. Plaintiff Howard Suh ("Plaintiff Suh") is a citizen and resident of the State of California. Plaintiff Suh was a customer of BOA prior to the Data Breach.

Plaintiff Ernesto Medina

30. Plaintiff Ernesto Medina ("Plaintiff Medina") is a citizen and resident of the State of California. Plaintiff Medina was a customer of BOA prior to the Data Breach.

Plaintiff Benedict Lozada

31. Plaintiff Benedict Lozada ("Plaintiff Lozada") is a citizen and resident of the State of California. Plaintiff Lozada received the May 22, 2023 Data Breach Notification Letter which purports to be for Pathward.

Plaintiff Edward Del Hierro

32. Plaintiff Edward Del Hierro ("Plaintiff Del Hierro") is a citizen and resident of the State of California. Plaintiff Del Hierro received the May 23, 2023 Data Breach Notification Letter which purports to be for Pathward.

Plaintiff Tobi Patterson

33. Plaintiff Tobi Patterson ("Plaintiff Patterson") is a citizen and resident of the State of Texas. Plaintiff Patterson was a customer of BOA prior to the Data Breach.

Plaintiff Jude-Law Palmer

34. Plaintiff Jude-Law Palmer ("Plaintiff Palmer") is a citizen and resident of the State of Georgia. Plaintiff Palmer was a customer of BOA prior to the Data Breach.

Plaintiff Kevin Bliss

35. Plaintiff Kevin Bliss ("Plaintiff Bliss") is a citizen and resident of the Commonwealth of Massachusetts. Plaintiff Bliss was a customer of BOA prior to the Data Breach.

Plaintiff Michael Teixeira

36. Plaintiff Michael Teixeira ("Plaintiff Teixeira") is a citizen and resident of the Commonwealth of Massachusetts. Plaintiff Teixeira was a customer of BOA prior to the Data Breach.

Plaintiff Diane Ross

37. Plaintiff Diane Ross ("Plaintiff Ross") is a citizen and resident of the State of California. Plaintiff Ross received the May 23, 2023 Data Breach Notification Letter which purports to be for Pathward.

Plaintiff Jacqueline O'Brien

38. Plaintiff Jacqueline O'Brien ("Plaintiff O'Brien") is a citizen and resident of the State of California. Plaintiff O'Brien received the May 23, 2023 Data Breach Notification Letter which purports to be for Pathward.

Plaintiff Kelly Matts

39. Plaintiff Kelly Matts ("Plaintiff Matts") is a citizen and resident of the State of California. Plaintiff Matts received the May 23, 2023 Data Breach Notification Letter which purports to be for Pathward.

Plaintiff Micael Martin

40. Plaintiff Micael Martin ("Plaintiff Martin") is a citizen and resident of the State of California. Plaintiff Martin received the May 23, 2023 Data Breach Notification Letter which purports to be for Pathward.

Plaintiff Bryan Woodlow

41. Plaintiff Bryan Woodlow ("Plaintiff Woodlow") is a citizen and resident of the State of Illinois. Plaintiff Woodlow was a customer of Bank of America prior to the Data Breach and has been a customer since approximately 2021.

Plaintiff Christine Neubauer

42. Plaintiff Christine Neubauer ("Plaintiff Neubauer") is a citizen and resident of the State of Florida. Plaintiff Neubauer was a previous customer of Bank of America prior to the Data Breach, and had not had an account with Bank of America for more than a decade prior to the data breach and, to the best of her knowledge, has never had any account with Bank of America sent to collections. Plaintiff believes her SPI to have been sent to Defendant in error by Bank of America.

II. Defendant

43. Defendant NCB is a domestic Pennsylvania corporation with its headquarters and principal place of business located at 1 Allied Drive, Trevose, Pennsylvania.

44. Founded in 1994, Defendant NCB is a national debt buyer, debt collector, and provider of Accounts Receivable Management ("ARM") and Call Center Management ("CCM") solutions for financial institutions and lenders, including BOA and Pathward.

ALLEGATIONS

I. The Data Breach

45. NCB has provided very little information about the full scope and causes of the Data Breach, which purports to be a *ransomware* cyber-attack on the company's network.

46. According to the U.S. Cybersecurity and Infrastructure Security Agency ("CISA"):

> Ransomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid. … Malicious actors continue to adjust their ransomware tactics over time, to include pressuring victims for payment by threatening to release stolen data if they refuse to pay, and publicly naming and shaming victims as secondary forms of extortion. ***Malicious actors engage in lateral movement to target critical data and propagate ransomware across entire networks.*** These actors also increasingly use tactics, such as deleting system backups, that make restoration and recovery more difficult or infeasible for impacted organizations.[3]

(emphasis added).

47. In a typical ransomware attack a hacker will deploy malware against a company's network that will encrypt a company's data and prevent access to the data until the ransom payment is paid and a decryption key is given, and the data is released. However, there is often no way to gauge the accuracy or truthfulness of any assurances that hackers might make, even if the ransom is paid. Ransomware attackers often use social engineering techniques, such as phishing, to gain access to a company's environment.

[3] CISA, *Ransomware 101*, *available at* https://www.cisa.gov/stopransomware/ransomware-101 (last visited July 20, 2023).

48. According to CISA, ransomware incidents "can severely impact business processes and leave organizations without the data they need to operate and deliver mission-critical services."[4]

49. The monetary value of ransom demands has increased, with some demands exceeding $1 million. Ransomware incidents have become more destructive and impactful in nature and scope. The economic and reputational impacts of ransomware incidents, throughout the initial disruption and, at times, extended recovery, have also proven challenging for organizations large and small."

50. On or around March 24, 2023, NCB publicly announced that confidential client account information maintained by NCB was accessed by an unauthorized party.

51. NCB via BOA began notifying only certain persons affected by the Data Breach via U.S. mail on or around March 24, 2023.[5]

52. According to the BOA Data Breach Notification Letter, NCB discovered on February 4, 2023, that an unauthorized party gained access to NCB's systems on February 1, 2023.[6] NCB confirmed on March 8, 2023, that client information previously connected with affected persons' BOA accounts were accessed by the unauthorized party.[7]

---

[4] *Id.*

[5] According to the Data Breach notification posting on the Maine Attorney General's website, it was BOA - *not* NCB - who notified the Maine Attorney General of NCB's Data Breach and sent the data breach notification letters to affected persons. The Maine Attorney General's website says the Data Breach notification was submitted to the state by "WilmerHale LLP" who is listed as "Outside counsel for Bank of America." However, the letter was signed by NCB. A sample letter to affected consumers of the NCB Data Breach is included on the Maine Attorney General's website. *See Data Breach Notifications*, Office of the Maine Att'y Gen., *available at* https://apps.web.maine.gov/online/aeviewer/ME/40/65d544dc-79b0-437c-a7f8-757ffec624af/d7667acf-0b40-44c3-a168-5efbdd973ca0/document.html (last visited July 20, 2023) (the "BOA Data Breach Notification Letter").

[6] *Id.*

[7] *Id.*

53. According to the BOA Data Breach Notification Letter, "[t]he unauthorized activity on NCB's systems has been stopped, and NCB has obtained *assurances* that the third party no longer has any of the information on its systems."[8] (emphasis added).

54. Based on NCB's own admission in the notice letter, NCB alludes to the fact that the Data Breach was the result of a ransomware type of cyber-attack, and that NCB at least communicated with the cyber criminals to receive those purported "assurances." It is unclear if NCB actually paid any ransom (and if so how much?) to the hackers and what "assurances" were given.

55. According to a recent March 21, 2023 article in *Bloomberg* entitled "Banks, Financial Industry Hit by Rising Ransomware Attacks," the Financial Services Information Sharing and Analysis Center's ("FS-ISAC") annual outlook on cyber threats in the financial services industry found that "ransomware remained the biggest concern," as the "increase in attacks was likely due to the proliferation of the ransomware-as-a-service model, in which hacking groups provide 'affiliates' with the malware and services necessary to carry out an attack, in exchange for a share of the criminal proceeds."[9] FS-ISAC cited "business email compromise" in which criminals send an email that appears to come from a known source making a legitimate request — as a major issue for the financial services sector, with members reporting a 300% increase from 2021 to 2022.[10]

56. According to UK security firm Sophos, cyber attackers on average have 11 days after breaching a target network before they're being detected and often when they are spotted it's

[8] *Id.*
[9] Andrew Martin, BLOOMBERG, *Banks, Financial Industry Buffeted by Rising Ransomware Attacks*, Mar. 21, 2023, *available at* https://www.bloomberglaw.com/bloomberglawnews/privacy-and-data-security/XAJON3U0000000?bna_news_filter=privacy-and-data-security#jcite (last visited July 20, 2023).
[10] *Id.*

because they've deployed ransomware. Sophos found that this was more than enough time for an attacker to get a thorough overview of what a target network looks like, where its weaknesses lie, and for ransomware attackers to wreck it.[11]

57. To put that timeframe into context, according to Sophos, "11 days potentially provide attackers with approximately 264 hours for malicious activity, such as lateral movement, reconnaissance, credential dumping, data exfiltration, and more. Considering that some of these activities can take just minutes or a few hours to implement, 11 days provide attackers with plenty of time to do damage."[12]

58. According to NCB's BOA Data Breach Notification Letter, the PII involved for BOA customers included first and last names, addresses, phone numbers, email addresses, dates of birth, employment positions, pay amounts, driver's license numbers, Social Security numbers, account numbers, credit card numbers, routing numbers, account balances, and/or account statuses.[13]

59. As noted above, the Data Breach was much larger and more extensive than what NCB initially disclosed on March 24, 2023. In the coming weeks, it was disclosed that in addition to BOA, three additional financial institutions (TDBank, Capital One, and Pathward) who were NCB clients, had their customers' PII accessed as part of the Data Breach.

60. To date, NCB has not revealed the full list of effected financial institutions who had their customers' PII accessed as part of the Data Breach. As described below, NCB has been particularly ambiguous with identifying those institutions to regulators and the public.

---

[11] *See* Liam Tung, ZDNET, *This is how long hackers will hide in your network before deploying ransomware or being spotted*, May 19, 2021, *available at* https://www.zdnet.com/article/this-is-how-long-hackers-will-spend-in-your-network-before-deploying-ransomware-or-being-spotted/ (last visited July 20, 2023).
[12] *Id.*
[13] *See* BOA Data Breach Notification Letter.

61. Supplemental notice letters went out by U.S. mail to additional affected individuals who were Pathward customers.

62. On May 22, 2023, NCB's outside counsel contacted the Maine Attorney General to notify the state that an additional NCB client, Pathward, had their customer information compromised as part of the Data Breach.[14] NCB's letter to the Maine Attorney General however only identified "[t]he NCB clients who have elected to be identified in this notification," which apparently was just Pathward.[15]

63. NCB was further ambiguous in identifying its "clients" when it stated that "NCB is providing notice on behalf of its business partners, including, *but not limited to*, [Pathward]."[16] (emphasis added). The Pathward Data Breach Notification Letter that was sent to affected individuals purportedly came from NCB as it was on NCB letterhead (unlike the BOA Letter) and signed by NCB.[17]

64. The Pathward Data Breach Notification Letter informed affected individuals that "confidential client account information maintained by NCB was accessed by an unauthorized party."[18] According to NCB's Pathward notice letter, the information accessed related to first and last name and Social Security numbers.[19] The Pathward Data Breach Notification Letter also stated that NCB only just "confirmed" on April 19, 2023, that customers' information was accessed, weeks after BOA customers were notified in March.[20]

---

[14] *See Data Breach Notifications*, Office of the Maine Att'y Gen., *available at* https://apps.web.maine.gov/online/aeviewer/ME/40/fcafcce5-ef56-4784-a86a-820c6b1aa127/36165108-5d54-4071-81cc-7ec0746e6a40/document.html (last visited July 20, 2023) (the "Pathward Data Breach Notification Letter").
[15] *Id.*
[16] *Id.*
[17] *Id.*
[18] *Id.*
[19] *Id.*
[20] *Id.*

II. Defendant Obtains, Collects, and Stores Plaintiffs' and Class Members' PII

65. In the ordinary course of doing business as a national debt collector and accounts receivable management company that provides account services to companies, such as BOA and Pathward, NCB regularly obtains, collects, and stores sensitive, personal, and private protected information, such as the PII involved here.

66. Financial institutions and lenders, such as BOA and Pathward, hired NCB to service, manage, and collect outstanding and overdue balances on their customer accounts. In turn they provide their customers' PII, including the PII of Plaintiffs and Class Members, to NCB.

67. NCB maintains, keeps, and exploits Plaintiffs' and Class Members' PII for NCB's own benefit, including long after individuals have paid off their accounts in full. Upon information and belief, NCB keeps and stores this legacy information on its systems in an unsecure manner.

68. NCB is in complete operation, control, and supervision of its servers and systems.

69. NCB intentionally configured and designed its servers and systems in such a way that allowed it to be susceptible to cyber-attack. Further, NCB intentionally configured and designed its servers and systems without adequate data security protections and without regard to Plaintiffs' and Class Members' PII, which was disclosed to cyber criminals.

70. BOA and Pathward entrusted NCB with their customers' PII. Further, these financial institutions did not properly verify, oversee, and supervise NCB's entrustment of their customers' PII.

71. By obtaining, using, disclosing, and deriving a benefit from Plaintiffs' and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiffs' and Class Members' PII from disclosure.

72. Plaintiffs and Class Members reasonably expect that financial institutions and their vendors, such as Defendant, will use the utmost care to keep their PII confidential and securely maintained, to use this information for business purposes only, to only store it until it is no longer needed, to properly dispose of it, and to make only authorized disclosures of this information.

73. Defendant failed to prioritize data and cyber security by adopting reasonable data and cyber security measures to prevent and detect the unauthorized access to Plaintiffs' and Class Members' PII.

74. Had Defendant remedied the security deficiencies, followed industry guidelines, and adopted security measures recommended by experts in the field, Defendant would have prevented the theft of Plaintiffs' and Class Members' confidential PII.

75. Given the rise in ransomware attacks in the financial services industry, NCB was a prime target in this Data Breach.

76. As noted, the Data Breach appears to be a ransomware attack. While NCB claims that it "discovered on February 4 that an unauthorized party gained access to NCB's systems on February 1, 2023," given what is known about ransomware attacks, how long hackers typically lie hidden in a company's systems before being discovered, how hackers propagate ransomware across entire networks, as well as the scope of the PII involved in this Data Breach—the hackers were likely in NCB's systems and servers well before February 1, with unfettered access to Plaintiffs' and Class Members' PII.

III. Defendant's Data Security Failures

77. By its own admission, NCB "blend[s] many years of ARM experience with the ***latest in new information systems*** and communication technology."[21] (emphasis added).

[21] NCB, *NCB Management Services, Inc. Partners with Interactions to Power Consumer-Centric Conversations*, Jan. 27, 2022, *available at* https://ncbi.com/NewsArticles/jan272022 (last visited July 20, 2023).

However, NCB's words ring hollow. As described *infra*, NCB's emphasis on proper data security in its "information systems" was woefully lacking and far from "new."

78. Prevention is the most effective defense against ransomware and it is critical to take precautions for protection. However, NCB took no such precautions to appropriately secure Plaintiffs' and Class Members' PII.

79. Further, NCB's data retention practices were also severely deficient. NCB continued to store and maintain PII for many years after NCB had appropriate use for such data. BOA and Pathward also failed to properly supervise NCB's data retention practices to ensure that customer data that was no longer needed was properly archived and/or removed from NCB's servers and systems.

80. NCB failed to archive such PII and remove it from its servers and systems, which allowed hackers to gain access to the PII in the Data Breach.

81. Up to and including the period when the Data Breach occurred, Defendant breached its duties, obligations, and promises to Plaintiffs and Class Members by their failure to:

a. hire qualified personnel and maintain a system of accountability over data security, thereby knowingly allowing data security deficiencies to persist;

b. properly supervise and train its employees, and ensure that their vendor's employees were supervised and trained, about the risk of cyber-attacks and how to mitigate them, including by failing to implement adequate security awareness training that would have instructed employees about the risks of common techniques, what to do if they suspect such attacks, and how to prevent them;

c. address well-known warnings that its systems and servers, and those of its vendors, were susceptible to a data breach;

d. implement certain protocols that would have prevented unauthorized programs, such as malware and ransomware, from being installed on its servers and systems that accessed customers' personal information and otherwise would have protected customers' sensitive personal information;

e. install software to adequately track access to its network, monitor the network for unusual activity, and prevent exfiltration of data, which would have detected the presence of hackers and prevented customers' sensitive personal information from being stolen. Specifically, there are recommended, available measures to prevent data from leaving protected systems and being sent to untrusted networks outside of the corporate systems; and

f. adequately safeguard customers' sensitive personal information and maintain an adequate data security environment to reduce the risk of a data breach or unauthorized disclosure.

82. Up to, and including, the period when the Data Breach occurred, Defendant breached its duties, obligations, and promises to Plaintiffs and Class Members by their failure to oversee the entrustment of Plaintiffs' and Class Members' PII.

IV. NCB's Failure to Comply with Government and Industry Guidelines, Standards, and Recommendations

83. According to NCB, "[a]chieving superior results and protecting [its clients'] reputation are NCB's highest priorities."[22] NCB says it "accomplishes" this by using "the latest technology advancements," "***apply[ing] the highest in security standards***" and "employ[ing] a well-trained, highly effective staff."[23] (emphasis added).

[22] NCB, *Financial Recovery*, *available at* https://www.ncbi.com/Financial (last visited July 20, 2023).
[23] *Id.*

84. However, NCB fell woefully short not only in its own self-professed "security standards," but also industry standards as well.

85. Hackers routinely target financial services providers and vendors, such as NCB, since they are particularly vulnerable to cyber-attacks because of the value of the PII which they collect and maintain.

86. Industry experts identify several best practices that, at a minimum, should be implemented by ARM companies such as NCB, including but not limited to: educating all employees, strong passwords, multi-layer security, including firewalls, anti-virus, and antimalware software, encryption, making data unreadable without a key, multi-factor authentication, backup data, and limiting which employees can access sensitive data.

87. Upon information and belief, NCB failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls ("CIS CSC"), which are all established standards in reasonable cybersecurity readiness.

88. CISA recommends the following precautions to organizations to protect them against the threat of ransomware:

- Update software and operating systems with the latest patches. Outdated applications and operating systems are the target of most attacks.
- Never click on links or open attachments in unsolicited emails.
- Back up data on a regular basis. Keep it on a separate device and store it offline.

- Follow safe practices when using devices that connect to the Internet. Read "Good Security Habits" for additional details.[24]

89. In addition, the U.S. Government also recommends that organizations employ the following best practices when it comes to ransomware:

- Restrict users' permissions to install and run software applications, and apply the principle of "least privilege" to all systems and services. Restricting these privileges may prevent malware from running or limit its capability to spread through a network.
- Use application allow listing to allow only approved programs to run on a network.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.

90. Upon information and belief, NCB failed to meet CISA and the federal government's above data security recommendations concerning ransomware. This failure resulted in the Data Breach.

91. The above government and industry frameworks are existing and applicable industry standards in the financial services industry. Upon information and belief, NCB failed to comply with these accepted standards, which left NCB susceptible to the Data Breach.

[24] CISA, *Ransomware FAQs*, *available at* https://www.cisa.gov/stopransomware/ransomware-faqs (last visited July 20, 2023).

92. At all times, NCB was in complete control of the configuration and design of its servers and systems.

V. Defendant's Data Security Failures Constitute Unfair and Deceptive Practices and Violations of Consumers' Privacy Rights

93. Defendant is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The U.S. Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for sensitive personal information is an "unfair practice" in violation of the FTC Act.

94. 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.

95. In 2007, the FTC published guidelines that establish reasonable data security practices for businesses. The guidelines note that businesses should protect the personal 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 for installing vendor-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone may be trying 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.

96. The FTC has also published a document entitled "FTC Facts for Business," which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.

97. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to private 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.

98. The FTC has also brought enforcement actions against businesses for failing to adequately and reasonably protect personal data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to sensitive personal information as an unfair act or practice prohibited by Section 5 of the FTC Act. The FTC has issued orders against businesses that have failed to employ reasonable measures to secure sensitive personal information. These orders provide further guidance to businesses regarding their data security obligations.

99. The FTC deems the failure to employ reasonable and appropriate measures to protect against unauthorized access to sensitive personal information an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

100. Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to PII or to prevent the disclosure of such information to unauthorized individuals, as reflected by the sensitive driver's license numbers and Social Security numbers stolen, constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

101. NCB was always fully aware of its obligations to protect PII since it was in the business as an ARM of obtaining, collecting, and disclosing PII as well as collecting, storing, and

using other confidential personal and financial information. Defendant was also aware of the significant repercussions that would result from its failure to do so.

102. Prior to and during the Data Breach, Defendant failed to follow guidelines set forth by the FTC and actively mishandled the management of their IT security.

103. Furthermore, by failing to have reasonable data security measures in place, Defendant engaged in an unfair act or practice within the meaning of Section 5 of the FTC Act.

VI. The Value of the Disclosed PII and Effects of Unauthorized Disclosure

104. Defendant understood that the protected PII it transfers, acquires, stores, and utilizes is highly sensitive and of significant value to the owners of the PII and those who would use it for wrongful purposes.

105. PII is a valuable commodity to identity thieves, particularly when it is aggregated in large numbers. Former United States Attorney General William P. Barr made clear that consumers' sensitive personal information commonly stolen in data breaches "has economic value."[25]

106. The purpose of stealing large caches of personal data is to use it to defraud individuals or to place it for illegal sale and profit from other criminals who buy the data and use it to commit fraud and identity theft. Indeed, cybercriminals routinely post stolen personal information on anonymous websites, making the information widely available to the criminal underworld.

107. There is an active and robust market for this information. As John Sancenito, President of Information Network Associates, a company which helps companies with recovery

[25] William P. Barr, U.S. DEPT. OF JUSTICE, *Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax*, Feb. 10, 2020, *available at* https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-four-members-china-s-military (last visited July 20, 2023).

after data breaches, explained after a data breach "[m]ost of the time what [data breach hackers] do is they steal the data and then they sell the data on the dark web to the people who actually commit the fraud."[26]

108. Some of the forms of PII involved in this Data Breach are particularly concerning. Unique Social Security and driver's license numbers cannot be easily replaced. Even when such numbers are replaced, the process of doing so results in a major inconvenience to the affected person, requiring a wholesale review of their relationships with government agencies and any number of private companies, in order to update the person's accounts with those entities.

109. ***Driver's license numbers***—which were compromised as a result of the Data Breach—are highly sought after by cybercriminals on the dark web because they are unique to a specific individual, extremely sensitive, and cannot easily be replaced.

110. Experian, a globally recognized credit reporting agency, has explained "[n]ext to your Social Security number, your driver's license number is one of the most important pieces of information to keep safe from thieves."[27] This is because a driver's license number is connected to an individual's vehicle registration, insurance policies, records on file with the state Department of motor vehicles, and other government agencies, financial institutions, places of employment, doctor's offices, and other entities.

111. For these reasons, driver's license numbers are highly sought out by cyber criminals because they are one of the most valuable pieces of information to facilitate identity theft and fraud. This information is valuable because cyber criminals can use this information to open credit

[26] Priscilla Liguori, ABC27 (WHTM), *Legislator, security expert weigh in on Rutter's data breach*, Feb. 14, 2020 (updated: Feb. 17, 2020), *available at* https://www.abc27.com/local-news/york/legislator-security-expert-weigh-in-on-rutters-data-breach/ (last visited July 20, 2023).

[27] Sue Poremba, EXPERIAN, *What Should I Do if My Driver's License Number is Stolen*, Oct. 24, 2018, *available at* https://web.archive.org/web/20191018195031/https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/ (last visited July 20, 2023).

card accounts, obtain insurance policies and submit fraudulent claims, open cell phone contracts, file fraudulent tax returns, file unemployment applications, as well as obtain bank loans under a person's name.

112. ***Social Security numbers***—which were also compromised as a result of the Data Breach—are highly sought after by cyber criminals on the dark web because they are unique to a specific individual and extremely sensitive and cannot easily be replaced.

113. Indeed, even the Social Security Administration ("SSA") warns that the process of replacing a Social Security number is a difficult one that creates other types of problems, and that it will not be a panacea for the affected person:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make it more difficult for you to get credit.[28]

114. Social Security numbers allow individuals to apply for credit cards, student loans, mortgages, and other lines of credit—among other services. Often, Social Security numbers can be used to obtain medical goods or services, including prescriptions. They are also used to apply for a host of government benefits. Access to such a wide range of assets makes Social Security

[28] SSA, *Identity Theft and Your Social Security Number*, Publication No. 05-10064 July 2021, *available at* https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited July 20, 2023).

numbers a prime target for cyber criminals and a particularly attractive form of PII to steal and then sell.

115. The ramifications of Defendant's failure to keep Plaintiffs' and Class Members' PII secure are long lasting and severe. To avoid detection, identity thieves often hold stolen data for months or years before using it. Also, the sale of stolen information on the "dark web" may take months or more to reach end-users, in part because the data is often sold in small batches as opposed to in bulk to a single buyer. Thus, Plaintiffs and Class Members must vigilantly monitor their financial accounts *ad infinitum*.

116. In light of this reality, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to it and the foreseeable consequences if its servers and systems were breached. However, NCB failed to take adequate cybersecurity measures to prevent the Data Breach from occurring.

117. As highly sophisticated parties that handle sensitive PII, Defendant failed to establish and/or implement appropriate administrative, technical and/or physical safeguards to ensure the security and confidentiality of Plaintiffs' and other Class Members' PII to protect against anticipated threats of intrusion of such information.

118. Identity thieves use stolen PII for various types of criminal activities, such as when personal and financial information is used to commit fraud or other crimes, including credit card fraud, phone or utilities fraud, bank fraud, and government fraud.

119. The PII exfiltrated in the Data Breach can also be used to commit identity theft by placing Plaintiffs and Class Members at a higher risk of "phishing," "vishing," "smishing," and "pharming," which are other ways for cyber criminals to exploit information they already have in order to get even more personally identifying information from a person through unsolicited email,

text messages, and telephone calls purportedly from a legitimate company requesting personal, financial, and/or login credentials.

120. There is often a lag time between the occurrence of fraud and its discovery. Similarly, a gap in time often exists between when PII is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[29]

121. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the cyber black market for years.

122. Plaintiffs and Class Members rightfully place a high value not only on their PII, but also on the privacy of that data.

123. Because of the Data Breach and the immense value of the PII that was stolen, Plaintiffs and Class Members face an increased risk of fraud and identity theft for many years into the future.

VII. The Driver's Privacy Protection Act ("DPPA")

124. NCB also had an obligation under the DPPA. The DPPA was enacted in 1994 in response to safety and privacy concerns stemming from the ready availability of personal information contained in state motor vehicle records. The DPPA was passed in the backdrop of the murder of actress Rebecca Schaeffer, whose murderer obtained her unlisted address through the California Department of Motor Vehicle ("DMV").

[29] GAO, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, June 2007, GAO-07-737, *available at* https://www.gao.gov/assets/a262904.html (last visited July 20, 2023).

125. Additional concerns were raised when witnesses testified in hearings before Congress regarding the privacy of DMV information of domestic violence victims and law enforcement officers, among other safety concerns surrounding driver information. To address these concerns, the DPPA restricts the disclosure of personal information from motor vehicle records to certain permissible purposes expressly defined by the Act.

126. Unauthorized disclosures of information have long been seen as injurious. The common law alone will sometimes protect a person's right to prevent the dissemination of private information. Indeed, it has been said that privacy torts have become well-ensconced in the fabric of American law. And with privacy torts, improper dissemination of information can itself constitute a cognizable injury. Because damages for a violation of an individual's privacy are a quintessential example of damages that are uncertain and possibly unmeasurable, causes of action such as the DPPA provide privacy tort victims with a monetary award calculated without the need of proving actual damages.

127. The DPPA states that "[a] [s]tate department of motor vehicles, and any officer, employee, or contractor thereof, shall not knowingly disclose or otherwise make available to any person or entity: (1) personal information, as defined in 18 U.S.C. [§] 2725(3), about any individual obtained by the department in connection with a motor vehicle record, except as provided in subsection (b) of this section. . . ." 18 U.S.C. § 2721(a)(1).

128. NCB had an obligation to use reasonable security measures under the DPPA, which further states that "[i]t shall be unlawful for any person knowingly to obtain or disclose personal information, from a motor vehicle record, for any use not permitted under section 2721(b) of this title." 18 U.S.C. § 2722(a).

129. Thus, the DPPA provides citizens with a private right of action in the event that their private information is knowingly obtained, disclosed, or used in a manner other than for the enumerated permissible purposes.

130. The DPPA states: "[a] person who knowingly obtains, discloses or uses personal information, from a motor vehicle record, for a purpose not permitted under this chapter [18 U.S.C. §§ 2721, et seq.] shall be liable to the individual to whom the information pertains, who may bring a civil action in a United States district court." 18 U.S.C. § 2724(a).

131. The default rule under the DPPA is non-disclosure. The DPPA is structured such that 18 U.S.C. § 2721(a)(1) and 18 U.S.C. § 2722(a) provide the general prohibition on the release and use of motor vehicle information, and § 2721(b) enumerates fourteen specific exceptions to the general prohibition. Disclosing information to cyber criminals is not one of them. Because the PII was disclosed to unauthorized individuals—i.e., cyber criminals—there is no feasible argument that disclosure was "for a permissible purpose."

132. If not for NCB's intentional configuration and design of its servers and systems, it would not have disclosed Plaintiffs' and Class Members' PII to cyber criminals.

133. The Data Breach was a direct and proximate result of NCB's flawed configuration and design of its servers and systems and its failure to implement and follow even basic security procedures.

COMMON INJURIES AND DAMAGES

134. As result of Defendant's ineffective and inadequate data security practices, Plaintiffs and Class Members now face a present and ongoing risk of fraud and identity theft.

135. Due to the Data Breach and the foreseeable consequences of PII ending up in the possession of cybercriminals, the risk of identity theft to Plaintiffs and Class Members has

materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy, (b) "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft, (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk, (d) "out of pocket" costs incurred due to actual identity theft, (e) loss of time incurred due to actual identity theft, (f) loss of time due to increased spam and targeted marketing emails, (g) the loss of benefit of the bargain, (h) diminution of value of their PII, and (i) the continued risk to their PII, which remains in Defendant's possession and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' PII.

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

136. The link between a data breach and the risk of identity theft is simple to grasp and well established: criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes, as discussed further below.

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

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

manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on victims.

139. The dark web is an unindexed layer of the internet that requires special software or authentication to access.[30] 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.[31] This anonymity prevents dark web marketplaces from being easily monitored by authorities or accessed by less sophisticated users.

140. 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 issue here.[32] The digital character of PII stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the internet while the buyer and seller 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.[33] As Microsoft warns "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others."[34]

---

[30] Louis DeNicola, EXPERIAN, *What Is the Dark Web?*, May 12, 2021, available at https://www.experian.com/blogs/ask-experian/what-is-the-dark-web (last visited July 20, 2023).
[31] *Id.*
[32] *What is the Dark Web?* – Microsoft 365, July 15, 2022, *available at* https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web (last visited July 20, 2023).
[33] *Id.*; *see also* Louis DeNicola, *supra*.
[34] *What is the Dark Web?* – Microsoft 365.

141. Social Security numbers, for example, are among the most devastating kind of PII to have stolen because they may be put to numerous serious fraudulent uses and are difficult for individuals to change. The Social Security Administration stresses that the loss of Social Security numbers, as occurred here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[35]

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

143. Even then, obtaining a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[36]

144. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name, but with the thief's picture, use the victim's name and Social Security number to obtain government benefits, or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain jobs using stolen Social Security

[35] SSA, *Identity Theft and Your Social Security Number*, *supra*.
[36] Brian Naylor, NPR, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, Feb. 9, 2015, *available at* http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited July 20, 2023).

numbers, rent houses or receive medical services in the victims' names, and may even give that personal information to police during arrests resulting in arrest warrants being issued in victims' names. Identity thieves can use stolen Social Security numbers to apply for additional credit lines.

145. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.[37]

146. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[38] Defendant, however, did not rapidly report to Plaintiffs and/or the Class that their PII had been stolen.

147. Victims of identity theft also often suffer embarrassment, blackmail or harassment—in person or online, and/or experience financial losses resulting from fraudulently opened accounts or the misuse of existing accounts.

148. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims spend a considerable time repairing the damage caused by the theft of their PII. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones and/or dispute charges with creditors.

149. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen private information. To protect themselves, Plaintiffs

[37] *See 2019 Internet Crime Report*, FBI (Feb. 11, 2020), *available at* https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120 (last visited July 20, 2023).
[38] *Id.*

and Class Members must, therefore, remain vigilant against unauthorized data use for years or even decades to come.

150. 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. Thus, the larger the data set, the greater potential for analysis and profit."[39]

151. The FTC has also issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making. According to the FTC, data security requires: (1) encrypting information stored on computer networks, (2) retaining payment card information only as long as necessary, (3) properly disposing of personal information that is no longer needed, (4) limiting administrative access to business systems, (5) using industry-tested and accepted methods for securing data, (6) monitoring activity on networks to uncover unapproved activity, (7) verifying that privacy and security features function properly, (8) testing for common vulnerabilities, and (9) updating and patching third-party software.[40]

152. According to the FTC, unauthorized PII disclosures are extremely damaging to consumers' finances, credit history and reputation and can take time, money and patience to resolve the fallout. The FTC treats the failure to employ reasonable and appropriate measures to

[39] FTC, Statement of FTC Commissioner Pamela Jones Harbour (Remarks Before FTC Exploring Privacy Roundtable), Dec. 7, 2009, *available at* http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf (last visited July 20, 2023).
[40] *See* FTC, *Protecting Personal Information: A Guide for Business*, *available at* https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited July 20, 2023).

protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act.[41]

153. Defendant's failure to properly and timely notify Plaintiffs and Class Members of the Data Breach exacerbated Plaintiffs' and Class Members' injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

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

154. As a result of the recognized risk of identity theft, when a Data Breach occurs and an individual is notified by a company that his/her PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm. In working to protect against future identity theft or fraud, however, an individual suffers harm to a different, but no less valuable, asset: time itself.

155. Thus, due to the actual and imminent risk of identity theft, Plaintiffs and Class Members must, as Defendant's notices of the Data Breach instructs them, to "[p]lease promptly review your credit reports and account statements over the next 12 to 24 months" [42] and "[i]t is recommended that you remain vigilant for incidents of fraud and identity theft."[43]

156. 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

[41] *See* FTC, *Commission Finds LabMD Liable for Unfair Data Security Practices*, *available at* https://www.ftc.gov/news-events/news/press-releases/2016/07/commission-finds-labmd-liable-unfair-data-security-practices (last visited July 20, 2023).
[42] *See* BOA Data Breach Notification Letter.
[43] *See* Pathward Data Breach Notification Letter.

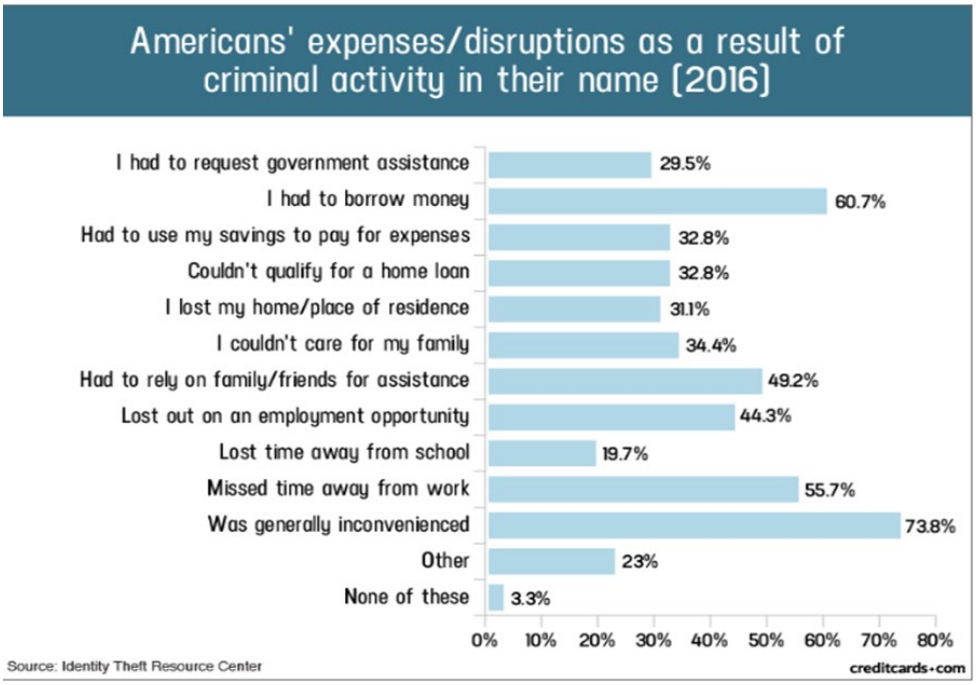
agencies, contacting financial institutions, closing, or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports, which may take years to discover and detect.

157. Plaintiffs' and Class Members' mitigation efforts are consistent with the U.S. Government Accountability Office's 2007 report regarding data breaches (the "GAO Report"), in which the GAO noted that victims of identity theft will undoubtedly face "substantial costs and time to repair the damage to their good name and credit record."[44]

158. Plaintiffs' and Class Members' mitigation efforts are also consistent with the steps that the FTC recommends that data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and 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.[45]

159. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[46]

[44] *See* GAO, GAO-07-737, *supra*.
[45] *See* FTC, *IdentityTheft.gov*, *available at* https://www.identitytheft.gov/Steps (last visited July 20, 2023).
[46] Jason Steele, *Credit Card and ID Theft Statistics*, Oct. 24, 2017, *available at* https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276 (last visited July 20, 2023).



160. The GAO Report noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[47] Indeed, the FTC recommends that identity theft victims take several steps and spend time 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.[48]

III. Diminution of Value of the Private Information

161. Undisclosed PII and/or PHI are valuable property rights.[49] Their value is axiomatic, considering the consequences for theft of that data. Even this obvious risk-to-reward analysis illustrates beyond doubt that PHI and/or PII has considerable market value.

[47] *See* GAO Report, *supra* note 95, at 2.
[48] *See* FTC, IdentityTheft.gov, https://www.identitytheft.gov/Steps, *supra*.
[49] *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

162. For example, drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase PII on the black market for the purpose of target-marketing their products and services.

163. Sensitive PII can sell for as much as $363 per record, according to the Infosec Institute.[50] According to account monitoring company, LogDog, medical data, such as PHI, sells for $50 and up on the Dark Web.[51]

164. An active and robust legitimate marketplace for private information like PII and/or PHI also exists. In 2019, the data brokering industry was worth roughly $200 billion.[52] In fact, the data marketplace is so sophisticated that consumers can sell their non-public information directly to a data broker who, in turn, aggregates the information and provides it to marketers or app developers.[53,54] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[55]

165. As a result of the Data Breach, Plaintiffs' and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished in its value by its unauthorized and potential release on the Dark Web, where it holds significant value for the threat actors.

---

obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[50] *See* Ashiq Ja, INFOSEC, *Hackers Selling Healthcare Data in the Black Market*, July 27, 2015, https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.

[51] Lisa Vaas, NAKED SECURITY, *Ransomware Attacks Paralyze and Sometimes Crush, Hospitals*, Oct. 3, 2019, *available at* https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content (last visited July 20, 2023)

[52] David Lazarus, LA TIMES, *Column: Shadowy data brokers make the most of their invisibility cloak*, Nov. 5, 2019), *available at* https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited July 20, 2023).

[53] https://datacoup.com/ (last visited May 17, 2023).

[54] https://digi.me/what-is-digime/.(last visited May 17, 2023).

[55] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited May 15, 2023).

IV. Loss of Benefit of the Bargain

166. Plaintiffs are entitled to expectation damages on the difference in banking service value considering the deficient data security and/or restitution for the conferred benefit in the form of account fees for the deficient data security that the Defendant failed to provide.

V. Injunctive Relief Is Necessary to Protect Against Future Data Breaches

167. Moreover, Plaintiffs and Class Members have an interest in ensuring that their PII, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including, but not limited to, ensuring that the storage of data or documents containing PII is not accessible online and that access to such data is password protected.

168. Money damages are inadequate to fully compensate as Defendant is in exclusive control over their operations and control the manner in which they store Plaintiffs' and Class Members' PII.

169. The deletion of unnecessary information is a low burden on Defendant. The implementation of other reasonable security measures is also achievable with a balanced costs and hardship on Defendant. Both types of injunctive relief are feasible and manageable for the court to enforce.

VI. Defendant's Representations and Privacy Policies

170. Plaintiffs were and are very careful about sharing their PII. Plaintiffs have never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

171. Plaintiffs stored any documents containing their PII in a safe and secure location or destroyed the documents. Moreover, Plaintiffs diligently chose unique usernames and passwords for their various online accounts.

172. Plaintiffs took reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep their PII confidential and securely maintained, to use this information for related business purposes only, and to make only authorized disclosures of this information.

173. BOA represents that customer security is its "top priority."[56] In fact, BOA's Privacy Policy states:

> 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.[57]

174. As a condition precedent to receiving banking services from BOA, Plaintiffs and Class Members who were BOA customers were required to provide sensitive PII. At that time, upon information and belief, Plaintiffs' and Class Members' PII was entered and stored on BOA's computer systems. Plaintiffs and Class Members did so with the understanding that BOA would take reasonable and appropriate measures to safeguard this confidential information with which it was entrusted.

175. In its Privacy Policy, Pathward assures its customers and potential customers that it takes steps to maintain the security of their Private Information, and states that:

> To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. The measures include computer safeguards and secured files and buildings. We also maintain other physical, electronic and procedural safeguards to protect this information and we limit access to information to those employees for whom access is appropriate.[58]

[56] *See* https://www.bankofamerica.com/security-center/overview/ (last visited July 19, 2023).
[57] *See* https://www.bankofamerica.com/security-center/consumer-privacy-notice/ (last visited July 19, 2023).
[58] *See* https://web.archive.org/web/20221220082906/https://www.pathward.com/content/dam/pathward/us/en/documents/pdfs/Privacy-Policy-Notice.pdf (last visited July 19, 2023).

176. As a condition precedent to receiving banking services from Pathward, upon information and belief, Plaintiffs and Class Members who were Pathward customers were required to provide sensitive PII. At that time, upon information and belief, Plaintiffs' and Class Members' PII was entered and stored on Pathward's computer systems. Plaintiffs and Class Members did so with the understanding that Pathward would take reasonable and appropriate measures to safeguard this confidential information with which it was entrusted.

177. Plaintiffs and Class Members place significant value on the security of their PII. Plaintiffs and Class Members provided their PII to the Defendant with the understanding and expectation that their information would remain secure and that any authorized third party custodian or vendor would be adequately screened and would employ reasonable and adequate and industry standard security measures to ensure that it would not be compromised.

178. Defendant knowingly acquired, stored, utilized, and benefited from Plaintiffs' PII during the course of its business operations. Upon information and belief, Defendant acquired Plaintiffs' PII through Plaintiffs' banking and/or credit relationship with either BOA and Pathward. The precise time, manner, and purpose by which Defendant acquired and utilized Plaintiffs' private information is within the exclusive control of Defendant.

179. By acquiring, storing, and benefiting from Plaintiffs' PII, Defendant owed and otherwise assumed duties to safeguard Plaintiffs' PII. Defendant, however, failed to provide adequate data security and placed Plaintiffs' and Class Members' PII at risk of compromise and unauthorized disclosure in a foreseeable data breach.

VII. Plaintiffs' Specific Experiences

Plaintiff Joseph Lindquist

180. Prior to the Data Breach, Plaintiff Lindquist was a customer of NCB and BOA and provided BOA his PII as a condition to receive banking and/or credit services. NCB serviced Plaintiff Lindquist's BOA account and therefore had access to his PII.

181. Plaintiff Lindquist relied upon Defendant to provide or ensure adequate data security to protect his PII. Plaintiff Lindquist reasonably expected adequate data security as a basic assumption of his implied contractual relationship with NCB and BOA.

182. Plaintiff Lindquist's PII was accessed and compromised due to Defendant's failures. Plaintiff Lindquist received a Notice Letter dated March 24, 2023, informing him that his 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 were exposed in the Data Breach, and that he should take specific steps to protect himself from future identity theft.

183. In response and as a result of the Data Breach, Plaintiff Lindquist has spent time and effort researching the Data Breach and reviewing and monitoring his accounts for fraudulent activity. Plaintiff Lindquist estimates that he spent approximately 2 hours monitoring his accounts for suspicious activity, signing up for credit monitoring, and otherwise addressing the Data Breach.

Plaintiff Lillian Mardikian

184. Prior to the Data Breach, Plaintiff Mardikian was a customer of NCB and BOA and provided BOA her PII as a condition to receive banking and/or credit services. NCB serviced Plaintiff Mardikian's BOA account and therefore had access to her PII.

185. Plaintiff Mardikian relied upon Defendants to provide or ensure adequate data security to protect her PII. Plaintiff Mardikian reasonably expected adequate data security as a basic assumption of her implied contractual relationship with NCB and BOA.

186. Plaintiff Mardikian's PII was accessed and compromised due to Defendant's failures. Plaintiff Lindquist received a Notice Letter dated March 24, 2023, informing her that 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 were exposed in the Data Breach, and that she should take specific steps to protect herself from future identity theft.

187. In response and as a result of the Data Breach, Plaintiff Mardikian has spent time and effort researching the Data Breach and reviewing and monitoring her accounts for fraudulent activity. Plaintiff Mardikian estimates that she spent approximately 13 to 15 hours monitoring her accounts for suspicious activity, signing up for credit monitoring, and otherwise addressing the Data Breach. Plaintiff Mardikian further signed up for credit monitoring as a result of the Data Breach at a rate of $20/month.

Plaintiff Howard Suh

188. Prior to the Data Breach, Plaintiff Suh was a customer of NCB and BOA and provided BOA his PII as a condition to receive banking and/or credit services. NCB serviced Plaintiff Suh's BOA account and therefore had access to his PII.

189. Plaintiff Suh relied upon Defendant to provide or ensure adequate data security to protect his PII. Plaintiff Suh reasonably expected adequate data security as a basic assumption of his implied contractual relationship with NCB and BOA.

190. Plaintiff Suh's PII was accessed and compromised due to Defendant's failure. He received a Notice Letter dated March 24, 2023 informing him that his fist 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 were exposed in the Data Breach and that he should take specific steps to protect himself from future identity theft.

191. In response and as a result of the Data Breach, Plaintiff Suh spent time and effort researching the Data Breach and reviewing and monitoring his accounts for fraudulent activity. He also had to change his automatic billing instructions tied to the compromised BOA account.

192. Notably, following the Data Breach, Plaintiff Suh experienced actual fraud and identity theft. In particular, following the Data Breach, an unauthorized and unknown third party submitted a loan application in his name, which was recorded on his Experian account. He also experienced unauthorized charges in the amount of $30 to his bank account in March. This was the same bank account that was compromised in the NCB Data Breach.

193. Further, Plaintiff Suh has received emails from Venmo that someone was trying to login to his account. Plaintiff Suh also received an email that someone was trying to apply for a loan in his name through an unknown company.

194. Moreover, following the Data Breach, Plaintiff Suh experienced an excessive increase in spam calls on his phone, forcing him to change his phone number.

195. In total, Plaintiff Suh estimates he spent approximately 15 hours addressing the Data Breach and fraudulent activity on his accounts.

Plaintiff Ernesto Medina

196. Prior to the Data Breach, Plaintiff Medina was a customer of NCB and BOA and provided BOA his PII as a condition to receive banking and/or credit services. NCB serviced Plaintiff Medina's BOA account and therefore had access to his PII.

197. Plaintiff Medina relied upon Defendant to provide or ensure adequate data security to protect his PII. Plaintiff Medina reasonably expected adequate data security as a basic assumption of his implied contractual relationship with NCB and BOA.

198. Plaintiff Medina's PII was accessed and compromised due to Defendant's failures. He received a Notice Letter dated March 24, 2023 informing him that his 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 were exposed in the Data Breach and that he should take specific steps to protect himself from future identity theft.

199. In response and as a result of the Data Breach, Plaintiff Medina has spent time and effort researching the Data Breach and reviewing and monitoring his accounts for fraudulent activity. Plaintiff Medina estimates that he spent approximately 8 hours monitoring his accounts for suspicious activity and otherwise addressing the Data Breach.

Plaintiff Benedict Lozada

200. Prior to the Data Breach, Plaintiff Lozada was a customer of NCB. NCB serviced Plaintiff Lozada's account that had gone to collections and therefore had access to his PII. Plaintiff Lozada received a Data Breach Notification letter purportedly from NCB purportedly pertaining to a Pathward account.

201. Plaintiff Lozada relied upon Defendant to provide or ensure adequate data security to protect his PII. Plaintiff Lozada reasonably expected adequate data security as a basic assumption of his implied contractual relationship with NCB and Pathward.

202. Plaintiff Lozada's PII was accessed and compromised due to Defendant's failures. Plaintiff Lozada received a Notice Letter dated May 22, 2023 informing him that his first and last name, and Social Security number were exposed in the Data Breach and that he should take specific steps to protect himself from future identity theft.

203. In response and as a result of the Data Breach, Plaintiff Lozada has spent time and effort researching the Data Breach and reviewing and monitoring his accounts for fraudulent activity. Plaintiff Lozada estimates that he spent approximately several hours monitoring his accounts for suspicious activity and otherwise addressing the Data Breach.

Plaintiff Edward Del Hierro

204. Prior to the Data Breach, Plaintiff Del Hierro was a customer of NCB. NCB serviced Plaintiff Del Hierro's account that had gone to collections and therefore had access to his PII. Plaintiff Del Hierro received a Data Breach Notification letter purportedly from NCB purportedly pertaining to a Pathward account.

205. Plaintiff Del Hierro relied upon Defendant to provide or ensure adequate data security to protect his PII. Plaintiff Del Hierro reasonably expected adequate data security as a basic assumption of his implied contractual relationship with NCB and Pathward.

206. Plaintiff Del Hierro's PII was accessed and compromised due to Defendant's failures. Plaintiff Del Hierro received a Notice Letter dated May 23, 2023 informing him that his first and last name, and Social Security number were exposed in the Data Breach and that he should take specific steps to protect himself from future identity theft.

207. In response and as a result of the Data Breach, Plaintiff Del Hierro has spent time and effort researching the Data Breach and reviewing and monitoring his accounts for fraudulent activity. Plaintiff Del Hierro estimates that he spent approximately 15 hours monitoring his accounts for suspicious activity and otherwise addressing the Data Breach.

Plaintiff Tobi Patterson

208. Prior to the Data Breach, Plaintiff Patterson was a customer of NCB and BOA and provided BOA her PII as a condition to receive banking and/or credit services. NCB serviced Plaintiff Patterson's BOA account and therefore had access to her PII.

209. Plaintiff Patterson relied upon Defendant to provide or ensure adequate data security to protect her PII. Plaintiff Patterson reasonably expected adequate data security as a basic assumption of her implied contractual relationship with NCB and BOA.

210. Plaintiff Patterson's PII was accessed and compromised due to Defendant's failures. Plaintiff Patterson received a Notice Letter dated May 23, 2023, informing her that her first and last name, and Social Security number were exposed in the Data Breach and that she should take specific steps to protect herself from future identity theft.

211. In response and as a result of the Data Breach, Plaintiff Patterson has spent time and effort researching the Data Breach and reviewing and monitoring her accounts for fraudulent activity. Plaintiff Patterson also experienced actual fraud and identity theft.

212. Moreover, following the Data Breach, Plaintiff Patterson has experienced actual fraud and misuse of her PII. Specially, an unauthorized and unknown third party applied for a secondary debit card SMI ONE in her name, and she received emails from loan companies that loans had been applied for in her name. Plaintiff Patterson also received an email from Experian indicating that an account was created using her email under the name "William" which she did

not authorize. In addition, Plaintiff Patterson experienced fraudulent charges on her payment card in the amount of $538 and a $35 charge for child support; Plaintiff Patterson did not authorize either of these charges. Notably, the card with the fraudulent activity was the same card that was tied to the compromised BOA account that was impacted by the Data Breach.

213. In response and as a result of the Data Breach, Plaintiff Patterson estimates that she spent approximately 25 hours addressing these issues, some of which are ongoing (including seeking reimbursement for the fraudulent charges). Plaintiff Patterson also spent approximately $30 to travel to the police department and the post office to address the instances of fraud.

Plaintiff Jude-Law Palmer

214. Prior to the Data Breach, Plaintiff Palmer was a customer of NCB and BOA and provided BOA his PII as a condition to receive banking and/or credit services. NCB serviced Plaintiff Palmer's BOA account and therefore had access to his PII.

215. Plaintiff Palmer relied upon Defendant to provide or ensure adequate data security to protect his PII. Plaintiff Palmer reasonably expected adequate data security as a basic assumption of his implied contractual relationship with NCB and BOA.

216. Plaintiff Palmer's PII was accessed and compromised due to Defendant's failures. Plaintiff Palmer received a Notice Letter dated March 24, 2023 informing him this his 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 was exposed in the Data Breach, and that he should take specific steps to protect himself from future identity theft.

217. In response and as a result of the Data Breach, Plaintiff Palmer has spent time and effort researching the Data Breach and reviewing and monitoring his accounts for fraudulent activity.

218. Plaintiff Palmer has additionally experienced an increase in spam calls following the Data Breach. He also received a suspicious invoice from PayPal that he did not recognize. Plaintiff Palmer estimates that he spent approximately 2.5 hours monitoring his accounts for suspicious activity, changing his passwords, freezing accounts, calling his bank, signing up for credit monitoring, and otherwise addressing the Data Breach.

Plaintiff Kevin Bliss

219. Prior to the Data Breach, Plaintiff Kevin Bliss was a customer of NCB and BOA and provided BOA his PII as a condition to receive banking and/or credit services. NCB serviced Plaintiff Bliss's BOA account and therefore had access to his PII.

220. Plaintiff Bliss relied upon Defendant to provide or ensure adequate data security to protect his PII. Plaintiff Bliss reasonably expected adequate data security as a basic assumption of his implied contractual relationship with NCB and BOA.

221. Plaintiff Bliss's PII was accessed and compromised due to Defendant's failures. He received a Notice Letter dated March 24, 2023 informing him that his 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 were exposed in the Data Breach and that he should take specific steps to protect himself from future identity theft.

222. In response and as a result of the Data Breach, Plaintiff Bliss has spent time and effort researching the Data Breach and reviewing and monitoring his accounts for fraudulent

activity. Plaintiff Bliss estimates that he spent approximately 5 hours monitoring his accounts for suspicious activity and otherwise addressing the Data Breach.

223. On or around April 16, 2023, Plaintiff Bliss received a letter from BOA indicating that someone fraudulently attempted to open up a BOA deposit account in his name.

Plaintiff Michael Teixeira

224. Prior to the Data Breach, Plaintiff Teixeira was a customer of NCB and BOA and provided BOA his PII as a condition to receive banking and/or credit services. NCB serviced Plaintiff Teixeira's BOA account and therefore had access to his PII.

225. Plaintiff Teixeira relied upon Defendant to provide or ensure adequate data security to protect his PII. Plaintiff Teixeira reasonably expected adequate data security as a basic assumption of his implied contractual relationship with NCB and BOA.

226. Plaintiff Teixeira's PII was accessed and compromised due to Defendant's failures. He received a Notice Letter dated March 24, 2023 informing him that his 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 were exposed in the Data Breach and that he should take specific steps to protect himself from future identity theft.

227. In response and as a result of the Data Breach, Plaintiff Teixeira has spent time and effort researching the Data Breach and reviewing and monitoring his accounts for fraudulent activity. Plaintiff Teixeira estimates that he spent approximately 5-10 hours monitoring his accounts for suspicious activity and otherwise addressing the Data Breach.

228. Furthermore, immediately after the Data Breach, Plaintiff Teixeira's password manager software on his iPhone indicated that his passwords associated with his GEICO and ADP

accounts showed that his passwords had "appeared in a data leak" which "puts this account at high risk of compromise."

Plaintiff Diane Ross

229. Prior to the Data Breach, Plaintiff Ross was a customer of NCB. NCB serviced Plaintiff Ross's account that had gone to collections and therefore had access to her PII. Plaintiff Ross received a Data Breach Notification letter purportedly from NCB purportedly pertaining to a Pathward account.

230. Plaintiff Ross relied upon Defendant to provide or ensure adequate data security to protect her PII. Plaintiff Ross reasonably expected adequate data security as a basic assumption of her implied contractual relationship with NCB and Pathward.

231. Plaintiff Ross's PII was accessed and compromised due to Defendant's failures. Plaintiff Ross received a Notice Letter dated May 23, 2023 informing her that her first and last name, and Social Security number were exposed in the Data Breach and that she should take specific steps to protect herself from future identity theft.

232. In response and as a result of the Data Breach, Plaintiff Ross has spent time and effort researching the Data Breach and reviewing and monitoring her accounts for fraudulent activity. Plaintiff Ross estimates that she spent approximately 8-10 hours monitoring her accounts for suspicious activity and otherwise addressing the Data Breach.

233. After the Data Breach occurred Plaintiff Ross's BOA account experienced approximately $1,200 in fraudulent charges.

Plaintiff Jacqueline O'Brien

234. Prior to the Data Breach, Plaintiff O'Brien was a customer of NCB. NCB serviced Plaintiff O'Brien's account that had gone to collections and therefore had access to her PII.

Plaintiff O'Brien received a Data Breach Notification letter purportedly from NCB purportedly pertaining to a Pathward account.

235. Plaintiff O'Brien relied upon Defendant to provide or ensure adequate data security to protect her PII. Plaintiff O'Brien reasonably expected adequate data security as a basic assumption of her implied contractual relationship with NCB and Pathward.

236. Plaintiff O'Brien's PII was accessed and compromised due to Defendant's failures. Plaintiff O'Brien received a Notice Letter dated May 23, 2023 informing her that her first and last name, and Social Security number were exposed in the Data Breach and that she should take specific steps to protect herself from future identity theft.

237. In response and as a result of the Data Breach, Plaintiff O'Brien has spent time and effort researching the Data Breach and reviewing and monitoring her accounts for fraudulent activity. Plaintiff O'Brien estimates that she spent approximately 7 hours monitoring her accounts for suspicious activity and otherwise addressing the Data Breach.

Plaintiff Kelly Matts

238. Prior to the Data Breach, Plaintiff Matts was a customer of NCB. NCB serviced Plaintiff Matts's account that had gone to collections and therefore had access to her PII. Plaintiff Matts received a Data Breach Notification letter purportedly from NCB purportedly pertaining to a Pathward account, however her NCB account pertained to debt she owed from a Rise Credit of California account.

239. Plaintiff Matts relied upon Defendant to provide or ensure adequate data security to protect her PII. Plaintiff Matts reasonably expected adequate data security as a basic assumption of her implied contractual relationship with NCB.

240. Plaintiff Matts's PII was accessed and compromised due to Defendant's failures. Plaintiff Matts received a Notice Letter dated May 23, 2023 informing her that her first and last name, and Social Security number were exposed in the Data Breach and that she should take specific steps to protect herself from future identity theft.

241. In response and as a result of the Data Breach, Plaintiff Matts has spent time and effort researching the Data Breach and reviewing and monitoring her accounts for fraudulent activity. Plaintiff Matts estimates that she spent approximately several hours monitoring her accounts for suspicious activity and otherwise addressing the Data Breach.

242. Furthermore, Plaintiff Matts's credit monitoring/identity theft monitoring software alerted and revealed that her Personal Information is now on the dark web.

Plaintiff Micael Martin

243. Prior to the Data Breach, Plaintiff Micael Martin was a customer of NCB. NCB serviced Plaintiff Martin's account that had gone to collections and therefore had access to her PII. Plaintiff Martin received a Data Breach Notification letter purportedly from NCB purportedly pertaining to a Pathward account, however her NCB account pertained to debt she owed from a Rise Credit of California account.

244. Plaintiff Martin relied upon Defendant to provide or ensure adequate data security to protect her PII. Plaintiff Martin reasonably expected adequate data security as a basic assumption of her implied contractual relationship with NCB.

245. Plaintiff Martin's PII was accessed and compromised due to Defendant's failures. Plaintiff Martin received a Notice Letter dated May 23, 2023 informing her that her first and last name, and Social Security number were exposed in the Data Breach and that she should take specific steps to protect herself from future identity theft.

246. In response and as a result of the Data Breach, Plaintiff Martin has spent time and effort researching the Data Breach and reviewing and monitoring her accounts for fraudulent activity. Plaintiff Martin estimates that she spent approximately 5 hours monitoring her accounts for suspicious activity and otherwise addressing the Data Breach.

Plaintiff Bryan Woodlow

247. Prior to the Data Breach, Plaintiff Bryan Woodlow was a customer of NCB. NCB serviced Plaintiff Woodlow's account that had gone to collections and therefore had access to his PII. Plaintiff Woodlow received a Data Breach Notification letter purportedly from NCB purportedly pertaining to a Pathward account.

248. Plaintiff Woodlow relied upon Defendant to provide or ensure adequate data security to protect his PII. Plaintiff Woodlow reasonably expected adequate data security as a basic assumption of his implied contractual relationship with NCB.

249. Plaintiff Woodlow's PII was accessed and compromised due to Defendant's failures. Plaintiff Woodlow received a Notice Letter dated May 23, 2023 informing him that his first and last name, and Social Security number were exposed in the Data Breach and that he should take specific steps to protect himself from future identity theft.

Plaintiff Christine Neubauer

250. Prior to the Data Breach, Plaintiff Christine Neubauer was a customer of NCB, though, to the best of her knowledge, Plaintiff has never had any account sent to NCB for collections. Plaintiff believes her PII to have been sent to Defendant in error. Plaintiff Neubauer received a Data Breach Notification letter purportedly from NCB purportedly pertaining to a Pathward account.

251. Plaintiff Neubauer relied upon Defendant to provide or ensure adequate data security to protect her PII. Plaintiff Neubauer reasonably expected adequate data security as a basic assumption of her implied contractual relationship with NCB.

252. Plaintiff Neubauer's PII was accessed and compromised due to Defendant's failures. Plaintiff Neubauer received a Notice Letter on or around March 28, 2023 informing her that her first and last name, and Social Security number were exposed in the Data Breach and that she should take specific steps to protect herself from future identity theft.

253. As a result of the breach, she must now and has been taking extra steps to ensure that her PII is not used fraudulently, including putting a credit freeze on her account. These steps have taken additional time and effort on her behalf.

254. Further, Plaintiff is at an imminent and heightened risk of increased further harm from the loss of her PII, and she must remain vigilant for years to come to ensure that her PII is not used to harm her.

255. Plaintiffs and Class Members suffered actual damages as a result of the failures of Defendant to adequately protect the sensitive information entrusted to it, including, without limitation, experiencing fraud or attempted fraud, purchasing credit monitoring as a result of the breach, time related to monitoring their accounts for fraudulent activity, exposure to increased and imminent risk of fraud and identity theft, the loss in value of their personal information, and other economic and non-economic harm. Plaintiffs and Class Members will now be forced to expend additional time to review their credit reports and monitor their accounts for fraud or identity theft.

256. As a result of the Data Breach, Plaintiffs and Class Members have been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages

for years to come. Such risk is certainly real and impending and is not speculative given the highly sensitive nature of the PII compromised by the Data Breach.

CLASS ACTION ALLEGATIONS

257. Plaintiffs brings this case as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and (b)(3) on behalf of the following Nationwide Class:

> All persons in the United States whose PII was compromised in the Data Breach first made public by NCB in March 2023, and as supplemented by NCB in May 2023 (the "Nationwide Class").

258. Plaintiffs reserve the right to modify, expand or amend the above Nationwide Class definition or to seek certification of a class or classes defined differently than above before any court determines whether certification is appropriate following discovery.

STATE SUBCLASSES

259. Plaintiffs brings this case as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and (b)(3) on behalf of the following State Subclasses:

Florida Subclass

> All persons in Florida whose PII was compromised in the Data Breach first made public by NCB in March 2023, and as supplemented by NCB in May 2023 (the "Florida Subclass").

California Subclass

> All persons in California whose PII was compromised in the Data Breach first made public by NCB in March 2023, and as supplemented by NCB in May 2023 (the "California Subclass").

New York

> All persons in New York whose PII was compromised in the Data Breach first made public by NCB in March 2023, and as supplemented by NCB in May 2023 (the "New York Subclass").

Texas

All persons in Texas whose PII was compromised in the Data Breach first made public by NCB in March 2023, and as supplemented by NCB in May 2023 (the "Texas Subclass").

Georgia

All persons in Georgia whose PII was compromised in the Data Breach first made public by NCB in March 2023, and as supplemented by NCB in May 2023 (the "Georgia Subclass").

Oregon

All persons in Oregon whose PII was compromised in the Data Breach first made public by NCB in March 2023, and as supplemented by NCB in May 2023 (the "Oregon Subclass").

Massachusetts

All persons in Massachusetts whose PII was compromised in the Data Breach first made public by NCB in March 2023, and as supplemented by NCB in May 2023 (the "Massachusetts Subclass").

260. Plaintiffs reserve the right to modify, expand or amend the above Florida, California, New York, Texas, Georgia, Oregon, and Massachusetts Subclass definitions or to seek certification of a class or classes defined differently than above before any court determines whether certification is appropriate following discovery.

261. Certification of Plaintiffs' claims for class-wide treatment are appropriate because all elements of Fed. R. Civ. P. 23(a) and (b)(2)-(3) are satisfied. Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

262. **Numerosity**. All requirements of Fed. R. Civ. P. 23(a)(1) are satisfied. The Members of the Nationwide Class and State Subclasses are so numerous and geographically dispersed that individual joinder of all Class and Subclass Members is impractical. While Plaintiffs

are informed and believe that there are likely millions of thousands of Members of the Classes, the precise number of Class and Subclass Members is unknown to Plaintiffs. According to information released by the Maine Attorney General, the number of persons affected is approximately 1,582,811 between BOA (494,969) and Pathward and other institutions (1,087,842).

263. Class Members may be identified through objective means. Indeed, Defendant has largely done so already. Class Members may be notified of the pendency of this action by recognized, court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

264. **Commonality and Predominance**. All requirements of Fed. R. Civ. P. 23(a)(2) and 23(b)(3) are satisfied. This action involves common questions of law and fact, which predominate over any questions affecting individual Class Members, including, without limitation:

a. Whether Defendant engaged in active misfeasance and misconduct alleged herein;

b. Whether Defendant owed a duty to Class Members to safeguard their sensitive personal information;

c. Whether Defendant breached their duty to Class Members to safeguard their sensitive personal information;

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

e. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of the Data Breach;

f. Whether Defendant's failure to provide adequate security proximately caused Plaintiffs' and Class Members' injuries; and

g. Whether Plaintiffs and Class Members are entitled to declaratory and injunctive relief.

265. **Typicality.** All requirements of Fed. R. Civ. P. 23(a)(3) are satisfied. Plaintiffs' claims are typical of the claims of all Class and Subclass Members because Plaintiffs, like other Class and Subclass Members, suffered theft of their sensitive personal information in the Data Breach.

266. **Adequacy of Representation.** All requirements of Fed. R. Civ. P. 23(a)(4) are satisfied. Plaintiffs are adequate Class representatives because they are Members of the Class and State Subclasses their interests do not conflict with the interests of other Class and Subclass Members that they seek to represent. Plaintiffs are committed to pursuing this matter for the Class with the Class's collective best interest in mind. Plaintiffs have retained counsel competent and experienced in complex class action litigation of this type and Plaintiffs intend to prosecute this action vigorously. Plaintiffs and their counsel will fairly and adequately protect the Class's interests.

267. **Predominance and Superiority.** All requirements of Fed. R. Civ. P. 23(b)(3) are satisfied. As described above, common issues of law or fact predominate over individual issues. Resolution of those common issues in Plaintiffs' case will also resolve them for the Class's claims. In addition, a class action is superior to any other available means for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiffs and other Class Members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for Members of the Class to individually seek redress for Defendant's wrongful conduct. Even if Class

Members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

268. **Cohesiveness**. All requirements of Fed. R. Civ. P. 23(b)(2) are satisfied. Defendant has acted, or refused to act, on grounds generally applicable to the Nationwide Class and Subclasses such that final declaratory or injunctive relief is appropriate.

269. Plaintiffs reserve the right to revise the foregoing class allegations and definitions based on newly learned facts or legal developments that arise following additional investigation, discovery, or otherwise.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(By all Plaintiffs on behalf of the Nationwide Class (or, alternatively, each of the State Subclasses) against Defendant)

270. Plaintiffs re-allege and incorporate by reference all preceding allegations as if fully set forth herein.

271. Defendant obtained, collected, transferred and stored Plaintiffs' and Class Members' PII in connection with its debt collection and accounts management operations.

272. By collecting and maintaining sensitive personal information, Defendant had a common law duty of care to use reasonable means to secure and safeguard the sensitive personal information and to prevent disclosure of the information to unauthorized individuals. Defendant's duty included a responsibility to implement processes by which it could detect a data breach of this type and magnitude in a timely manner.

273. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with the various statutory requirements, regulations, and other notices described above.

274. Defendant was in a position to ensure that its servers and systems were sufficient to protect against the foreseeable risk that a data breach could occur that would result in substantial harm to Plaintiffs and Class Members.

275. NCB was subject to an "independent duty" untethered to any contract between Plaintiffs and Class Members and Defendant.

276. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect customers' sensitive personal information. Defendant's negligent acts and omissions include, but are not limited to, the following:

a. failure to employ systems and educate employees and others to protect against malware and/or ransomware;
b. failure to comply with industry standards for software and server security;
c. failure to track and monitor access to its network and personal information;
d. failure to limit access to those with a valid purpose;
e. failure to adequately staff and fund its data security operation;
f. failure to remove, delete, or destroy highly sensitive personal information of consumers that is no longer being used for any valid business purpose;
g. failure to use due care in hiring, promoting, and supervising those responsible for its data security operations; and
h. failure to recognize that hackers were stealing personal information from its network while the Data Breach was taking place.

277. It was foreseeable to Defendant that a failure to use reasonable measures to protect its customers' sensitive personal information could result in injury to consumers. Further, actual and attempted breaches of data security were reasonably foreseeable to Defendant given the known frequency of data breaches and various warnings from industry experts.

278. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members sustained damages as alleged herein. Plaintiffs and Class Members are entitled to actual, compensatory, consequential, incidental, punitive, and nominal damages, in an amount to be proven at trial.

279. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, among other things: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide free credit monitoring and identity theft insurance to all Class Members for a time period to be determined at trial.

COUNT II
FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT
Fla. Stat. §§ 501.201, *et seq.*
(By Plaintiff Neubauer and the Florida Subclass against Defendant)

280. Plaintiffs re-allege and incorporate by reference all preceding allegations as if fully set forth herein.

281. Plaintiff Neubauer and Florida Subclass Members are "consumers" as defined by Fla. Stat. § 501.203.

282. Defendant advertised, offered, or sold goods or services in Florida and engaged in trade or commerce directly or indirectly affecting the people of Florida.

283. Defendant engaged in unconscionable, unfair, and deceptive acts and practices in the conduct of trade and commerce, in violation of Fla. Stat. § 501.204(1), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Neubauer and Florida Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of 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 Neubauer and Florida Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, F.S.A. § 501.171(2), which was a direct and proximate cause of the Data Breach;

d. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Neubauer and Florida Subclass Members' PII; and

e. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff Neubauer and Florida Subclass Members' PII including by implementing and maintaining reasonable security measures.

284. These omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' PII. Plaintiff Neubauer and Florida Subclass Members would have discontinued Defendant's access to their PII had this information been disclosed.

285. As a direct and proximate result of Defendant's unconscionable, unfair, and deceptive acts and practices, Plaintiff Neubauer and Florida Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Defendant's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

286. Plaintiff Neubauer and Florida Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages under Fla. Stat. § 501.211; declaratory and injunctive relief; reasonable attorneys' fees and costs, under Fla. Stat. § 501.2105(1); and any other relief that is just and proper.

COUNT III
DECLARATORY AND INJUNCTIVE RELIEF
(By all Plaintiffs on behalf of the Nationwide Class against Defendant)

287. Plaintiffs re-allege and incorporate by reference all preceding allegations as if fully set forth herein.

288. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the statutes described in this Complaint.

289. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and statutory duties to reasonably safeguard its customers' sensitive personal information and whether Defendant is currently maintaining data

security measures adequate to protect Plaintiffs and Class Members from further data breaches. Plaintiffs alleges that Defendant's data security practices remain inadequate.

290. Plaintiffs and Class Members continue to suffer injury as a result of the compromise of their sensitive personal information and remain at imminent risk that further compromises of their personal information will occur in the future.

291. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that Defendant continues to owe a legal duty to secure consumers' sensitive personal information, to timely notify consumers of any data breach, and to establish and implement data security measures that are adequate to secure customers' sensitive personal information.

292. The Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect consumers' sensitive personal information.

293. If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable injury, for which they lack an adequate legal remedy. The threat of another data breach is real, immediate, and substantial. If another data breach at NCB occurs, Plaintiffs and Class Members will not have an adequate remedy at law because not all of the resulting injuries are readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

294. The hardship to Plaintiffs and Class Members if an injunction does not issue greatly exceeds the hardship to Defendant if an injunction is issued. If another data breach occurs, Plaintiffs and Class Members will likely be subjected to substantial risk of identity theft and other damages. On the other hand, the cost to Defendant of complying with an injunction by employing

reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

295. Issuance of the requested injunction will serve the public interest by preventing another data breach at NCB, thus eliminating the additional injuries that would result to Plaintiffs and the hundreds of thousands of consumers whose confidential information would be further compromised.

REQUEST FOR RELIEF

Plaintiffs, on behalf of all others similarly situated, requests that the Court enter judgment against Defendant including the following:

1. Determining that this matter may proceed as a class action and certifying the Class asserted herein;

2. Appointing Plaintiffs as representatives of the applicable Class and appointing Plaintiffs' counsel as Class Counsel;

3. An award to Plaintiffs and the Class of actual, compensatory, consequential, incidental, punitive, nominal statutory, double, treble, and restitution damages, in an amount to be proven at trial as set forth above;

4. Ordering injunctive relief requiring Defendant to, among other things: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; (iii) provide lifetime credit monitoring and identity theft insurance to all Class Members; (iv) timely notify consumers of any future data breaches; and (v) delete or destroy any legacy consumer data that it is not necessary to keep for business purposes;

5. Entering a declaratory judgment stating that Defendant owes a legal duty to secure customers' sensitive personal information, to timely notify consumers of any data breach, and to

establish and implement data security measures that are adequate to secure sensitive personal information;

6. An award of attorneys' fees, costs, and expenses, as provided by law or equity;

7. An award of pre-judgment and post-judgment interest, as provided by law or equity; and

8. Such other relief as the Court may allow.

DEMAND FOR JURY TRIAL

Plaintiffs demands a trial by jury for all issues so triable.

DATED: May 1, 2025

Respectfully submitted,

/s/ Benjamin F. Johns

Benjamin F. Johns
PA ID# 201373
Samantha E. Holbrook
PA ID# 311829
SHUB JOHNS & HOLBROOK LLP
Four Tower Bridge
200 Barr Harbor Drive, Suite 400
Conshohocken, PA 19428
Telephone: (610) 477-8380
Email: bjohns@shublawyers.com
Email: sholbrook@shublawyers.com

Joseph M. Lyon (admitted *pro hac vice*)
THE LYON LAW FIRM, LLC
2754 Erie Avenue
Cincinnati, OH 45208
Telephone: (513) 381-2333
Email: jlyon@thelyonfirm.com

Christian Levis (admitted *pro hac vice*)
Amanda G. Fiorilla (admitted *pro hac vice*)
LOWEY DANNENBERG, P.C.
44 South Broadway, Suite 1100
White Plains, NY 10601
Telephone: (914) 997-0500
Email: clevis@lowey.com
Email: afiorilla@lowey.com

Anthony M. Christina
PA ID# 322528
LOWEY DANNENBERG, P.C.
One Tower Bridge
100 Front Street, Suite 520
West Conshohocken, PA 19428
Telephone: (215) 399-4770
Email: achristina@lowey.com

Interim Co-Lead Class Counsel

Charles E. Schaffer
PA ID# 76259
LEVIN SEDRAN & BERMAN
510 Walnut Street, Suite 500
Philadelphia, PA 19106
Telephone: (215) 592-1500
Email: cschaffer@lfsblaw.com

Plaintiffs' Liaison Counsel

Terence R. Coates (admitted *pro hac vice*)
MARKOVITS, STOCK & DEMARCO, LLC
119 E. Court Street, Suite 530
Cincinnati, OH 45202
Telephone: 855-843-5442
Email: TCoates@msdlegal.com

Joseph B. Kenney
PA ID# 316557
SAUDER SCHELKOPF LLC
1109 Lancaster Avenue
Berwyn, PA 19312
Telephone: (610) 200-0583
Email: jbk@sstriallawyers.com

Danielle L. Perry (admitted *pro hac vice*)
MASON LLP
5335 Wisconsin Avenue, N.W., Suite 640
Washington, D.C. 20015
Telephone: (202) 640-1168
Email: dperry@masonllp.com

Plaintiffs' Steering Committee

CERTIFICATE OF SERVICE

I hereby certify that on May 1, 2025, I electronically filed the foregoing Amended Consolidated Class Action Complaint. Notice of this filing will be sent by electronic mail to all parties who filed a notice of appearance by operation of the Court's electronic filing system. Parties may access this filing through the Court's CM/ECF system.

/s/ Benjamin F. Johns
Benjamin F. Johns