David Hilton Wise, Esq.
Nevada Bar No. 11014
**WISE LAW FIRM, PLC**
421 Court Street
Reno, Nevada, 89501
(775) 329-1766
(703) 934-6377
dwise@wiselaw.pro

*Counsel for Plaintiff(s) and the Proposed Class*

[Additional counsel appear on signature page]

**UNITED STATES DISCTRICT COURT**
**DISTRICT OF NEVADA**

| | |
|---|---|
| JANINE BIVONA-TRUMAN, individually and on behalf of all others similarly situated,<br><br>Plaintiff(s),<br><br>v.<br><br>NATIONS DIRECT MORTGAGE, LLC,<br><br>Defendant(s). | Case No.:<br><br>**CLASS ACTION COMPLAINT**<br><br>**Case No. 24-595**<br><br>**JURY TRIAL DEMANDED** |

## CLASS ACTION COMPLAINT

Plaintiff(s) Janine Bivona-Truman ("Plaintiff(s)"), individually and on behalf of all persons who are similarly situated, bring this action against Defendant Nations Direct Mortgage, LLC ("Nations Direct" or "Defendant") to obtain damages, restitution, and injunctive relief from Defendant. Plaintiff(s) make the following allegations upon information and belief, except as to their own actions, the investigation of their counsel, and facts that are a matter of public record.

## NATURE OF THE ACTION

1. This class action arises out of the recent data security incident and data breach that was perpetrated against Defendant Nations Direct (the "Data Breach"), which held in its possession certain personally identifiable information ("PII") and protected health information ("PHI") (collectively, "the Private Information") of Plaintiff(s) and other individuals associated with Defendant Nations Direct, the putative Class Members ("Class"). These individuals, upon information and belief, include mortgagors and employees with Nations Direct. This Data Breach occurred on or about December 30, 2023.

2. The Private Information compromised in the Data Breach included certain personally identifiable information including, but not limited to: full names, addresses, Social Security numbers, and unique Nations Direct loan numbers.

3. The Private Information was compromised in what Nations Direct refers to as an "incident" in which there was "unauthorized access to certain systems within its computer information technology network." In other words, the cybercriminals intentionally targeted Nations Direct for the highly sensitive Private Information it stores on its computer network, attacked the insufficiently secured network, then had unfettered access to Defendant's computer network, exfiltrating highly sensitive PII, including Social Security numbers. As a result, the Private Information of Plaintiff(s) and Class remains in the hands of those cyber-criminals.[1]

4. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect individuals' Private Information with which it was entrusted with for mortgage lending purposes or employment.

[1] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/1ee1929d-4e0f-4b9e-b202-59cb6d9e567d.shtml (*see* link to notice letter); *see also* Plaintiff(s)' Notice Letter, attached as Exhibit A.

5. Plaintiff(s) bring this class action lawsuit on behalf of themselves and all citizens who are similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained, for failing to promptly detect the cyber attack, and for failing to provide timely and adequate notice to Plaintiff(s) and other Class Members that their information had been subject to the unauthorized access and exfiltration by cybercriminals.

6. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant Nations Direct's computer network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiff(s)' and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

7. Defendant disregarded the rights of Plaintiff(s) and Class Members by, inter alia, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Plaintiff(s)' and Class Members' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiff(s) and Class Members with prompt and full notice of the Data Breach.

8. In addition, Defendant Nations Direct failed to properly monitor the computer network and systems that housed the Private Information. Had Nations Direct properly monitored its property, it would have discovered the intrusion sooner rather than allowing cybercriminals almost a year of unimpeded access to the PII mof Plaintiff(s) Class Members.

9. Plaintiff(s)' and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Defendant Nations Direct collected and maintained is now in the hands of cyber criminals, and their Private Information has been sold or is in imminent risk of being sold on the Dark Web.

10. Armed with the Private Information accessed in the Data Breach, cyber criminals can commit a variety of crimes including, e.g., opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, filing false medical claims using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

11. As a result of the Data Breach, Plaintiff(s) and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff(s) and Class Members must now and for years into the future closely monitor their financial accounts to guard against identity theft.

12. Plaintiff(s) and Class Members have or soon may incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

13. Through this Complaint, Plaintiff(s) seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data Breach.

14. Accordingly, Plaintiff(s) bring this action against Defendant seeking redress for its unlawful conduct, and asserting claims for: negligence, breach of implied contract, unjust enrichment, and declaratory relief, seeking redress for Nations Direct's unlawful conduct.

15. Plaintiff(s) seek remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, as well as long-term and adequate credit monitoring services funded by Defendant.

## PARTIES

16. Plaintiff Janine Bivona-Truman is and at all times mentioned herein was an individual citizen of the State of Nevada, and she applied for employment with Nations Direct. Ms. Janine Bivona-Truman received notice of the Data Breach dated February 28, 2024 attached in Exhibit A.

17. Defendant Nations Direct Mortgage, LLC is a limited liability company, with its principal place of business located at 2475 Village View Drive, Suite 100, Henderson., Nevada 89074.

## JURISDICTION AND VENUE

18. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

19. The Court has general personal jurisdiction over Defendant because, personally or through its agents, Defendant operates, conducts, engages in, or carries on a business or business

venture in this State; it is registered with the Secretary of State as a foreign limited liability compaby; it maintains its headquarters in Nevada; and committed tortious acts in Nevada.

20. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because it is the district within which Nations Direct has the most significant contacts.

## FACTUAL ALLEGATIONS

### *Defendant's Business*

21. Established in 2007, Defendant Nations Direct services the residential mortgage industry as a wholesale lending partner.[2]

22. Nations Direct claims to be a "direct seller" to Fannie Mae, Fredde Mac, and Ginne Mae, which allows them to "to provide a wide array of flexible mortgage products that suit the specific needs of you and your borrowers.[3]

23. Nations Direct claims that it "strives to manifest lasting prosperity not only for our partners, but for our borrowers, our communities, our industry and our nation."[4]

24. Nations Direct "specializes in residential lending, including FHA, VA, Conventional and Non-QM loan products. We originate loans through an exclusive network of Broker/Banker partners."[5]

25. For the purposes of this Class Action Complaint, all of Nations Direct's associated locations and subentities will be referred to collectively as "Nations Direct."

26. In the ordinary course of receiving lending services from Defendant Nations Direct, each individual seeking a mortgage and other services or employment must provide (and

[2] https://myndm.com/about/; https://www.linkedin.com/company/myndm/ (last accessed Mar. 27, 2024).
[3] *Id.*
[4] *Id.* (last accessed Mar. 27, 2024).
[5] https://www.facebook.com/myNDM/about_details (last accessed Mar. 27, 2024).

Plaintiff(s) did provide) Defendant Nations Direct with sensitive, personal, and private information, such as their:

- Name, address, phone number, and email address;
- Employment information;
- Financial account or payment information;
- Date of birth;
- Social Security number;
- Demographic information;
- Driver's license or state or federal identification;

27. Upon information and belief, Nations Direct has a privacy policy that is provided to every applicant for services both prior to receiving assistance and upon request.[6]

28. Defendant Nations Direct agreed to and undertook legal duties to maintain the protected personal information entrusted to it by Plaintiff(s) and Class Members safely, confidentially, and in compliance with all applicable laws, including the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45 and the California Online Privacy Protection Act.

29. Yet, through its failure to properly secure the Private Information of Plaintiff(s) and Class, Nations Direct has not adhered to its own promises of individuals' rights.[7]

30. The Private Information held by Defendant Nations Direct in its computer system and network included the highly sensitive Private Information of Plaintiff(s) and Class Members.

[6] https://myndm.com/privacy-policy/ (last accessed Mar. 27, 2024).
[7] https://www.kimco.com/privacy-policy/ (last accessed Mar. 27, 2024).

***The Data Breach***

31. A Data Breach occurs when cyber criminals intend to access and steal Private Information that has not been adequately secured by a business entity like Nations Direct.

32. According to it's website notice and February 28, 2024 dated "Notice of Data Breach" that Nations Direct sent to Plaintiff(s), "[o]n or about December 30, 2023, Nations Direct became aware of unauthorized access to certain systems within its computer information technology network. [8]

33. Nations Direct ultimately determined that its computer systems had been compromised by an unauthorized third party. Nations Direct claims they are unable to confirm all of the information that was specifically impacted.

34. It claims "Based on our investigation, we understand that names, address, social security number, and unique Nations Direct loan numbers may have been obtained by the unauthorized third party bad actor."[9]

35. Nations Direct failed to notify Plaintiff and class members of the data breach for nearly 6 whole months.

36. Yet, Nations Direct claims "[y]our [p]rivacy [m]atters to [u]s..." However, it failed to notify victims of the breach for about 2 months, while these cybercriminals were able to have free reign with the stolen data.[10]

[8] *See* Notice Letter, Exhibit A; https://myndm.com/notice-of-potential-data-breach/ (last accessed Mar. 27, 2024).
[9] *Id*.
[10] *Id.;* https://myndm.com/privacy-policy/ (last accessed Mar. 27, 2024).

37. Defendant had obligations created by the s FTCA, contract, industry standards, state law, common law, and representations made to Plaintiff(s) and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

38. Plaintiff(s) and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

***The Data Breach was a Foreseeable Risk of which Defendant was on Notice.***

39. It is well known that PII, including Social Security numbers in particular, is a valuable commodity and a frequent, intentional target of cyber criminals. Organizations that collect such information, including Nations Direct, are well-aware of the risk of being targeted by cybercriminals.

40. Individuals place a high value not only on their PII, but also on the privacy of that data. Identity theft causes severe negative consequences to its victims, as well as severe distress and hours of lost time trying to fight against the impact of identity theft.

41. A data breach increases the risk of becoming a victim of identity theft. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice, "[a] direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are

not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss."[11]

42. Individuals, like Plaintiff(s) and Class Members, are particularly concerned with protecting the privacy of their Social Security numbers, which are the key to stealing any person's identity and is likened to accessing your DNA for hacker's purposes.

43. Data Breach victims suffer long-term consequences when their Social Security numbers are taken and used by hackers. Even if they know their Social Security numbers are being misused, Plaintiff(s) and Class Members cannot obtain new numbers unless they become a victim of Social Security number misuse.

44. The Social Security Administration has warned that "a new number probably won't 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) 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 won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same."[12]

45. In 2021, there were a record 1,862 data breaches last year, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[13]

46. Additionally in 2021, there was a 15.1% increase in cyberattacks and data breaches since 2020. Over the next two years, in a poll done on security executives, they have predicted an

[11] "Victims of Identity Theft, 2018," U.S. Dep't of Justice (Apr. 2021, NCJ 256085) available at: https://bjs.ojp.gov/content/pub/pdf/vit18.pdf (last accessed Mar. 27, 2024).
[12] https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Mar. 27, 2024).
[13] https://www.cnet.com/tech/services-and-software/record-number-of-data-breaches-reported-in-2021-new-report-says/ (last accessed Mar. 27, 2024).

increase in attacks from "social engineering and ransomware" as nation-states and cybercriminals grow more sophisticated. Unfortunately, these preventable causes will largely come from "misconfigurations, human error, poor maintenance, and unknown assets."[14]

47. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, and hopefully can ward off a cyberattack.

48. According to an FBI publication, "[r]ansomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return. Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data."[15] This publication also explains that "[t]he FBI does not support paying a ransom in response to a ransomware attack. Paying a ransom doesn't guarantee you or your organization will get any data back. It also encourages perpetrators to target more victims and offers an incentive for others to get involved in this type of illegal activity."[16]

49. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its own acknowledgment of its duties to keep PII private and secure, Nations Direct failed to take appropriate steps to protect the PII of Plaintiff(s) and the proposed Class from being compromised.

***Defendant Fails to Comply with FTC Guidelines.***

50. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices.

[14] https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=176bb6887864 (last accessed Mar. 27, 2024).
[15] https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware (last accessed Mar. 27, 2024).
[16] *Id.*

According to the FTC, the need for data security should be factored into all business decision-making.

51. In October 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[17] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[18]

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

53. The FTC has brought enforcement actions against organizations like Nations Direct's for failing to adequately and reasonably protect individuals' data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission

[17] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Mar. 27, 2024).
[18] *Id.*

Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

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

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

56. Defendant was at all times fully aware of its obligation to protect the Private Information of individuals seeking or receiving services. Defendant was also aware of the significant repercussions that would result from its failure to do so.

***Defendant Fails to Comply with Industry Standards.***

57. As shown above, experts studying cyber security routinely identify social service providers as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

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

59. Other best cybersecurity practices that are standard in the service industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

60. Defendant 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.

61. These frameworks are existing and applicable industry standards in the healthcare industry, yet Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

***Defendant has Breached its Obligations to Plaintiff(s) and Class.***

62. Defendant breached its obligations to Plaintiff(s) and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard Nations Direct's computer systems and Class Members' data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect Class Members' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to ensure that vendors with access to Defendant's data employed reasonable security procedures;

e. Failing to ensure the confidentiality and integrity of electronic Private Information it created, received, maintained, and/or transmitted;

f. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PII to allow access only to those persons or software programs that have been granted access rights;

g. Failing to implement policies and procedures to promptly prevent, detect, contain, and correct security violations;

h. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports;

i. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic data;

j. Failing to protect against reasonably anticipated uses or disclosures of electronic PII that are not permitted under the privacy rules regarding individually identifiable health information;

l. Failing to train all members of Defendant's workforce effectively on the policies and procedures regarding PII as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of PII; and/or

m. Failing to render the electronic PII it maintained unusable, unreadable, or indecipherable to unauthorized individuals.

63. As the result of maintaining its computer systems in manner that required security upgrading, inadequate procedures for handling emails containing ransomware or other malignant computer code, and inadequately trained employees who opened files containing the ransomware

virus, Defendant negligently and unlawfully failed to safeguard Plaintiff(s)' and Class Members' Private Information.

64. Accordingly, as outlined below, Plaintiff(s) and Class Members now face an increased risk of fraud and identity theft.

***Data Breaches Put Consumers at an Increased Risk Of Fraud and Identify Theft.***

65. Data Breaches such as the one experienced by Nations Direct's customers are especially problematic because of the disruption they cause to the overall daily lives of victims affected by the attack.

66. In 2019, the United States Government Accountability Office released a report addressing the steps consumers can take after a data breach.[19] Its appendix of steps consumers should consider, in extremely simplified terms, continues for five pages. In addition to explaining specific options and how they can help, one column of the chart explains the limitations of the consumers' options. *See* GAO chart of consumer recommendations, reproduced and attached as Exhibit B. It is clear from the GAO's recommendations that the steps Data Breach victims (like Plaintiff(s) and Class) must take after a breach like Nations Direct's are both time consuming and of only limited and short term effectiveness.

67. The GAO has long recognized that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record," discussing the same in a 2007 report as well ("2007 GAO Report").[20]

[19] https://www.gao.gov/assets/gao-19-230.pdf (last accessed Mar. 27, 2024). *See* attached as Ex. B.

[20] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Gov't Acct. Off. (June 2007), https://www.gao.gov/new.items/d07737.pdf (last accessed Jan. 2, 2024) ("2007 GAO Report").

68. The FTC, like the GAO (see Exhibit B), recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[21]

69. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

70. 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.

71. Theft of Private Information is also gravely serious. Private Information is a valuable property right.[22]

72. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which has conducted studies 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.

[21] *See* https://www.identitytheft.gov/Steps (last accessed Mar. 27, 2024).
[22] *See, e.g.,* John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3–4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

> As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

*See* 2007 GAO Report, at p. 29.

73. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

74. There is a strong probability that the entirety of the stolen information has been dumped on the black market or will be dumped on the black market, meaning Plaintiff(s) and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff(s) and Class Members must vigilantly monitor their personal, financial, and medical accounts for many years to come.

75. Furthermore, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[23] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[24] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

76. Moreover, it is not an easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and

[23] *Identity Theft and Your Social Security Number* at 1, Soc. Sec. Admin. (2018), Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Mar. 27, 2024).
[24] *Id.* at 4.

evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[25]

77. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[26]

78. In recent years, medical and financial service industries have experienced disproportionally higher numbers of data theft events than other industries. Defendant therefore knew or should have known this and strengthened its data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

## PLAINTIFF(S)' EXPERIENCE

***Plaintiff Janine Bivona-Truman***

79. Plaintiff Janine Bivona-Truman is and at all times mentioned herein was an individual citizen residing in the State of Nevada.

80. In the past, Plaintiff Bivona-Truman was an employee at Nations Direct, at which time she provided Nations Direct with her full name, date of birth, Social Security number, state

[25] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last accessed Mar. 27, 2024).

[26] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Mar. 27, 2024).

identification/driver's license number, and government identification number, as well as other information required on Nations Direct's forms.

81. Plaintiff Bivona-Truman received a Notice of Data Breach Letter, related to Nations Direct's Data Breach that is dated February 28, 2024. *See* Exhibit A.

82. The Notice Letter that Plaintiff Bivona-Truman received indicated that Nations Direct learned of the Data Breach almost 2 months before she was notified. The letter generically informed her that her critical PII was accessed. The letter stated the information included her "name, address, social security number, and unique Nations Direct loan number." Ex. A.

83. Since the Data Breach, Plaintiff has been notified that her date of birth, passwords, and social security number has been found on the dark web. Additionally, Someone hacked into Plaintiff's social media accounts and locked her out of Instagram and Facebook. She has been in contact with Facebook and Instagram about the issues.

84. Since the Data Breach, Plaintiff Bivona-Truman began receiving an excessive number of spam calls and emails on the same contact information as she used at Nations Direct. Once she received the Notice Letter, and given the timing of the Data Breach, she believes that the calls and emails are likely to be related to her stolen PII.

85. Plaintiff Bivona-Truman reasonably believes that her Private Information was sold on the Dark Web as a part of this Data Breach. As a result of this breach, Plaintiff Bivona-Truman has taken efforts to mitigate the impacts of identity theft and fraud by closely monitoring her credit with the help of her monthly paid credit monitoring subscription for $29.99, changing her passwords, freezing her credit, contacting credit bureaus and contacting an attorney for help.

86. Since the Data Breach, Plaintiff Bivona-Truman monitors her financial accounts for about an two to three hours per week. This is more time than she spent prior to learning of the

Nations Direct's Data Breach. Having to do this every week not only wastes her time as a result of Nations Direct's negligence, but it also causes her great concern. Furthermore, Nations Direct specifically said she and Class members should expend this time as its recommendation about steps they should take after its Data Breach.

87. Plaintiff Bivona-Truman is alarmed and very concerned that her Private Information is in the hands of cybercriminals, and especially because the stolen information includes her Social Security number. She is aware that cybercriminals often sell Private Information, and that hers could be abused months or even years after this Data Breach.

88. Had Plaintiff Bivona-Truman been aware that Nations Direct's computer systems were not secure, she would not have entrusted Nations Direct with her Private Information.

**PLAINTIFF(S)' AND CLASS MEMBERS' INJURIES**

89. To date, Defendant Nations Direct has done absolutely nothing to compensate Plaintiff(s) and Class Members for the damages they sustained in the Data Breach.

90. Defendant Nations Direct has merely offered two year credit monitoring services through Kroll, a tacit admission that its failure to protect their Private Information has caused Plaintiff(s) and Class great injuries. *See* Ex. A. This one-year limitation is inadequate when victims are likely to face many years of identity theft.

91. Nations Direct's offer fails to sufficiently compensate victims of the Data Breach, who commonly face multiple years of ongoing identity theft, and it entirely fails to provide any compensation for its unauthorized release and disclosure of Plaintiff(s)' and Class Members' Private Information, out of pocket costs, and the time they are required to spend attempting to mitigate their injuries.

92. Furthermore, Defendant Nations Direct's credit monitoring offer and advice (see Ex. A) to Plaintiff(s) and Class Members squarely places the burden on Plaintiff(s) and Class Members, rather than on the Defendant, to investigate and protect themselves from Defendant's tortious acts resulting in the Data Breach. Defendant merely sent instructions to Plaintiff(s) and Class Members about actions they can affirmatively take to protect themselves.

93. Plaintiff(s) and Class Members have been damaged by the compromise and exfiltration of their Private Information in the Data Breach, and by the severe disruption to their lives as a direct and foreseeable consequence of this Data Breach.

94. Plaintiff(s)'and Class Members' Private Information was compromised and exfiltrated by cyber-criminals as a direct and proximate result of the Data Breach.

95. Plaintiff(s) and Class were damaged in that their Private Information is now in the hands of cyber criminals, sold and potentially for sale for years into the future.

96. As a direct and proximate result of Defendant's conduct, Plaintiff(s) and Class Members have been placed at an actual, imminent, and substantial risk of harm from fraud and identity theft.

97. As a direct and proximate result of Defendant's conduct, Plaintiff(s) and Class Members have been forced to expend time dealing with the effects of the Data Breach.

98. Plaintiff(s) and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft. Plaintiff(s) and Class Members have or may in the near future incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

99. Plaintiff(s) and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff(s) and Class Members.

100. Plaintiff(s) and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

101. Plaintiff(s) and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

102. Plaintiff(s) and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Placing “freezes” and “alerts” with credit reporting agencies;

g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

h. Contacting financial institutions and closing or modifying financial accounts;

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

j. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

k. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

103. Moreover, Plaintiff(s) and Class Members have an interest in ensuring that their Private Information, 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, making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password-protected.

104. Further, as a result of Defendant's conduct, Plaintiff(s) and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

105. Defendant's delay in identifying and reporting the Data Breach caused additional harm. Early notification helps a victim of a Data Breach mitigate their injuries, and in the converse, delayed notification causes more harm and increases the risk of identity theft.

## CLASS ACTION ALLEGATIONS

106. Plaintiff(s) bring this action on behalf of themselves and on behalf of all other persons similarly situated.

107. Plaintiff(s) propose the following Class definition, subject to amendment as appropriate:

> All persons whose Private Information was compromised as a result of the Data Breach discovered by Nations Direct in December 2023 and for which it provided notice in or about February 2024 (the "Class").

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

109. Plaintiff(s) hereby reserve the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

110. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. Upon information and belief the number of Class Members is in excess of **83,108** individuals.

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

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff(s)' and Class Members' Private Information;

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

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

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

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

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

g. Whether computer hackers obtained Class Members' Private Information in the Data Breach;

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

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

j. Whether Defendant's conduct was negligent;

k. Whether Defendant's conduct was per se negligent;

l. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

m. Whether Defendant was unjustly enriched;

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

o. Whether Plaintiff(s) and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

112. Typicality. Plaintiff(s)' claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach.

113. Adequacy of Representation. Plaintiff(s) will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff(s)' counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

114. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff(s) and Class Members, in that all the Plaintiff(s)' and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

115. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for

Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

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

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

a. Whether Defendant failed to timely notify the public of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiff(s) and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

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

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

e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

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

## CAUSES OF ACTION
### First Count
### Negligence
### (On Behalf of Plaintiff(s) and Class Members)

119. Plaintiff(s) re-allege and incorporate the above allegations as if fully set forth herein.

120. Defendant Nations Direct required Plaintiff(s) and Class Members to submit non-public personal information in order to obtain financial or employment services.

121. By collecting and storing this data in Nations Direct's computer property, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a Data Breach.

122. Defendant owed a duty of care to Plaintiff(s) and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

123. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or

affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

124. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

125. Defendant breached its duties, and thus were negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Failure to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to detect in a timely manner that Class Members' Private Information had been compromised;

f. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

g. Failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

126. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach

of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

127. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

128. Plaintiff(s) and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

129. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiff(s) and Class Members in an unsafe and unsecure manner.

130. Plaintiff(s) and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

**Second Count**
**Breach of Implied Contract**
**(On Behalf of Plaintiff(s) and All Class Members)**

131. Plaintiff(s) re-allege the above allegations as if fully set forth herein.

132. Plaintiff and Class Members were required to provide their PII to Defendant as a condition of receiving other services provided by Defendant.

133. Plaintiff and Class Members provided their PII to Defendant or its third-party agents in exchange for Nations Direct's services. In exchange for the PII, Defendant promised to protect their PII from unauthorized disclosure.

134. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiff's and Class Members' Private Information would remain protected.

135. Implicit in the agreement between Plaintiff and Class Members and the Defendant to provide Private Information, was the latter's obligation to: (a) use such Private Information for business purposes only, (b) take reasonable steps to safeguard that Private Information, (c) prevent unauthorized disclosures of the Private Information, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information, (e) reasonably safeguard and protect the Private Information of Plaintiff and Class Members from unauthorized disclosure or uses, (f) retain the Private Information only under conditions that kept such information secure and confidential.

136. When Plaintiff and Class Members provided their Private Information to Defendant as a condition of relationship, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

137. Defendant required Class Members to provide their Private Information as part of Defendant's regular business practices.

138. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

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

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

141. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their Private Information.

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

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

144. Plaintiff and Class Members are also entitled to nominal damages for the breach of implied contract.

145. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate long term credit monitoring to all Class Members for a period longer than the grossly inadequate one-year currently offered.

**Third Count**
**Unjust Enrichment**
**(On Behalf of Plaintiff(s) and All Class Members)**

146. Plaintiff(s) restate and reallege the foregoing paragraphs as if fully set forth herein.

147. Plaintiff and Class Members conferred a monetary benefit on Defendant in the form of the provision of their Private Information and Defendant would be unable to engage in its regular course of business without that Private Information.

148. Defendant appreciated that a monetary benefit was being conferred upon it by Plaintiff and Class Members and accepted that monetary benefit.

149. However, acceptance of the benefit under the facts and circumstances outlined above make it inequitable for Defendant to retain that benefit without payment of the value thereof.

Specifically, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff' and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite data security.

150. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary benefit belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures.

151. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

152. If Plaintiff and Class Members knew that Defendant had not secured their Private Information, they would not have agreed to provide their Private Information to Defendant.

153. Plaintiff and Class Members have no adequate remedy at law.

154. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered or will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover

from identity theft; (vi) the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

155. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

156. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them.

**Fourth Count**
**Declaratory Judgment**
**(On Behalf of Plaintiff(s) and Class Members)**

157. Plaintiff(s) restate and reallege all of the foregoing paragraphs as if fully set forth herein.

158. 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 federal and state statutes described in this Complaint.

159. An actual controversy has arisen in the wake of the Nations Direct data breach regarding its present and prospective common law and other duties to reasonably safeguard its customers' Private Information and whether Nations Direct is currently maintaining data security

measures adequate to protect Plaintiff and Class members from further data breaches that compromise their Private Information.

160. Plaintiff alleges that Nations Direct's data security measures remain inadequate. Plaintiff will continue to suffer injury as a result of the compromise of their Private Information and remain at imminent risk that further compromises of their Private Information will occur in the future.

161. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Nations Direct continues to owe a legal duty to secure consumers' Private Information and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and various state statutes;

b. Nations Direct continues to breach this legal duty by failing to employ reasonable measures to secure consumers' Private Information.

162. The Court also should issue corresponding prospective injunctive relief requiring Nations Direct to employ adequate security protocols consistent with law and industry standards to protect consumers' Private Information.

163. If an injunction is not issued, Plaintiff and Class members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Nations Direct. The risk of another such breach is real, immediate, and substantial. If another breach at Nations Direct occurs, Plaintiff and class members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

164. The hardship to Plaintiff and class members if an injunction does not issue exceeds the hardship to Nations Direct if an injunction is issued. Among other things, if another massive data breach occurs at Nations Direct, Plaintiff and class members will likely be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Nations Direct of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Nations Direct has a pre-existing legal obligation to employ such measures.

165. Issuance of the requested injunction will not do a disservice to the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Nations Direct, thus eliminating the additional injuries that would result to Plaintiffs and the millions of consumers whose Private Information would be further compromised.

## PRAYER FOR RELIEF

WHEREFORE, Plaintiff(s) pray for judgment as follows:

a) For an Order certifying this action as a class action and appointing Plaintiff(s) and their counsel to represent the Class;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff(s)' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff(s) and Class Members;

c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e) Ordering Defendant to pay for not less than ten years of credit monitoring services for Plaintiff(s) and the Class;

f) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g) For an award of punitive damages, as allowable by law;

h) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i) Pre- and post-judgment interest on any amounts awarded; and

j) Such other and further relief as this court may deem just and proper.

**JURY TRIAL DEMANDED**

Plaintiff(s) demand a trial by jury on all claims so triable.

Dated: March 27, 2024

Respectfully submitted,

/s/ David Hilton Wise
David Hilton Wise, Esq.
Nevada Bar No. 11014
**WISE LAW FIRM, PLC**
421 Court Street
Reno, Nevada, 89501
(775) 329-1766
(703) 934-6377
dwise@wiselaw.pro

Gary E. Mason*
Danielle L. Perry*
Lisa A. White*
**MASON LLP**
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015
Tel: (202) 429-2290
Email: gmason@masonllp.com
Email: dperry@masonllp.com
Email: lwhite@masonllp.com

*Counsel for Plaintiff(s) and Putative Class*
**Pro Hac Vice* Application forthcoming

# EXHIBIT A

[redacted]

[redacted]

February 28, 2024

JANINE BIVONA-TRUMAN
[redacted]
LAS VEGAS, NV 89138-[redacted]
[redacted]

Re: **NOTICE OF POTENTIAL DATA BREACH**

Dear Janine Bivona-Truman,

We are writing to notify you of a recent event that may have impacted your personal information as a current or former customer or employee of Nations Direct Mortgage, LLC ("Nations Direct"). As of the date of this notice of data breach, Nations Direct has no indication of any fraudulent use of your personal information as a result of this incident. Nations Direct is providing this notice to you to explain how the company was the victim of a crime by bad actors and the resources we are making available to you in connection therewith.

**What Happened?**

On or about December 30, 2023, Nations Direct became aware of unauthorized access to certain systems within its computer information technology network. Upon becoming aware of the incident, Nations Direct immediately commenced an investigation with the assistance of third-party experts, notified certain law enforcement and governmental authorities, and began taking measures to assess and contain the incident. The incident has been contained.

The investigation has determined that an unauthorized third party obtained access to and potentially removed data of certain individuals from across the country. As part of the review of the potentially impacted data, we and the third party experts retained by us have identified that some of your personal information may have been among that data. It is important to note that we have not identified any fraudulent use of your personal information as a result of this incident.

***What Information Was Involved?***

Based on our investigation, we understand that your name, address, social security number, and unique Nations Direct loan number may have been obtained by the unauthorized third party bad actor.

**What We Are Doing**

Upon learning of the incident, we promptly launched an investigation into the nature and scope of the incident and notified law enforcement. We also took immediate measures to further secure our information systems from further breach.

To help address concerns you may have about this incident, we have secured the services of Kroll to provide identity monitoring services at no cost to you for twenty-four (24) months. Your identity monitoring services include Credit Monitoring, Web Watcher, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and identity Theft Restoration. Additional information describing these services is included below. To activate these services, please take the following steps:

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.
*You have until **June 6, 2024** to activate your identity monitoring services.*
Membership Number: [redacted]

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional information describing your services is included with this letter.

[redacted]

# EXHIBIT B

# Appendix II: What Can Consumers Do After a Data Breach?

Figure 3 below provides information on actions consumers can take to monitor for identity theft or other forms of fraud, protect their personal information, and respond if they have been a victim of identity theft. This information summarizes prior GAO work and comments of academic, consumer organization, industry, and government experts.[1]

[1]GAO, *Identity Theft Services: Services Offer Some Benefits but Are Limited in Preventing Fraud*, GAO-17-254 (Washington, D.C.: Mar. 30, 2017).

**Figure 3: What Can Consumers Do After a Data Breach?**

## Prevent Fraud on New Credit Accounts

| Consumer Option | How This Option Can Help | Consumers Should Be Aware |
|---|---|---|
|  **Place a credit freeze** on credit reports at Equifax, Experian, and TransUnion—the three nationwide consumer reporting agencies. | • Prevents identity thieves from opening new credit accounts in an individual's name—where credit reports are required.<br>• Guardians can place credit freezes for minor children (under age 16) or adults who are incapacitated. | • Consumers must request a freeze at each of the three agencies separately.<br>• Could still cause delays in approval of loans or other credit applications, especially if consumer forgets or loses the personal information number (PIN) the agencies give to consumers to unfreeze their credit reports.<br>• Freezes do not prevent fraud on existing accounts (for example, the use of a stolen credit card number to make charges on a credit card).<br>• Freezes do not prevent other types of harm, such as tax refund or medical identity fraud.<br>• Not all access to credit reports is frozen (for example, still allowed for insurance underwriting and employment background checks).<br>• Credit reports at agencies other than Equifax, Experian, and TransUnion will not be frozen (for example, those used to open utility accounts). |
|  **Place a fraud alert** at the three nationwide consumer reporting agencies, which lasts 1 year and can be renewed. | • Fraud alerts let businesses know that a consumer may have been a victim of fraud.<br>• Businesses must take extra steps to verify the identity of the individual seeking to open accounts.<br>• Members of the military can place active duty alerts. | • Consumers can request a fraud alert at one of the three agencies and this agency must notify the other two to place the alert.<br>• Victims of identity theft can place extended fraud alerts that last for 7 years.<br>• Fraud alerts still allow access to credit reports.<br>• Businesses that do not use the three agencies will not see the alert. |

Sources: GAO analysis, Federal Trade Commission, Consumer Financial Protection Bureau, and consumer and industry organizations. | GAO-19-230

## Monitor for Some Types of Fraud on Financial Accounts

| Consumer Option | How This Option Can Help | Consumers Should Be Aware |
|---|---|---|
|  **Review free credit reports every 12 months** (from Equifax, Experian, and TransUnion) at annualcreditreport.com. | • Can help consumers spot suspicious activity or fraud involving credit accounts. | • Consumers can check one of the three reports every 4 months to improve chances of catching problems throughout the year. |
|  **Review bank and other financial account statements regularly or set up free automatic alerts.** | • Can alert consumers to suspicious activity on their accounts. | • The availability and features of alerts may vary among financial institutions. |
|  **Consider enrolling in credit or identity monitoring services.** | • Credit monitoring can alert consumers after the fact that someone may have used their personal information to open a credit account (take out a loan or sign up for a credit card).<br>• Identity monitoring can alert consumers of misuse of personal information or appearance of their information on illicit websites (the “dark web”). | • These services do not directly address risks of medical identity theft, identity theft tax refund fraud, or government benefits fraud.<br>• Credit monitoring can spot fraud but generally cannot prevent it, and does not identify fraud on existing or noncredit accounts.<br>• Identity monitoring also cannot prevent fraud.<br>• It is unclear what actions consumers can take once alerted that their information appears on the dark web other than continuing to monitor their accounts.<br>• These services may be part of a package of identity theft services, including restoration services, or identity theft insurance.<br>• Free services that entities that have experienced data breaches may offer to affected consumers vary in the type and level of service and may only last for 1-2 years. Risks can exist for much longer.<br>• Paid services typically cost $5–$30 a month. |

Sources: GAO analysis, Federal Trade Commission, Consumer Financial Protection Bureau, and consumer and industry organizations. | GAO-19-230

## Monitor for Other Types of Identity Theft or Fraud

| Consumer Option | How This Option Can Help | Consumers Should Be Aware |
|---|---|---|
|  **Mobile Phone or Utility Account Fraud** | | |
| **Review mobile phone and utility bills regularly.** | • Can spot suspicious activity on existing accounts. | • Consumers with credit freezes may need to lift them before applying for new utility or phone accounts. |
|  **Medical Identity Theft** | | |
| **Review medical bills and health insurance explanations of benefits.** | • Can spot suspicious activity, such as bills or insurance claims for services consumers did not receive. | • Consumers who spot problems can contact fraud departments at health insurers. |
|  **Identity Theft Tax Refund Fraud** | | |
| **File tax returns early.** | • Provides less time for a fraudster to file in an individual's name. | • Consumers who experience identity theft tax refund fraud can file affidavits with the Internal Revenue Service (IRS) and through IdentityTheft.gov, and may be eligible to obtain an Identity Protection Personal Identification Number from IRS. |
|  **Government Benefits Fraud** | | |
| **Set up an online account at the Social Security Administration** and check it regularly. | • Can spot suspicious activity, such as benefits redirected to another address. | • Other government benefits, such as unemployment insurance, also can be susceptible to identity fraud. |

Sources: GAO analysis, Federal Trade Commission, Consumer Financial Protection Bureau, and consumer and industry organizations. | GAO-19-230

## How to Respond after Identity Theft

| Consumer Option | How This Option Can Help | Consumers Should Be Aware |
|---|---|---|
| **Visit identityTheft.gov** to set up an account, fill out, and file necessary reports. | • Helps users determine what steps to take depending on the type of information stolen or type of identity theft.<br>• Can generate an Identity Theft Report that can be used to help contact consumer reporting agencies, law enforcement, and other entities.<br>• Can generate an IRS Identity Theft Affidavit (IRS Form 14039) that can be submitted directly to IRS.<br>• Provides information on what companies to contact and how to remove incorrect information. | • The Federal Trade Commission (FTC) also has a telephone help line and online chat feature. |
| **Contact state or local government resources**, such as consumer protection help lines or victim services offices. | • Some states and local governments can provide one-on-one assistance. | • States and localities vary in the services offered. |
| **Consider using commercial identity restoration services.** | • Can reduce consumer time and effort in dealing with the effects of identity theft, such as by interacting with creditors on the consumer's behalf. | • Service levels can vary significantly among companies. Some provide hands-on assistance, while others largely provide information.<br>• May be included in a package of identity theft services, which may also include credit or identity monitoring or identity theft insurance. Paid services typically cost $5–$30 a month and free services may only be offered for 1-2 years. |

Sources: GAO analysis, Federal Trade Commission, Consumer Financial Protection Bureau, and consumer and industry organizations. | GAO-19-230

| Protect Personal Information in Other Ways | | |
|---|---|---|
| Consumer Option | How This Option Can Help | Consumers Should Be Aware |
|  **Adopt Good Practices for Online Accounts**<br>• Protect passwords and do not re-use them.<br>• Use two-factor authentication when offered (for example, entering a one-time code sent to a mobile phone when logging in to an online account).<br>• Choose strong passwords and consider using a software application that helps manage passwords.<br>• Do not click on links in emails or open attachments from unknown senders.<br>• Remember that public WiFi may not be secure. | • Can prevent unauthorized access to online accounts and other data intrusions. | • While personal security practices are important, consumers have limited control over how private entities secure their data. |
|  **Protect social media accounts** by checking privacy settings, and consider limiting information shared. | • Restricts how much information is visible to strangers and their ability to misuse it. | • Privacy terms and conditions can change, so it is important to check settings periodically. |
|  **Do not provide personal information over the phone (or by email or text) unless you've initiated the call (or communication).** | • Prevents identity thieves from obtaining information that can be used to commit fraud. | • Consumers can do online searches to verify identities of requesters, or check with experts, before giving out information.<br>• Consumers should not trust caller ID and should hang up on robocalls and report such calls to FTC at ftc.gov/complaint. |
|  **Shred documents and mail with Social Security numbers or other personal information.** | • Prevents identity thieves from finding sensitive information in trash. | • Consumers can contact the U.S. Postal Service if they believe their mail is being stolen or misdirected.<br>• Consumers can opt out of receiving credit card and other offers in the mail at 1-888-5-OPT-OUT (1-888-567-8688) or www.optoutprescreen.com. |

Sources: GAO analysis, Federal Trade Commission, Consumer Financial Protection Bureau, and consumer and industry organizations. | GAO-19-230

# ClassAction.org



---