REESE LLP
Michael R. Reese (State Bar No. 206773)
mreese@reesellp.com
100 West 93rd Street, 16th Floor
New York, New York 10025
Phone: (212) 643-0500

LAUKAITIS LAW FIRM LLC
Kevin Laukaitis (Pro hac vice application forthcoming)
klaukaitis@laukaitislaw.com
737 Bainbridge Street, #155
Philadelphia, Pennsylvania 19147
Phone: (215) 789-4462

[Additional Attorneys in Signature Block]

Attorneys for Plaintiff and the Putative Class

CGC-23-604214

IN THE SUPERIOR COURT OF THE STATE OF CALIFORNIA
IN AND FOR THE COUNTY OF SAN FRANCISCO

JOHN DOE,[1] individually and on behalf of all others similarly situated,

Plaintiff,

v.

LASTPASS US, LLC, and GOTO TECHNOLOGIES USA, INC.

Defendants.

Case No.

CLASS ACTION COMPLAINT

1. Negligence
2. Breach of Implied Contract
3. Breach of the Implied Covenant of Good Faith and Fair Dealing
4. Unjust Enrichment
5. Violation of California Unfair Competition Law, Cal. Bus. & Prof Code § 17200 *et seq.*
6. Violation of California Customer Records Act, Cal. Civ. Code § 1798.80 *et seq.*

JURY TRIAL DEMANDED

[1] Because of the nature of the allegations herein, Plaintiff is identified conditionally by a pseudonym in order to preserve the confidentiality and privacy of his personal information. Plaintiff intends to file a motion to proceed using a pseudonym in accordance with *Department of Fair Employment & Housing v. Superior Court of Santa Clara County*, 82 Cal. App. 5th 105, 111 (2022).

INTRODUCTION

1. Plaintiff John Doe ("Plaintiff") brings this class action against Defendants LastPass US, LLC ("LastPass") and GoTo Technologies USA, Inc. ("GoTo") (collectively "Defendants"), for their failure to properly secure and safeguard Plaintiff's and Class Members' personally identifiable information stored within Defendants' information network, including, without limitation, names, billing addresses, email addresses, telephone numbers, as well as a vault of unencrypted data which stored website usernames and passwords, secure notes, and form-filled data (this type of information, inter alia, being hereafter referred to as "personally identifiable information" or "PII").[2]

2. Plaintiff seeks to hold Defendants responsible for the harms they caused and will continue to cause Plaintiff and countless other similarly situated persons in the massive and preventable cyberattack purportedly discovered by Defendants in August 2022, by which cybercriminals infiltrated Defendants' inadequately protected network servers and accessed highly sensitive PII and financial information, which was being kept unprotected (the "Data Breach").

3. On information and belief, while Defendants claim to have discovered the breach as early as August 2022, Defendants did not begin informing victims of the Data Breach until December 22, 2022. Indeed, Plaintiff and Class Members were unaware of the Data Breach until they received letters from Defendants informing them of it. The Notice received by Plaintiff was dated December 22, 2022.

4. Moreover, on January 25, 2023, Defendant GoTo confirmed that encrypted customer data was stolen in the Data Breach. Furthermore, GoTo stated that an encryption key may have been stolen, which could be used to unscramble some of the sensitive data.[3]

[2] 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).

[3] *See Last Pass Owner GoTo Confirms Hackers Stole Customer Data* available athttps://www.siliconrepublic.com/enterprise/goto-lastpass-encryption-key-data-breach

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

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

7. Defendants disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff's and Class Members' PII was safeguarded, failing to take available steps to prevent 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, the PII of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party—an undoubtedly nefarious third party that seeks to profit off this disclosure by defrauding Plaintiff and Class Members in the future. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they are entitled to injunctive and other equitable relief.

JURISDICTION AND VENUE

8. **Personal Jurisdiction.** Defendants have purposefully availed themselves of the privilege of doing business within the State. This action arises out of and relates to Defendants' contacts with this forum. Specifically, Defendants knowingly directed their services through the stream of commerce into this forum. Defendants have advertised and marketed within this forum through the wires and mails, and via mobile applications and websites through which residents of this forum can purchase Defendants' services. Defendants knowingly direct electronic activity into this forum with the intent to engage in business interactions and have in fact engaged in such interactions. Defendants offer services to consumers in this forum who made purchases using Defendants' services in this forum, and whose losses were incurred here. The Court has specific personal jurisdiction over Defendants as they can be said to have reasonably anticipated being hauled into court in this forum.

9. **Subject Matter Jurisdiction.** This Court has subject matter jurisdiction over this action pursuant to Article VI, section 10 of the California Constitution and Code of Civil Procedure section 410.10. Jurisdiction also exists under Business & Professions Code section 17203.

10. **Venue** is Venue is proper because Defendants conduct business in this county that brought about the business transactions at issue in this case. In addition, a substantial part of the acts and conduct charged herein occurred in this County. Venue also is proper because many Class members did business with Defendants and engaged in transactions in this County, and Defendants have reaped substantial profits from customers who engaged in transactions in this County.

PARTIES

Plaintiff

11. Plaintiff John Doe is an adult individual and, at all relevant times herein, a resident and citizen of California, residing in San Francisco, California. Plaintiff is a victim of the Data Breach.

12. Defendants received highly sensitive personal and financial information from Plaintiff in connection with the goods/services they had received or requested. As a result, Plaintiff's information was among the data accessed by an unauthorized third-party in the Data Breach.

13. Plaintiff received—and was a "consumer" —for purposes of obtaining services from Defendants, specifically Plaintiff was a LastPass customer and used LastPass's services to store his passwords and sensitive information.

14. At all times herein relevant, Plaintiff is and was a member of the Nationwide Class and the California Subclass.

15. As required in order to obtain services from Defendants, Plaintiff provided Defendants with highly sensitive personal and financial information.

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

17. Plaintiff received a letter from Defendants, dated December 22, 2022, stating that his PII and/or financial information was involved in the Data Breach (the "Notice").

18. As a result, 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 its accounts, and seeking legal counsel regarding its options for remedying and/or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured.

19. Plaintiff suffered actual injury in the form of damages to and diminution in the value of its PII—a form of intangible property that they entrusted to Defendants, which was compromised in and as a result of the Data Breach.

20. 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 its PII and/or financial information.

21. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from its PII and financial information, in combination with its name, being placed in the hands of unauthorized third parties/criminals.

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

Defendants

23. Defendant LastPass is a Massachusetts corporation with a principal place of business located at 320 Summer St, Boston, Massachusetts 02210. Defendant is a password management business designed to save and protect all passwords using a browser extension.[4]

24. Defendant GoTo is a Delaware corporation with its principal place of business in Boston, Massachusetts.

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 Plaintiff. 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.

[4] https://www.lastpass.com/how-lastpass-works (last accessed January 25, 2023).

COMMON FACTUAL ALLEGATIONS

The Data Breach

26. During the Data Breach, one or more unauthorized third parties accessed Class Members' sensitive data, including, but not limited to, names, Social Security numbers, and financial account information. Plaintiff was among the individuals whose data was accessed in the Data Breach.

27. Plaintiff was provided the information detailed above upon receiving a letter from Defendants, dated December 22, 2022. Plaintiff was unaware of the Data Breach until that time.

Defendants' Failed Response to the Breach

28. Upon information and belief, the unauthorized third-party cybercriminals gained access to Plaintiff's and Class Members' PII and financial information with the intent of engaging in the misuse of the PII and financial information, including marketing and selling Plaintiff's and Class Members' PII.

29. Not until roughly four months after they claim to have discovered the Data Breach did Defendants begin sending the Notice to persons whose PII and/or financial information Defendants confirmed was potentially compromised as a result of the Data Breach. The Notice provided basic details of the Data Breach and Defendants' recommended next steps.

30. The Notice included, *inter alia*, the claims that Defendants had learned of the Data Breach on August 2022, and later discovered the unauthorized access began as early as May 25, 2022, and continued until August 2022.

31. Upon information and belief, the unauthorized third-party cybercriminals gained access to Plaintiff's and Class Members' PII and financial information with the intent of engaging in the misuse of the PII and financial information, including marketing and selling Plaintiff's and Class Members' PII.

32. Defendants had and continue 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 Plaintiff's and Class Members' PII confidential and to protect such PII from unauthorized access.

33. Plaintiff and Class Members were required to provide their PII and financial

information to Defendants in order to receive services therefrom, and as part of services, Defendants created, collected, and stored 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.

34. Despite this, 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 and financial information going forward. 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.

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

Defendants Collected/Stored Class Members' PII and Financial Information

36. Defendants acquired, collected, and stored, and assured reasonable security over Plaintiff's and Class Members' PII and financial information.

37. As a condition of its relationships with Plaintiff and Class Members, Defendants required that Plaintiff and Class Members entrust Defendants with highly sensitive and confidential PII and financial information. Defendants, in turn, stored that information in their system that was ultimately affected by the Data Breach.

38. By obtaining, collecting, and storing Plaintiff's and Class Members' PII and financial information, Defendants assumed legal and equitable duties and knew or should have known that they were thereafter responsible for protecting Plaintiff's and Class Members' PII and financial information from unauthorized disclosure.

39. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality

of their PII and financial information. Plaintiff and Class Members relied on Defendants to keep their PII and financial information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

40. Defendants could have prevented the Data Breach, which began no later than August 2022, by properly securing and encrypting and/or more securely encrypting its servers generally, as well as Plaintiff's and Class Members' PII and financial information.

41. Defendants' negligence in safeguarding Plaintiff's and Class Members' PII and financial information 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.

42. 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 and, therefore, should have assumed and adequately performed the duty of preparing for such an imminent attack. This is especially true given that Defendants operate large, sophisticated businesses with the resources to put adequate data security protocols in place.

43. Yet, despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect Plaintiff's and Class Members' PII and financial information from being compromised.

Defendants Had an Obligation to Protect the Stolen Information

44. Defendants' failure to adequately secure Plaintiff's and Class Members' sensitive data breaches duties they owe Plaintiff and Class Members under statutory and common law. Defendants have a statutory duty under other federal and state statutes to safeguard Plaintiff's and Class Members' data. Moreover, Plaintiff and Class Members surrendered their highly sensitive personal data to Defendants under the implied condition that Defendants would keep it private and secure. Accordingly, Defendants also have an implied duty to safeguard their data, independent of any statute.

45. In addition to its obligations under state laws, Defendants owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII and financial information in Defendants' possession from being compromised, lost, stolen, accessed, and/or misused by unauthorized persons. Defendants owed a duty to 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 the PII and financial information of Plaintiff and Class Members.

46. Defendants owed a duty to Plaintiff and Class Members to design, maintain, and test their computer systems, servers, and networks to ensure that the PII and financial information in its possession was adequately secured and protected.

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

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

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

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

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

52. Defendants owed a duty to Plaintiff and Class Members to encrypt and/or more reliably encrypt Plaintiff's and Class Members' PII and financial information and monitor user behavior and activity in order to identify possible threats.

Value of the Relevant Sensitive Information

53. The high value of PII and financial information to criminals is further evidenced by the prices they will pay 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]

54. These criminal activities have and will result in devastating financial and personal losses to 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 to Plaintiff and Class Members for the rest of their lives. They will need to remain constantly vigilant.

55. 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."

56. Identity thieves can use PII and financial information, such as that of 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.

57. The ramifications of Defendants' failure to secure Plaintiff's and Class Members' PII and financial information are long-lasting and severe. Once PII and financial information are stolen, particularly identification numbers, fraudulent use of that information and damage to victims may

[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/

[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/

[7] In the Dark, VPNOverview, 2019, *available at* https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/

continue for years. Indeed, the PII and/or financial information of Plaintiff and Class Members was taken by hackers to engage in identity theft or to sell it to other criminals who will purchase the PII and/or financial information for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

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

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[8]

59. The harm to Plaintiff and Class Members is especially acute given the nature of the leaked data. When cybercriminals access Social Security numbers, financial account information, and other personally sensitive data—as they did here—there is no limit to the amount of fraud to which Defendants may have exposed Plaintiff and Class Members.

60. 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] They 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]

61. 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]

---

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

[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.*

62. Here, Defendants knew of the importance of safeguarding PII and financial information and of the foreseeable consequences that would occur if Plaintiff's and Class Members' PII and financial information were stolen, including the significant costs that would be placed on Plaintiff and Class Members as a result of a breach of this magnitude. As detailed above, Defendants a large, sophisticated companies with the resources to deploy robust cybersecurity protocols. Each Defendant knew, or should have known, that the development and use of such protocols were necessary to fulfill their statutory and common law duties to Plaintiff and Class Members. Defendants' failure to do so is, therefore, intentional, willful, reckless and/or grossly negligent.

63. Defendants disregarded the rights of Plaintiff and Class Members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that their network servers were protected against unauthorized intrusions, (ii) failing to disclose that they did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiff's and Class Members' PII and/or financial information, (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 Plaintiff and Class Members prompt and accurate notice of the Data Breach.

CLASS ACTION ALLEGATIONS

64. Pursuant to California Code of Civil Procedure section 382, Plaintiff brings this action on behalf of the proposed Classes defined as follows:

Nationwide Class: All individuals within the United States of America whose PII and/or financial information was exposed to unauthorized third parties as a result of the Data Breach discovered by Defendants in August 2022.

California Subclass: All individuals within the State of California whose PII and/or financial information was exposed to unauthorized third parties as a result of the Data Breach discovered by Defendants in August 2022.

65. Excluded from the Classes are the following individuals and/or entities: Defendants and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants have 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 any departments, agencies, divisions, bureaus, boards, sections, groups, counsels, and/or subdivisions and all judges assigned to hear any aspect of this litigation, as well as its immediate family members.

66. Also, in the alternative, Plaintiff requests additional Subclasses as necessary based on the types of PII that were compromised. Plaintiff reserves the right to amend the above definition or to propose subclasses in subsequent pleadings and motions for class certification.

67. Certification of Plaintiff's claims for class-wide treatment is appropriate because the questions presented are of a common and general interest, and the parties are so numerous that it is impracticable to bring them all before the court and because Plaintiff can prove the elements of the claims on a class-wide basis using the same evidence as individual Class members would use to prove those elements in individual actions alleging the same claims.

68. The size of the Classes is so large that joinder of all Class members is impracticable. Plaintiff is informed and believes and, on that basis, alleges that the total number of Class Members is in the hundreds of thousands of individuals. Membership in the classes will be determined by analysis of Defendants' records.

69. Questions of law and fact of common and general interest to the Classes predominate over any questions that affect only individual Class members. Common legal and factual questions/issues include but are not limited to:

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

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

c. Whether Defendants' security procedures and practices to protect their systems were reasonable in light of the measures recommended by data security experts;

d. Whether Defendant's failure to implement adequate data security measures allowed the Data Breach to occur;

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

f. Whether Defendants adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. How and when Defendants actually learned of the Data Breach;

h. 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 the PII of Plaintiff and Class Members;

i. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members;

k. Whether Defendants violated the California statutes alleged herein;

l. Whether 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;

m. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct.

70. Defendants engaged in a common course of conduct in contravention of the laws Plaintiff seeks to enforce individually and on behalf of the Classes. Similar or identical violations of law, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the predominant common questions. Moreover, the common questions will yield common answers that will substantially advance the resolution of the case.

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

72. There are no defenses available to Defendants that are unique to the named Plaintiff.

73. Plaintiff is a fair and adequate representative of the Classes because Plaintiff's interests do not conflict with the Class members' interests. Plaintiff will prosecute this action vigorously and is highly motivated to seek redress against Defendants. Furthermore, Plaintiff has selected competent

counsel who are experienced in class actions and other complex litigation, including data breach class actions. Plaintiff and Plaintiff's counsel are committed to prosecuting this action vigorously on behalf of the Classes and have the resources to do so.

74. The class action mechanism is superior to other available means for the fair and efficient adjudication of this controversy for reasons including but not limited to the following:

a. The damages individual Class members suffered are small compared to the burden and expense of individual prosecution of the complex and extensive litigation needed to address Defendants' misconduct.

b. It would be virtually impossible for the Class members individually to redress effectively the wrongs done to them. Even if Class members themselves could afford such individual litigation, the court system could not. Individualized litigation would unnecessarily increase the delay and expense to all parties and to the court system and presents a potential for inconsistent or contradictory rulings and judgments. By contrast, the class action device presents far fewer management difficulties, allows the hearing of claims which might otherwise go unaddressed because of the relative expense of bringing individual lawsuits, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

c. The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications, which would establish incompatible standards of conduct for Defendants.

d. The prosecution of separate actions by individual Class members would create a risk of adjudications with respect to them that would, as a practical matter, be dispositive of the interests of other Class members not parties to the adjudications or that would substantively impair or impede their ability to protect their interests.

75. Defendants have acted on grounds applicable to the Classes as a whole, so that final injunctive and declaratory relief concerning the Classes as a whole are appropriate.

76. Plaintiff suffers threat of future harm because unless a Class-wide injunction is issued, Defendants may continue in their failure to properly secure the PII and/or financial information of Class Members, and Defendants may continue to act unlawfully as set forth in this Complaint.

77. Plaintiff and Plaintiff's counsel anticipate that notice to the proposed Classes will be effectuated through recognized, Court-approved notice dissemination methods, which may include United States mail, electronic mail, Internet postings, Social media, and/or published notice.

CAUSES OF ACTION

COUNT I

NEGLIGENCE

(On behalf of the Nationwide Class and the Subclasses)

78. Plaintiff restates and realleges all preceding allegations above and hereafter as if fully set forth herein.

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

80. Among these duties, Defendants were expected:

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

b. to protect Plaintiff's and Class Members' PII and financial information 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 act on warnings about data breaches timely; and

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

81. Defendants knew that the PII and financial information were private and confidential and should be protected as private and confidential and, thus, Defendant owed a duty of care not to subject Plaintiff and Class Members to an unreasonable risk of harm because they were foreseeable

and probable victims of any inadequate security practices.

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

83. Defendants knew, or should have known, that their data systems and networks did not adequately safeguard Plaintiff's and Class Members' PII and financial information.

84. Only Defendants were in the position to ensure that their systems and protocols were sufficient to protect the PII and financial information that Plaintiff and Class Members had entrusted to them.

85. Defendants breached their duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the PII and financial information of Plaintiff and Class Members.

86. Because Defendants knew that a breach of their systems could damage thousands of individuals, including Plaintiff and Class Members, Defendants had a duty to adequately protect their data systems and the PII and financial information contained therein.

87. Plaintiff's and Class Members' willingness to entrust Defendants with their PII and financial information 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 and financial information they stored on them from attack. Thus, Defendants had a special relationship with Plaintiff and Class Members.

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

89. Defendants breached their general duty of care to 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 the PII and financial information of Plaintiff and Class Members;

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

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

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

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

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

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

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

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

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

92. The law further imposes an affirmative duty on Defendants to timely disclose the unauthorized access and theft of the PII and financial information to 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 and financial information.

93. Defendants breached their duty to notify Plaintiff and Class Members of the unauthorized access by waiting months after learning of the Data Breach to notify Plaintiff and Class Members and then by failing and continuing to fail to provide Plaintiff and Class Members sufficient information regarding the breach. To date, Defendants have not provided sufficient information to Plaintiff and Class Members regarding the extent of the unauthorized access and continue to breach their disclosure obligations to Plaintiff and Class Members.

94. Further, through their failure to provide timely and clear notification of the Data Breach to Plaintiff and Class Members, Defendants prevented Plaintiff and Class Members from taking meaningful, proactive steps to secure their PII and financial information.

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

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

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

98. 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 Defendants, of failing to use reasonable measures to protect PII and financial information. The FTC publications and orders described above also form part of the basis of Defendants' duty.

99. Defendants violated 15 U.S.C. §45 by failing to use reasonable measures to protect PII and financial information and not complying with applicable industry standards, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of PII and financial information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and Class Members.

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

101. As a direct and proximate result of Defendants' negligence and negligence per se, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft, (ii) the loss of the opportunity of how their PII and financial information is used, (iii) the compromise, publication, and/or theft of their PII and financial information, (iv) out-of-pocket

expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and financial 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 embarrassment and identity theft, (vi) the continued risk to their PII and financial information, which may remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII and financial 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 PII and financial information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

102. As a direct and proximate result of Defendants' negligence and negligence per se, 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 non-economic losses.

103. Additionally, as a direct and proximate result of Defendants' negligence and negligence per se, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their PII and financial information, which remain in Defendants' possession and are subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII and financial information in its continued possession.

COUNT II

BREACH OF IMPLIED CONTRACT

(On behalf of the Nationwide Class and the Subclasses)

104. Plaintiff restates and realleges all preceding allegations above and hereafter as if fully set forth herein.

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

106. Defendants required Plaintiff and Class Members to provide and entrust their PII and financial information as a condition of obtaining Defendants' services.

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

108. As a condition of their relationship with Defendants, Plaintiff and Class Members provided and entrusted their PII and financial information to Defendants. In so doing, 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 Plaintiff and Class Members if their data had been breached and compromised or stolen.

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

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

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

112. As a direct and proximate result of Defendants' above-described breach of implied contract, Plaintiff and Class Members have suffered (and will continue to suffer) (a) ongoing, imminent, and the impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm, (b) actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm, (c) loss of the confidentiality of the stolen confidential data; (d) the illegal sale of the compromised data on the dark web, (e) lost work time and (f) other economic and non-economic harm.

COUNT III

BREACH OF THE IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING

(On behalf of the Nationwide Class and the Subclasses)

113. Plaintiff restates and realleges all preceding allegations above and hereafter as if fully set forth herein.

114. 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.

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

116. 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 and financial information, failing to timely and accurately disclose the Data Breach to Plaintiff and Class Members and continued acceptance of PII and financial information 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.

117. Defendants acted in bad faith and/or with malicious motive in denying 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.

COUNT IV

UNJUST ENRICHMENT

(On behalf of the Nationwide Class and/or California Subclass)

118. Plaintiff restates and realleges all preceding allegations above and hereafter as if fully set forth herein.

119. Plaintiff brings this Count under California Law individually and on behalf of the Nationwide Class and/or California Subclass ("Class") against Defendants.

120. By their wrongful acts and omissions described herein, Defendants have obtained a benefit by unduly taking advantage of Plaintiff and Class Members.

121. Defendants, prior to and at the time Plaintiff and Class Members entrusted their PII and financial information to Defendants for the purpose of obtaining services, caused Plaintiff and Class Members to reasonably believe that Defendants would keep such PII and financial information secure.

122. Defendants were aware, or should have been aware, that reasonable consumers would have wanted their PII and financial information kept secure and would not have contracted with Defendants, directly or indirectly, had they known that Defendants' information systems were sub-standard for that purpose.

123. Defendants were also aware that, if the substandard condition of and vulnerabilities in their information systems were disclosed, they would negatively affect Plaintiff's and Class Members' decision to seek services therefrom.

124. Defendants failed to disclose facts pertaining to its substandard information systems, defects, and vulnerabilities therein before Plaintiff and Class Members made their decisions to make purchases, engage in commerce therewith, and seek services or information. Instead, Defendants suppressed and concealed such information. By concealing and suppressing that information, Defendants denied Plaintiff and Class Members the ability to make a rational and informed purchasing decision and took undue advantage of Plaintiff and Class Members.

125. Defendants were unjustly enriched at the expense of Plaintiff and Class Members. Defendants received profits, benefits, and compensation, in part, at the expense of Plaintiff and Class Members. By contrast, Plaintiff and Class Members did not receive the benefit of their bargain because they paid for products and/or services that did not satisfy the purposes for which they bought/sought them.

126. Since Defendants' profits, benefits and other compensation were obtained by improper means, Defendants are not legally or equitably entitled to retain any of the benefits, compensation or profits it realized from these transactions.

127. Plaintiff and Class Members seek an Order of this Court requiring Defendants to refund, disgorge, and pay as restitution any profits, benefits, or other compensation obtained by Defendants from their wrongful conduct and/or the establishment of a constructive trust from which Plaintiff and Class Members may seek restitution.

COUNT V

VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW, CAL. BUS. & PROF. CODE § 17200 *ET SEQ.*

(On Behalf of the California Subclass)

128. Plaintiff restates and realleges all preceding allegations above and hereafter as if fully set forth herein.

129. Each Defendant is a "person" as defined by Cal. Bus. & Prof. Code § 17201.

130. Defendants violated Cal. Bus. & Prof. Code §§ 17200, et seq. ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

131. Defendants' unlawful, unfair acts and deceptive acts and practices include:

a. Defendants failed to implement and maintain reasonable security measures to protect Plaintiff and the California Subclass Members from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

b. Defendants failed to:

i. Secure their website;

ii. Secure access to their servers;

iii. Comply with industry-standard security practices;

iv. Employ adequate network segmentation;

v. Implement adequate system and event monitoring;

vi. Utilize modern payment systems that provide more security against intrusion;

vii. Install updates and patches in a timely manner, and

viii. Implement the systems, policies, and procedures necessary to prevent this type of data breach.

c. Defendants failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiff and the California

Subclass Members whose PII has been compromised;

d. Defendants' failure to implement and maintain reasonable security measures also was contrary to legislatively declared public policy that seeks to protect consumer data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTCA, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.81.5 et seq., and California's Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq.;

e. Defendants' failure to implement and maintain reasonable security measures also led to substantial injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because Plaintiff and the California Subclass Members could not know of Defendants' inadequate security, consumers could not have reasonably avoided the harms that Defendants caused;

f. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff and the California Subclass Members' PII, including by implementing and maintaining reasonable security measures;

g. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and the California Subclass Members' PII, including duties imposed by the FTCA, 15 U.S.C § 45; California's Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq.; and California's Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq.;

h. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff and the California Subclass Members' PII;

i. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and the California Subclass Members' PII, including duties imposed

by the FTCA, 15 U.S.C § 45; California's Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq.; and California's Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq.;

j. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82; and

k. Among other ways to be discovered and proved at trial.

132. Defendants' representations and material omissions of fact, as alleged herein, to Plaintiff and the California Subclass Members were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the privacy of consumers' PII.

133. Defendants intended to mislead Plaintiff and the California Subclass Members and induce them to rely on their misrepresentations and material omissions of fact as alleged herein.

134. Had Defendants disclosed to Plaintiff and the California Subclass Members that their data systems were not secure and, thus, vulnerable to attack, Defendants would have been unable to continue in business, and they would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendants received, maintained, and compiled Plaintiff and the California Subclass Members' PII as part of the services and goods Defendants provided without advising Plaintiff and the California Subclass Members that Defendants' data security practices were insufficient to maintain the safety and confidentiality of Plaintiff and the California Subclass Members. Accordingly, Plaintiff and the California Subclass Members acted reasonably in relying on Defendants' misrepresentations and material omissions of fact, the truth of which they could not have discovered.

135. Defendants acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff's and the California Subclass Members' rights.

136. As a direct and proximate result of Defendants' unfair, unlawful, and fraudulent acts and practices, Plaintiff and the California Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages as

described herein and as will be proved at trial.

137. Plaintiff and the California Subclass Members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Defendants' unfair, unlawful, and fraudulent business practices or use of their PII; declaratory relief; injunctive relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; and other appropriate equitable relief.

138. Plaintiff and California Class Members are also entitled to injunctive relief requiring Defendants to, e.g., (a) strengthen their data security systems and monitoring procedures; (b) submit to future annual audits of those systems and monitoring procedures; and (c) continue to provide adequate credit monitoring to all California Class Members.

COUNT VI

VIOLATION OF CALIFORNIA CUSTOMER RECORDS ACT ("CCRA")

CAL. CIV. CODE § 1798.80 *ET SEQ.*

(On behalf of the California Subclass)

139. Plaintiff restates and realleges all preceding allegations above and hereafter as if fully set forth herein.

140. This Count is brought on behalf of Plaintiff and the California Subclass against Defendants.

141. "[T]o ensure that Personal Information about California residents is protected," the California legislature enacted Cal. Civ. Code §1798.81.5, which requires that any business that "owns, licenses, or maintains Personal Information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the Personal Information from unauthorized access, destruction, use, modification, or disclosure."

142. Each Defendant is a business that maintains PII about Plaintiff and California Subclass Members within the meaning of Cal. Civ. Code §1798.81.5.

143. As a direct and proximate result of Defendants' violations of the Cal. Civ. Code §1798.81.5, Plaintiff and California Subclass members suffered damages, as described above and as will be proven at trial.

144. Plaintiff and California Subclass members seek relief under Cal. Civ. Code §1798.84, including actual damages, civil penalties, injunctive relief, and reasonable attorneys' fees and costs.

RELIEF SOUGHT

WHEREFORE, Plaintiff, on behalf of itself and each member of the proposed National Class and the California Subclass, respectfully requests that the Court enter judgment in its favor 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 each of the proposed classes and/or any other appropriate subclasses under California Code of Civil Procedure section 382, including the appointment of 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 Plaintiff's and Class Members' PII, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;

5. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of 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 laws;

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

   d. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of 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 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 Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' 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 Plaintiff and Class Members;

j. requiring Defendants to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' 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 Defendants' 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;

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.

JURY DEMAND

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

Date: January 25, 2023

Respectfully Submitted:

By: */s/ Michael R. Reese*

Michael R. Reese (State Bar No. 206773)
mreese@reesellp.com
REESE LLP
100 West 93rd Street, 16th Floor
New York, New York 10025
Phone: (212) 643-0500

Kevin Laukaitis (Pro hac vice application forthcoming)
klaukaitis@laukaitislaw.com
LAUKAITIS LAW FIRM LLC
737 Bainbridge Street, #155
Philadelphia, Pennsylvania 19147
Phone: (215) 789-4462

George V. Granade (State Bar No. 316050)
ggranade@reesellp.com
REESE LLP
8484 Wilshire Boulevard, Suite 515
Los Angeles, California 90211
Phone: (310) 393-0070
Facsimile: (212) 253-4272

Charles D. Moore (Pro hac vice application forthcoming)
cmoore@reesellp.com
REESE LLP
100 South 5th Street, Suite 1900
Minneapolis, Minnesota 55402
Phone: (212) 643-0500

Attorneys for Plaintiff and the Putative Class