Scott Edward Cole, Esq. (S.B. #160744)
Laura Grace Van Note, Esq. (S.B. #310160)
Cody Alexander Bolce, Esq. (S.B. #322725)
COLE & VAN NOTE
555 12th Street, Suite 2100
Oakland, California 94607
Telephone: (510) 891-9800
Facsimile: (510) 891-7030
Email: sec@colevannote.com
Email: lvn@colevannote.com
Email: cab@colevannote.com
Web: www.colevannote.com

Attorneys for Representative Plaintiff and the Plaintiff Class(es)

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

ROBBIE HURTADO, individually, and on behalf of all others similarly situated,

Plaintiff,

v.

PENSION BENEFIT INFORMATION, LLC dba PBI RESEARCH SERVICES, BERWYNGROUP, INC. and PROGRESS SOFTWARE CORPORATION,

Defendants.

Case No.

CLASS ACTION

COMPLAINT FOR DAMAGES, INJUNCTIVE RELIEF AND EQUITABLE RELIEF FOR:

1. **NEGLIGENCE;**
2. **BREACH OF IMPLIED CONTRACT;**
3. **BREACH OF IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING.**

[JURY TRIAL DEMANDED]

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

INTRODUCTION

1. Representative Plaintiff Robbie Hurtado ("Representative Plaintiff") brings this class action against Defendants Pension Benefit Information, LLC ("PBI"), BerwynGroup, Inc. ('BGI") and Progress Software Corporation ("PSG") (collectively "Defendants") for their failure to properly secure and safeguard Representative Plaintiff's and Class Members' personally identifiable information stored within Defendant's information network, including without limitation, full names, dates of birth, Social Security numbers and dependents'/childrens' names (these types of information, *inter alia*, being thereafter referred to, collectively, as "personally identifiable information" or "PII").[1]

2. With this action, Representative Plaintiff seeks to hold Defendants responsible for the harms it caused and will continue to cause Representative Plaintiff and, at least, hundreds of thousands of other similarly situated persons in the massive and preventable cyberattack purportedly discovered by PBI on or around June 6, 2023 by which cybercriminals infiltrated Defendants' inadequately protected file transfer application and accessed highly sensitive PII which was being kept unprotected (the "Data Breach").

3. While PBI claims to have discovered the breach as early as June 6, 2023, Defendants did not begin informing victims of the Data Breach until June 22, 2023 and failed to inform victims when or for how long the Data Breach occurred. Indeed, Representative Plaintiff and Class Members were wholly unaware of the Data Breach until they received letters informing them of it. The Notice received by Representative Plaintiff was dated June 22, 2023.

4. Defendants acquired, collected and stored Representative Plaintiff's and Class Members' PII. Therefore, at all relevant times, Defendants knew or should have known that Representative Plaintiff and Class Members would use Defendants' services to store and/or share sensitive data, including highly confidential PII.

[1] Personally identifiable information ("PII") generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on its face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers, etc.).

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

5. By obtaining, collecting, using and deriving a benefit from Representative Plaintiff's and Class Members' PII, Defendants assumed legal and equitable duties to those individuals. These duties arise from state and federal statutes and regulations as well as common law principles.

6. Defendants disregarded the rights of Representative Plaintiff and Class Members by intentionally, willfully, recklessly and/or negligently failing to take and implement adequate and reasonable measures to ensure that Representative Plaintiff's and Class Members' PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, Representative Plaintiff's and Class Members' PII was compromised through disclosure to an unknown and unauthorized third party—an undoubtedly nefarious third party seeking to profit off this disclosure by defrauding Representative Plaintiff and Class Members in the future. Representative Plaintiff and Class Members have a continuing interest in ensuring their information is and remains safe and are entitled to injunctive and other equitable relief.

JURISDICTION AND VENUE

7. Jurisdiction is proper in this Court under 28 U.S.C. § 1332 (diversity jurisdiction). Specifically, this Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action where the amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class and at least one other Class Member is a citizen of a state different from Defendant.

8. Supplemental jurisdiction to adjudicate issues pertaining to state law is proper in this Court under 28 U.S.C. § 1367.

9. Defendants routinely conduct business in the State where this District is located, have sufficient minimum contacts in this State and have intentionally availed themselves of this jurisdiction by marketing and selling products and services, and by accepting and processing payments for those products and services within this State.

10. Venue is proper in this Court under 28 U.S.C. § 1391 because a substantial part of the events that gave rise to Representative Plaintiff's claims took place within this District, and Defendants do business in this Judicial District.

PLAINTIFF

11. Representative Plaintiff is an adult individual and, at all relevant times herein, was a resident and citizen of the State of California. Representative Plaintiff is a victim of the Data Breach. Representative Plaintiff is a member of the California Public Employees' Retirement System ("CalPERS") and receives her retirement benefits therefrom.

12. Defendants received highly sensitive PII from Representative Plaintiff in connection with services they provide to CalPERS. As a result, Representative Plaintiff's information was among the data accessed by an unauthorized third party in the Data Breach.

13. At all times herein relevant, Representative Plaintiff is and was a member of each of the Classes.

14. Representative Plaintiff's PII was exposed in the Data Breach because Defendants stored and/or shared Representative Plaintiff's PII. Representative Plaintiff's PII was within the possession and control of Defendants at the time of the Data Breach.

15. Representative Plaintiff received a letter from CalPERS stating Representative Plaintiff's PII was involved in the Data Breach (the "Notice").

16. As a result, Representative Plaintiff spent time dealing with the consequences of the Data Breach, which included and continues to include time spent verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self-monitoring Representative Plaintiff's accounts and seeking legal counsel regarding Representative Plaintiff's options for remedying and/or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured.

17. Representative Plaintiff suffered actual injury in the form of damages to and diminution in the value of Representative Plaintiff's PII—a form of intangible property that

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

Representative Plaintiff entrusted to Defendants, which was compromised in and as a result of the Data Breach.

18. Representative Plaintiff suffered lost time, annoyance, interference and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using and selling Representative Plaintiff's PII.

19. Representative Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft and misuse resulting from Representative Plaintiff's PII, in combination with Representative Plaintiff's name being placed in the hands of unauthorized third parties/criminals.

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

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

DEFENDANTS

21. Defendant PBI is a Delaware corporation with a principal place of business located at 333 South Seventh Street, Suite 2400 Minneapolis, Minnesota 55402. PBI bills itself as death audit and beneficiary research experts for pension plans.[2]

22. Defendant BGI is a Delaware corporation with a principal place of business located at 2 Summit Park Drive Suite 610, Independence, Ohio 44131. BGI is "the industry leader in mortality verification (death audits) and new address determination (locator services) or pension fund and 401(k) administrators, insurance companies, banks, unions, public and municipal employee retirement systems, state teacher's retirement systems, investment firms, credit card companies, epidemiology departments and organizations that have a financial interest in knowing the mortality or current addresses of their pensioners, policyholders, beneficiaries, members, account holders, etc."[3]

[2] https://www.pbinfo.com/who-we-are/ (last accessed July 6, 2023).
[3] https://staff.berwyngroup.com/db/Home.asp (last accessed July 6, 2023).

23. Defendant PSG is Delaware corporation with a principal place of business located at 15 Wayside Road, Suite 400 Burlington, Massachusetts 01803. PSG operates the MOVEit application which it claims can "Transfer data securely, assure compliance and easily automate transfers while controlling user access."[4] Defendants were using the MOVEit application to transfer the data accessed in the Data Breach.

24. Defendants provide death auditing and other research services to CalPERS. Defendants were in possession of Representative Plaintiff's and Class Members' PII at the time of the breach.

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

CLASS ACTION ALLEGATIONS

26. Representative Plaintiff brings this action pursuant to the provisions of Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, on behalf of Representative Plaintiff and the following Class:

> **Nationwide Class:**
> "All individuals within the United States of America whose PII was exposed to unauthorized third parties as a result of the data breach discovered by Defendants on or around June 6, 2023."

27. Excluded from the Class are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors and any entity in which any Defendant has a controlling interest, all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out, any and all federal, state or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards,

[4] https://www.progress.com/products (last accessed July 6, 2023).

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

sections, groups, counsel and/or subdivisions, and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

28. In the alternative, Representative Plaintiff requests additional Subclasses as necessary based on the types of PII that were compromised.

29. Representative Plaintiff reserves the right to amend the above definition or to propose subclasses in subsequent pleadings and motions for class certification.

30. This action has been brought and may properly be maintained as a class action under Federal Rule of Civil Procedure Rule 23 because there is a well-defined community of interest in the litigation and membership in the proposed Classes is easily ascertainable.

a. Numerosity: A class action is the only available method for the fair and efficient adjudication of this controversy. The members of the Plaintiff Classes are so numerous that joinder of all members is impractical, if not impossible. Representative Plaintiff is informed and believe and, on that basis, alleges that the total number of Class Members is in the tens of thousands of individuals. Membership in the Classes will be determined by analysis of Defendants' records.

b. Commonality: Representative Plaintiff and the Class Members share a community of interest in that there are numerous common questions and issues of fact and law which predominate over any questions and issues solely affecting individual members, including but not necessarily limited to:

1) Whether Defendants had a legal duty to Representative Plaintiff and the Classes to exercise due care in collecting, storing, using and/or safeguarding their PII;

2) Whether Defendants knew or should have known of the susceptibility of their data security systems to a data breach;

3) Whether Defendant's security procedures and practices to protect their systems were reasonable in light of the measures recommended by data security experts;

4) Whether Defendants' failure to implement adequate data security measures allowed the Data Breach to occur;

5) Whether Defendants failed to comply with their own policies and applicable laws, regulations and industry standards relating to data security;

6) Whether Defendants adequately, promptly and accurately informed Representative Plaintiff and Class Members that their PII had been compromised;

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

7) How and when Defendants actually learned of the Data Breach;

8) Whether Defendants' conduct, including their failure to act, resulted in or was the proximate cause of the breach of their systems, resulting in the loss of Representative Plaintiff's and Class Members' PII;

9) Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

10) Whether Defendants engaged in unfair, unlawful or deceptive practices by failing to safeguard Representative Plaintiff's and Class Members' PII;

11) Whether Representative Plaintiff and Class Members are entitled to actual and/or statutory damages and/or whether injunctive, corrective and/or declaratory relief and/or an accounting is/are appropriate as a result of Defendants' wrongful conduct;

12) Whether Representative Plaintiff and Class Members are entitled to restitution as a result of Defendants' wrongful conduct.

c. Typicality: Representative Plaintiff's claims are typical of the claims of the Plaintiff Classes. Representative Plaintiff and all members of the Plaintiff Classes sustained damages arising out of and caused by Defendants' common course of conduct in violation of law, as alleged herein.

d. Adequacy of Representation: Representative Plaintiff in this class action is an adequate representative of each of the Plaintiff Classes in that the Representative Plaintiff has the same interest in the litigation of this case as the Class Members, is committed to vigorous prosecution of this case and has retained competent counsel who are experienced in conducting litigation of this nature. Representative Plaintiff is not subject to any individual defenses unique from those conceivably applicable to other Class Members or the Classes in their entireties. Representative Plaintiff anticipates no management difficulties in this litigation.

e. Superiority of Class Action: Since the damages suffered by individual Class Members, while not inconsequential, may be relatively small, the expense and burden of individual litigation by each member makes or may make it impractical for members of the Plaintiff Classes to seek redress individually for the wrongful conduct alleged herein. Should separate actions be brought or be required to be brought by each individual member of the Plaintiff Classes, the resulting multiplicity of lawsuits would cause undue hardship and expense for the Court and the litigants. The prosecution of separate actions would also create a risk of inconsistent rulings which might be dispositive of the interests of the Class Members who are not parties to the adjudications and/or may substantially impede their ability to adequately protect their interests.

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

31. Class certification is proper because the questions raised by this Complaint are of common or general interest affecting numerous persons, such that it is impracticable to bring all Class Members before the Court.

32. This class action is also appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to Class Members, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Classes in their entireties. Defendants' policies and practices challenged herein apply to and affect Class Members uniformly and Representative Plaintiff's challenge of these policies and practices hinges on Defendants' conduct with respect to the Classes in their entireties, not on facts or law applicable only to Representative Plaintiff.

33. Unless a Class-wide injunction is issued, Defendants may continue in their failure to properly secure the PII of Class Members, and Defendants may continue to act unlawfully as set forth in this Complaint.

34. Further, Defendants have acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

COMMON FACTUAL ALLEGATIONS

The Cyberattack

35. In the course of the Data Breach, one or more unauthorized third parties accessed Class Members' sensitive data, including but not limited to full names, dates of birth, Social Security numbers and dependents'/childrens' names. Representative Plaintiff was among the individuals whose data was accessed in the Data Breach.

36. Representative Plaintiff was provided the information detailed above upon Representative Plaintiff's receipt of a letter from CalPERS. Representative Plaintiff was not aware of the Data Breach until receiving that letter.

Defendant's Failed Response to the Breach

37. Upon information and belief, the unauthorized third-party cybercriminals gained access to Representative Plaintiff's and Class Members' PII with the intent of misusing the PII, including marketing and selling Representative Plaintiff's and Class Members' PII.

38. Not until after roughly two weeks after PBI claims to have discovered the Data Breach did CalPERS begin sending the Notice to persons whose PII Defendants confirmed was potentially compromised as a result of the Data Breach. The Notice provided basic details of the Data Breach and CalPERS recommended next steps.

39. Defendants have and continues to have obligations created by applicable federal and state law as set forth herein, reasonable industry standards, common law and their own assurances and representations to keep Representative Plaintiff's and Class Members' PII confidential and to protect such PII from unauthorized access.

40. Representative Plaintiff and Class Members were required to provide their PII to Defendants in order to participate in CalPERS, and as part of providing services Defendants created, collected and stored Representative Plaintiff's and Class Members' PII with the reasonable expectation and mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

41. Despite this, Representative Plaintiff and the Class Members remain, even today, in the dark regarding what particular data was stolen, the particular malware used and what steps are being taken, if any, to secure their PII going forward. Representative Plaintiff and Class Members are thus left to speculate as to where their PII ended up, who has used it and for what potentially nefarious purposes. Indeed, they are left to further speculate as to the full impact of the Data Breach and how exactly Defendants intend to enhance their information security systems and monitoring capabilities so as to prevent further breaches.

42. Representative Plaintiff's and Class Members' PII may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII for targeted marketing without Representative Plaintiff's and/or Class Members' approval. Either way, unauthorized individuals can now easily access Representative Plaintiff's and Class Members' PII.

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

Defendants Collected/Stored Class Members' PII

43. Defendants acquired, collected, stored and assured reasonable security over Representative Plaintiff's and Class Members' PII.

44. As a condition of its relationships with Representative Plaintiff and Class Members, CalPERS required that Representative Plaintiff and Class Members entrust it with highly sensitive and confidential PII. CalPERS, in turn, provided that information to Defendants who were ultimately affected by the Data Breach.

45. By obtaining, collecting and storing Representative Plaintiff's and Class Members' PII, Defendants assumed legal and equitable duties over the PII and knew or should have known that it was thereafter responsible for protecting Representative Plaintiff's and Class Members' PII from unauthorized disclosure.

46. Representative Plaintiff and Class Members have taken reasonable steps to maintain their PII's confidentiality. Representative Plaintiff and Class Members relied on Defendants to keep their PII confidential and securely maintained, to use this information for auditing purposes only and to make only authorized disclosures of this information.

47. Defendants could have prevented the Data Breach by properly securing and encrypting and/or more securely encrypting their servers generally, as well as Representative Plaintiff's and Class Members' PII.

48. Defendants' negligence in safeguarding Representative Plaintiff's and Class Members' PII is exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

49. Due to the high-profile nature of these breaches, and other breaches of its kind, Defendants were and/or certainly should have been on notice and aware of such attacks occurring in their industry and, therefore, should have assumed and adequately performed the duty of preparing for such an imminent attack. This is especially true given that Defendants are large, sophisticated operations with the resources to put adequate data security protocols in place.

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

50. And yet, despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect Representative Plaintiff's and Class Members' PII from being compromised.

Defendants Had an Obligation to Protect the Stolen Information

51. In failing to adequately secure Representative Plaintiff's and Class Member's sensitive data, Defendants breached duties it owed Representative Plaintiff and Class Members under statutory and common law. Defendants were prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

52. In addition to their obligations under federal and state laws, Defendants owed a duty to Representative Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PII in Defendants' possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants owed a duty to Representative Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements and to ensure that their computer systems, networks and protocols adequately protected Representative Plaintiff's and Class Members' PII.

53. Defendants owed a duty to Representative Plaintiff and Class Members to design, maintain and test their computer systems, servers and networks to ensure that all PII in their possession was adequately secured and protected.

54. Defendants owed a duty to Representative Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect all PII in their possession, including not sharing information with other entities who maintained sub-standard data security systems.

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

55. Defendants owed a duty to Representative Plaintiff and Class Members to implement processes that would immediately detect a breach on their data security systems in a timely manner.

56. Defendants owed a duty to Representative Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

57. Defendants owed a duty to Representative Plaintiff and Class Members to disclose if their computer systems and data security practices were inadequate to safeguard individuals' PII from theft because such an inadequacy would be a material fact in the decision to entrust their PII to Defendants.

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

59. Defendants owed a duty to Representative Plaintiff and Class Members to encrypt and/or more reliably encrypt Representative Plaintiff's and Class Members' PII and monitor user behavior and activity in order to identity possible threats.

Value of the Relevant Sensitive Information

60. The high value of PII to criminals is further evidenced by the prices they will pay for it through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[5] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[6] Criminals can also purchase access to entire company data breaches from $999 to $4,995.[7]

[5] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed July 6, 2023).

[6] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed July 6, 2023).

[7] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed July 6, 2023).

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

61. These criminal activities have and will result in devastating financial and personal losses to Representative Plaintiff and Class Members. For example, it is believed that certain PII compromised in the 2017 Experian data breach was being used three years later by identity thieves to apply for COVID-19-related benefits in the state of Oklahoma. Such fraud will be an omnipresent threat for Representative Plaintiff and Class Members for the rest of their lives. They will need to remain constantly vigilant.

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

63. Identity thieves can use PII, such as that of Representative Plaintiff and Class Members which Defendants failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

64. The ramifications of Defendants' failure to keep secure Representative Plaintiff's and Class Members' PII are long lasting and severe. Once PII is stolen, particularly identification numbers, fraudulent use of that information and damage to victims may continue for years. Indeed, Representative Plaintiff's and Class Members' PII was taken by hackers to engage in identity theft or to sell it to other criminals who will purchase the PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

65. There may be a time lag between when harm occurs versus when it is discovered and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

> [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.[8]

66. And data breaches are preventable.[9] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[10] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised…."[11]

67. Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules and procedures. Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*.[12]

68. Here, Defendants knew of the importance of safeguarding PII and of the foreseeable consequences that would occur if Representative Plaintiff's and Class Members' PII was stolen, including the significant costs that would be placed on Representative Plaintiff and Class Members as a result of a breach of this magnitude. As detailed above, Defendants knew or should have known that the development and use of such protocols were necessary to fulfill their statutory and common law duties to Representative Plaintiff and Class Members. Their failure to do so is therefore intentional, willful, reckless and/or grossly negligent.

69. Defendants disregarded the rights of Representative Plaintiff and Class Members by, *inter alia*, (i) intentionally, willfully, recklessly and/or negligently failing to take adequate and reasonable measures to ensure that their network servers were protected against unauthorized

---

[8] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf (last accessed July 6, 2023).

[9] Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012)

[10] *Id.* at 17.

[11] *Id.* at 28.

[12] *Id.*

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

intrusions, (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Representative Plaintiff's and Class Members' PII, (iii) failing to take standard and reasonably available steps to prevent the Data Breach, (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time, and (v) failing to provide Representative Plaintiff and Class Members prompt and accurate notice of the Data Breach.

FIRST CLAIM FOR RELIEF
Negligence
(On behalf of the Nationwide Class)

70. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

71. At all times herein relevant, Defendants owed Representative Plaintiff and Class Members a duty of care, *inter alia*, to act with reasonable care to secure and safeguard their PII and to use commercially reasonable methods to do so. Defendants took on this obligation upon accepting and storing Representative Plaintiff's and Class Members' PII on their computer systems and networks.

72. Among these duties, Defendants were expected:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PII in their possession;

b. to protect Representative Plaintiff's and Class Members' PII using reasonable and adequate security procedures and systems that were/are compliant with industry-standard practices;

c. to implement processes to quickly detect the Data Breach and to timely act on warnings about data breaches; and

d. to promptly notify Representative Plaintiff and Class Members of any data breach, security incident or intrusion that affected or may have affected their PII.

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

73. Defendants knew the PII was private and confidential and should be protected as private and confidential and, thus, Defendants owed a duty of care not to subject Representative Plaintiff and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

74. Defendants knew or should have known of the risks inherent in collecting and storing PII, the vulnerabilities of their data security systems and the importance of adequate security. Defendants knew about numerous, well-publicized data breaches.

75. Defendants knew or should have known that their data systems and networks did not adequately safeguard Representative Plaintiff's and Class Members' PII.

76. Only Defendants were in the position to ensure that their systems and protocols were sufficient to protect the PII that Representative Plaintiff and Class Members had entrusted to it.

77. Defendants breached their duties to Representative Plaintiff and Class Members by failing to provide fair, reasonable or adequate computer systems and data security practices to safeguard Representative Plaintiff's and Class Members' PII.

78. Because Defendants knew that a breach of their systems could damage thousands of individuals, including Representative Plaintiffs and Class Members, Defendants had a duty to adequately protect their data systems and the PII contained thereon.

79. Representative Plaintiff's and Class Members' willingness to entrust Defendants with their PII was predicated on the understanding that Defendants would take adequate security precautions. Moreover, only Defendants had the ability to protect their systems and the PII stored on them from attack. Thus, Defendants had a special relationship with Representative Plaintiff and Class Members.

80. Defendants also had independent duties under state and federal laws that required Defendants to reasonably safeguard Representative Plaintiff's and Class Members' PII and promptly notify them about the Data Breach. These "independent duties" are untethered to any contract between Defendants and Representative Plaintiff and/or the remaining Class Members.

81. Defendants breached their general duty of care to Representative Plaintiff and Class Members in, but not necessarily limited to, the following ways:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Representative Plaintiff's and Class Members' PII;

b. by failing to timely and accurately disclose that Representative Plaintiff's and Class Members' PII had been improperly acquired or accessed;

c. by failing to adequately protect and safeguard the PII by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PII;

d. by failing to provide adequate supervision and oversight of the PII with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather Representative Plaintiff's and Class Members' PII, misuse the PII and intentionally disclose it to others without consent;

e. by failing to adequately train their employees to not store PII longer than absolutely necessary;

f. by failing to consistently enforce security policies aimed at protecting Representative Plaintiff's and the Class Members' PII;

g. by failing to implement processes to quickly detect data breaches, security incidents or intrusions; and

h. by failing to encrypt Representative Plaintiff's and Class Members' PII and monitor user behavior and activity in order to identify possible threats.

82. Defendants' willful failure to abide by these duties was wrongful, reckless and/or grossly negligent in light of the foreseeable risks and known threats.

83. As a proximate and foreseeable result of Defendants' grossly negligent conduct, Representative Plaintiff and Class Members have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

84. The law further imposes an affirmative duty on Defendants to timely disclose the unauthorized access and theft of the PII to Representative Plaintiff and Class Members so that they could and/or still can take appropriate measures to mitigate damages, protect against adverse consequences and thwart future misuse of their PII.

85. Defendants breached their duty to notify Representative Plaintiff and Class Members of the unauthorized access by weeks after learning of the Data Breach to notify

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

Representative Plaintiff and Class Members and then by failing and continuing to fail to provide Representative Plaintiff and Class Members sufficient information regarding the breach. To date, Defendants have not provided sufficient information to Representative Plaintiff and Class Members regarding the extent of the unauthorized access and continues to breach their disclosure obligations to Representative Plaintiff and Class Members.

86. Further, through their failure to provide timely and clear notification of the Data Breach to Representative Plaintiff and Class Members, Defendants prevented Representative Plaintiff and Class Members from taking meaningful, proactive steps to, *inter alia*, secure and/or access their PII.

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

88. Defendants' wrongful actions, inactions and omissions constituted (and continue to constitute) common law negligence.

89. The damages Representative Plaintiff and Class Members have suffered (as alleged above) and will continue to suffer were and are the direct and proximate result of Defendants' grossly negligent conduct.

90. Additionally, 15 U.S.C. § 45 (FTC Act, Section 5) prohibits "unfair […] practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

91. Defendants violated 15 U.S.C. § 45 by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of PII it obtained

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

and stored and the foreseeable consequences of the immense damages that would result to Representative Plaintiff and Class Members.

92. Defendants' violation of 15 U.S.C. § 45 constitutes negligence *per se.*

93. As a direct and proximate result of Defendants' negligence and negligence *per se*, Representative Plaintiff and Class Members have suffered and will continue to suffer injury, including but not limited to (i) actual identity theft, (ii) the loss of the opportunity of how their PII is used, (iii) the compromise, publication and/or theft of their PII, (iv) out-of-pocket expenses associated with the prevention, detection and recovery from identity theft, tax fraud and/or unauthorized use of their PII, (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 embarrassment and identity theft, (vi) lost continuity in relation to their personal records, (vii) the continued risk to their PII, which may remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect Representative Plaintiff's and Class Members' PII in their continued possession, and (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Representative Plaintiff and Class Members.

94. As a direct and proximate result of Defendants' negligence and negligence *per se*, Representative Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including but not limited to anxiety, emotional distress, loss of privacy and other economic and noneconomic losses.

95. Additionally, as a direct and proximate result of Defendants' negligence and negligence *per se*, Representative Plaintiff and Class Members have suffered and will continue to suffer the continued risks of exposure of their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect PII in their continued possession.

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

SECOND CLAIM FOR RELIEF
Breach of Implied Contract
(On behalf of the Nationwide Class)

96. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

97. Through their course of conduct, Defendants, Representative Plaintiff and Class Members entered into implied contracts for Defendants to implement data security adequate to safeguard and protect the privacy of Representative Plaintiff's and Class Members' PII.

98. Defendants required Representative Plaintiff and Class Members to provide and entrust their PII as a condition of obtaining Defendant's services from Defendants.

99. Defendants solicited and invited Representative Plaintiff and Class Members to provide their PII as part of Defendants' regular business practices. Representative Plaintiff and Class Members accepted Defendants' offers and provided their PII to Defendants.

100. Representative Plaintiff and Class Members provided and entrusted their PII to Defendants. In so doing, Representative Plaintiff and Class Members entered into implied contracts with Defendants by which Defendants agreed to safeguard and protect such non-public information, to keep such information secure and confidential and to timely and accurately notify Representative Plaintiff and Class Members if their data had been breached and compromised or stolen.

101. A meeting of the minds occurred when Representative Plaintiff and Class Members agreed to, and did, provide their PII to Defendants, in exchange for, amongst other things, the protection of their PII.

102. Representative Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendants.

103. Defendants breached the implied contracts it made with Representative Plaintiff and Class Members by failing to safeguard and protect their PII and by failing to provide timely and accurate notice to them that their PII was compromised as a result of the Data Breach.

104. As a direct and proximate result of Defendant's above-described breach of implied contract, Representative Plaintiff and Class Members have suffered and will continue to suffer (i)

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

ongoing, imminent and impending threat of identity theft crimes, fraud and abuse, resulting in monetary loss and economic harm, (ii) actual identity theft crimes, fraud and abuse, resulting in monetary loss and economic harm, (iii) loss of the confidentiality of the stolen confidential data, (iv) the illegal sale of the compromised data on the dark web, (v) lost work time, and (vi) other economic and noneconomic harm.

THIRD CLAIM FOR RELIEF
Breach of the Implied Covenant of Good Faith and Fair Dealing
(On behalf of the Nationwide Class)

105. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth therein.

106. Every contract in this State has an implied covenant of good faith and fair dealing. This implied covenant is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

107. Representative Plaintiff and Class Members have complied with and performed all conditions of their contracts with Defendants.

108. Defendants breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard PII, failing to timely and accurately disclose the Data Breach to Representative Plaintiff and Class Members and continued acceptance of PII and storage of other personal information after Defendants knew or should have known of the security vulnerabilities of the systems that were exploited in the Data Breach.

109. Defendants acted in bad faith and/or with malicious motive in denying Representative Plaintiff and Class Members the full benefit of their bargains as originally intended by the parties, thereby causing them injury in an amount to be determined at trial.

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

RELIEF SOUGHT

WHEREFORE, Representative Plaintiff, on Representative Plaintiff's own behalf and on behalf of each member of the proposed National Class, respectfully requests the Court enter judgment in favor of Representative Plaintiff and the Class and for the following specific relief against Defendants as follows:

1. That the Court declare, adjudge and decree that this action is a proper class action and certify the proposed Class and/or any other appropriate Subclasses under F.R.C.P. Rule 23 (b)(1), (b)(2), and/or (b)(3), including appointment of Representative Plaintiff's counsel as Class Counsel;

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

3. That the Court enjoin Defendants, ordering them to cease and desist from unlawful activities;

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

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

   a. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

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

   c. requiring Defendants to delete and purge Representative Plaintiff's and Class Members' PII unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Representative Plaintiff and Class Members;

   d. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Representative Plaintiff's and Class Members' PII;

e. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests and audits on Defendants' systems on a periodic basis;

f. prohibiting Defendants from maintaining Representative Plaintiff's and Class Members' PII on a cloud-based database;

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

h. requiring Defendants to conduct regular database scanning and securing checks;

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

j. requiring Defendants to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs and systems for protecting personal identifying information;

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

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

6. For prejudgment interest on all amounts awarded, at the prevailing legal rate;

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

8. For all other Orders, findings and determinations identified and sought in this Complaint.

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

JURY DEMAND

Representative Plaintiff, individually and on behalf of the Plaintiff Class, hereby demands a trial by jury for all issues triable by jury.

Dated: July 6, 2023

By: */s/ Cody A. Bolce*

Scott Edward Cole, Esq.
Cody Alexander Bolce, Esq.
COLE & VAN NOTE
555 12th Street, Suite 2100
Oakland, California 94607
Telephone: (510) 891-9800
Facsimile: (510) 891-7030
Email: sec@colevannote.com
Email: cab@colevannote.com

Attorneys for Representative Plaintiff and the Plaintiff Classes