UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

ERIC LAPRAIRIE, ***on behalf of himself and all other employees similarly situated,***

Plaintiff,

v.

PRESIDIO, INC., PRESIDIO HOLDINGS INC., PRESIDIO LLC, PRESIDIO NETWORKED SOLUTIONS LLC, PRESIDIO NETWORKED SOLUTIONS GROUP, LLC, AND PRESIDIO TECHNOLOGY CAPITAL, LLC,

Defendants.

AMENDED COMPLAINT AND DEMAND FOR JURY TRIAL

Case No. 1:21-cv-08795-JFK

Plaintiff Eric LaPrairie ("Named Plaintiff"), individually and on behalf of all other individuals similarly situated (collectively "Plaintiffs" or "Class Members"), by and through his attorneys, Thomas & Solomon LLP, brings this first amended class action complaint against Presidio, Inc., Presidio Holdings Inc., Presidio LLC, Presidio Networked Solutions, LLC, Presidio Networked Solutions Group, LLC, and Presidio Technology Capital, LLC ("Presidio" or "Defendants"), and alleges as follows:

NATURE OF ACTION

1. Named Plaintiff brings this action on behalf of himself and all other employees similarly situated against Presidio as a result of Presidio's failure to adequately safeguard and protect the personally identifiable information ("PII") of their employees and by negligently disclosing such employee PII to cyber criminals.

2. Plaintiffs are all current or former employees of Defendants whose PII was compromised as a result of an unknown third-party gaining unauthorized access to Presidio's software and/or systems on or about March 5, 2020 (hereinafter the "Data Breach" or

"Breach").

3. The Breach resulted in the disclosure of Plaintiffs' private and sensitive PII, including their names, Social Security numbers, compensation and tax information.

4. For the rest of their lives, Named Plaintiff and Class Members will bear an immediate and heightened risk of all manners of identity theft.

5. Indeed, Plaintiffs have also suffered concrete harm almost immediately after the Data Breach. For example, Named Plaintiff himself fell victim to attempted identity theft just months after the Data Breach and was forced to spend numerous hours rectifying the harm caused by Defendants' conduct. Additionally, the unauthorized third party also altered direct deposits of some Class Members and wrongfully diverted such direct deposit funds.

6. Accordingly, Named Plaintiff brings this action as a direct and/or proximate result of the Data Breach. Plaintiffs have incurred, and will continue to incur, damages in the form of, among other things, attempted identity theft, time and expense in mitigating harms caused by Defendants' conduct, increased risk of harm, diminished value of their PII, loss of privacy, and/or additional damages as set forth herein.

JURISDICTION AND VENUE

7. The jurisdiction of this Court is invoked pursuant to Class Action Fairness Act of 2005, 28 U.S.C. §§ 1332(d)(2), because there are at least 100 class members, the amount in controversy exceeds five million, and there is minimal diversity of citizenship.

8. This Court has personal jurisdiction over Defendants because Defendants maintain their principal place of business in this District and have sufficient minimum contacts with New York.

9. Venue is appropriate in the Southern District of New York because Defendants

reside in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

THE PARTIES

Named Plaintiff

10. Named Plaintiff Eric LaPrairie is a resident of Michigan and a former employee of Presidio.

11. Named Plaintiff worked for Presidio from approximately January 2019 to August 2019 and he received a notice on or around April 26, 2020 from Presidio informing him that his PII had been disclosed in a data breach.

Defendants

12. Defendant Presidio, Inc. is a Delaware corporation with its principal place of business in New York.

13. According to its website, Defendant Presidio, Inc. maintains locations in Arkansas, California, Colorado, Connecticut, Florida, Georgia, Idaho, Illinois, Indiana, Massachusetts, Maryland, Michigan, Minnesota, Mississippi, North Carolina, New Jersey, New York, Ohio, Oklahoma, Oregon, Pennsylvania, Tennessee, Texas, Utah, Virginia, and Wisconsin.

14. As a result of having offices in each of these locations, Defendants have employees in: Arkansas, California, Colorado, Connecticut, Florida, Georgia, Idaho, Illinois, Indiana, Massachusetts, Maryland, Michigan, Minnesota, Mississippi, North Carolina, New Jersey, New York, Ohio, Oklahoma, Oregon, Pennsylvania, Tennessee, Texas, Utah, Virginia, and Wisconsin.

15. Defendant Presidio Holdings Inc. is a Delaware corporation with its principal

place of business in New York.

16. Defendant Presidio LLC is a Georgia limited liability company with its principal place of business in New York.

17. Defendant Presidio Networked Solutions LLC is a Florida limited liability company with its principal place of business in New York.

18. Defendant Presidio Networked Solutions Group, LLC is a Delaware limited liability company with its principal place of business in New York.

19. Defendant Presidio Technology Capital, LLC is a Georgia limited liability company with its principal place of business in New York.

FACTS

20. As a condition of Plaintiffs' employment, Plaintiffs provided their PII to Defendants in order to verify their identities, receive compensation, and for Defendants to maintain complete employee records for, among other things, tax purposes.

21. On or about March 5, 2020, an unauthorized third-party gained access to Defendants' servers and systems resulting in the Data Breach and subsequent exposure of PII of thousands of current and former employees of Presidio.

22. In approximately late April 2020, over a month after the Breach, Plaintiffs received correspondence from Defendants informing them of the circumstances of the Breach.

23. This correspondence, signed by Elliot Brecher, Presidio's Senior Vice President and General Counsel, indicated that the unauthorized individual who had unauthorized access to Defendants' software systems accessed "the name, Social security number, and total annual compensation of each Presidio employee who received from Presidio a 2019 W-2" as well as "the names and wage/tax information of employees listed on a 2020 payroll register report."

24. Being in the cybersecurity industry, Presidio knew or should have known of the importance of safeguarding employee PII, as well as the consequences of the unauthorized disclosure of employees' PII. Defendants, however, failed to implement adequate policies and procedures to safeguard Plaintiffs' PII from being disclosed by hackers and cyber criminals.

25. Despite being aware of their common law and statutory duty to adequately safeguard Plaintiffs' PII, Defendants breached that duty by disclosing Plaintiffs' PII through their negligent actions and/or inactions.

26. Defendants negligently failed to take the necessary precautions required to safeguard and protect Plaintiffs' PII from unauthorized disclosure. Defendants' actions and/or inactions amount to a flagrant disregard of Plaintiffs' rights to privacy and property.

27. Defendants' actions and/or inactions caused Plaintiffs to suffer injury and damages as described herein.

28. As a result, Defendants are liable to Named Plaintiff and Class Members as described herein.

29. Additionally, Defendants are liable under the statutes, laws, and regulations of each state in which they operate throughout the United States.

Personally Identifiable Information (PII)

30. PII "refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as data and place of birth, mother's maiden name, etc." *See* Office of Mgmt. & Budget, Memorandum M-07-16, *Safeguarding Against & Responding to the Breach of Personally Identifiable Information*, at n.1 (May 22, 2007),

https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2007/m07-16.pdf.

31. PII is of great value to hackers and cyber criminals, and the data compromised in the Data Breach can be used in a variety of unlawful manners that cause great harm to the individuals who have had their PII exposed.

32. The PII of individuals is of high value to criminals, as evidenced by the prices they will pay through the dark web. For example, personal information can be sold at prices ranging from $40 to $200. *See* Anita George, *Your Personal Data is for Sale on the Dark Web. Here's How Much it Costs*, Digital Trends (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.

33. Neal O'Farrell, a security and identity theft expert for Credit Sesame, calls a Social Security number "your secret sauce," and that is "as good as your DNA to hackers." *See* Cameron Huddleston, *How to Protect Your Kids from the Anthem Data Breach*, Kiplinger (Feb. 10, 2015), https://www.kiplinger.com/article/credit/t048-c011-s001-how-to-protect-your-kids-from-the-anthem-data-brea.html.

34. In the event of a compromised Social Security number, an individual must wait until she becomes a victim of identity theft before she can obtain a new one. Even then, the Social Security Administration warns "that a new number probably won't solve all [] problems . . . [and] won't guarantee [] a fresh start." *See* Soc. Sec. Admin., *Identity Theft and Your Social Security Number*, at 6 (June 2018), https://www.ssa.gov/pubs/EN-05-10064.pdf. In fact, "[f]or some victims of identity theft, a new number actually creates new problems." *Id.* For example, a brand new Social Security number will have a completely blank credit history, making it difficult for an identity theft victim to get extended credit for years unless it is linked to the

old compromised number.

35. Given the Data Breach at issue resulted in an unauthorized third-party gaining access to Plaintiffs' PII, it is reasonably foreseeable that cyber criminals can and will use the compromised PII in a variety of different unlawful ways to the detriment of Plaintiffs.

Defendants Were Aware of the Risk of Cyberattacks

36. In today's world, data security breaches are becoming increasingly common. So common that the Federal Trade Commission ("FTC") has issued an abundance of guidance for business to combat the ever-increasing threat to employees' PII. *See, e.g.*, FTC, *Data Breach Response: A Guide for Business* (May 2019), https://www.ftc.gov/system/files/documents/plain-language/pdf-0154_data-breach-response-guide-for-business-042519-508.pdf; FTC, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.bulkorder.ftc.gov/publications/protecting-personal-information-guide-business; FTC, *Start with Security: A Guide for Business* (Jun. 2015), https://www.bulkorder.ftc.gov/system/files/publications/pdf0205-startwithsecurity.pdf.

37. Given Presidio's position as a "leading North American IT solutions provider focused on . . . Cloud [and] Security & Emerging solutions[,]" Presidio was certainly aware of the risk of data breaches. To be sure, the front page of Presidio's website currently highlights October as "Cybersecurity Awareness Month" and offers assistance to its customers to "help *accelerate* required annual Cybersecurity *compliance* and *testing* initiatives." (emphasis in original).

38. Indeed, according to Presidio's 10-K annual report for the fiscal year ending June 30, 2019, Presidio identifies "cyber risk management, infrastructure security and managed security solutions" as one of its core business offerings. Presidio goes on to note that its cyber "[s]ecurity revenue increased $44.6 million, or 15.9%, . . . driven by higher demand from

customers as they look to stay ahead of increasingly complex cyber security threats[.]"

39. In the same annual filing, Presidio identified "[d]isruptions or breaches of security in our information technology systems and the misappropriation of our clients' data could impair our reputation, expose us to liability and adversely impact our business" as a risk factor to its business.

40. As such, Presidio was well aware of the risk that data security breaches by "hackers and cyberterrorists . . . could [] expose [Presidio] to legal claims, investigations, proceedings and liability and to regulatory penalties under laws that protect the privacy of personal information[.]"

41. Thus, being in the cyber security field themselves, Defendants clearly knew or should have known of the risk of data breaches and should have maintained adequate safeguards for their own employees' PII.

Named Plaintiff and Class Members Have Suffered Concrete Injuries

42. Named Plaintiff and Class Members were obligated to provide Defendants with sensitive personal information.

43. As a direct and/or proximate result of Defendants' failure to adequately safeguard Plaintiffs' PII, Plaintiffs have or will suffer actual concrete injuries.

44. These actual injuries include out of pocket expenses and the value of their time reasonable incurred to remedy or mitigate the effect of the Data Breach relating to:

- Closely reviewing and monitoring bank accounts and credit reports;
- Purchasing credit monitoring and identity theft prevention;
- Addressing their inability to withdraw funds linked to compromised accounts;
- Placing "freezes" and "alerts" with credit reporting agencies;

- Contacting financial institutions and closing or modifying financial accounts.

45. Further, some Plaintiffs have already suffered concrete harm in the form of altered and wrongfully diverted direct deposit funds immediately following the Data Breach.

46. Additionally, Named Plaintiff himself suffered concrete harm in the form of identity theft shortly after the Data Breach.

47. Specifically, in approximately May 2020, Named Plaintiff was victim to a "SIM swap" attack where a third-party used Named Plaintiff's PII to enter a T-Mobile store and swap Named Plaintiff's telephone number over to the third-party's mobile phone. This allowed the unauthorized third-party to obtain Named Plaintiff's telephone number for unlawful use and access Named Plaintiff's email account he used for a variety of different online accounts.

48. Prior to Defendants' Data Breach, Named Plaintiff was unaware of any other instances in which his Social Security number was breached.

49. With access to Named Plaintiff's telephone number and email, the third-party was able to reset Named Plaintiff's online account passwords in an effort to gain unauthorized access to Named Plaintiff's online accounts, including his financial accounts, Dropbox account containing his personal documents, and Microsoft account.

50. After becoming aware of this identity attack, Named Plaintiff spent approximately 15-20 hours contacting T-Mobile support and fraud services, researching how to better protect his personal information from fraudulent intruders, implementing heightened security measures on his device and accounts to protect against fraudsters, and rectifying the harm caused by the identity attack. As a result, Named Plaintiff suffered harm in the form of lost time and invasion of privacy as a direct and/or proximate cause of Defendants' actions and/or inactions giving rise to the Data Breach.

51. Named Plaintiff not only suffered a concrete harm as described above, but will also continue to suffer an imminent and continuing injury of heightened risk of identity theft and/or unauthorized use of his PII.

52. Named Plaintiff and Class Members will forever be subject to an increased risk that cyber criminals will use their PII as a result of Defendants' failure to adequately safeguard Plaintiffs' PII. As a result, Named Plaintiff and Class Members have incurred, and will continue to incur, damages in the form of, among other things, time and out-of-pocket expenses in mitigating harms caused by Defendants' conduct, diminished value of their PII, loss of privacy, and/or additional damages as set forth herein.

53. As a direct and/or proximate result of Defendants' failure to adequately safeguard Plaintiffs' PII, Plaintiffs have been deprived of the value of their PII, for which there is a well-established national and international market.

54. Defendants' actions have further placed Plaintiffs at an imminent, immediate, and continuing risk of identity theft and identity fraud. There is also a high likelihood that significant identity theft and/or identity fraud has not yet been discovered or reported by Plaintiffs.

Defendants Response to the Data Breach is Inadequate to Protect the Plaintiffs

55. Despite failing to adequately safeguard Plaintiffs' PII, Defendants have failed to provide adequate compensation to the Plaintiffs harmed by their negligent acts and/or omissions.

56. Defendants have offered Plaintiffs just twelve (12) months, and only in some cases twenty-four (24) months, of credit monitoring service through *my*TrueIdentity. Even if a Plaintiff signs up for *my*TrueIdentity service, it will not provide Plaintiffs any compensation for

the costs and burdens associated with fraudulent activity resulting from the Data Breach that took place prior to Plaintiffs signing up for the offered services. This is especially concerning where some Plaintiffs were not informed that their PII was compromised until over a month following the Breach.

57. Additionally, given the fact that Plaintiffs face a lifetime of increased risk of identity theft, twelve or twenty-four months of protection is wholly inadequate to compensate Plaintiffs for Defendants' wrongful conduct.

CLASS ACTION ALLEGATIONS

58. Plaintiffs bring this action on behalf of themselves and on behalf of all other persons similarly situated (the "Class") pursuant to Rule 23 (b)(2), (b)(3) and (c)(4) of the Federal Rules of Civil Procedure.

59. Plaintiffs propose the following Class Members definition, subject to amendment as appropriate:

> All persons whose PII was compromised in the Data Breach that occurred on or about March 5, 2020.

60. Excluded as Class Members are Defendants' officers and directors, and any entity in which Defendants have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendants.

61. Defendants are liable to Class Members under the statutes, laws, and regulations of each state in which Class Members lived and/or worked.

62. This includes all causes of action that are designed to prevent companies from allowing the improper disclosure of PII, including, but not limited to:

- Cal. Bus. & Prof. Code § 17200 *et seq.*
- Cal. Civil Code §§ 56.06, 1785.11.2, 1797.29, 1798.80, 1798.81.5, 1798.82, 1798.84

- Mass. Gen. Laws ch. 93A § 9, ch. 93H
- Tex. Bus. & Com. Code Ann. § 521.052
- Utah Code §§ 13-44-101, 102, 202, 301
- Minn. Stat. §§ 325E.61, 325E.64
- Wis. Stat. § 895.507
- 815 ILCS 530/1 *et seq.*
- Ind. Code §§ 24-4.0 *et seq.*, 4-1-11 *et seq.*
- Ga. Code §§ 10-1-910, 912
- Fla. Stat. § 817.5681
- Md. Code Com. Law § 14-3501
- N.J. Stat. 56:8-163
- N.Y. Gen. Bus. Law § 899-aa

63. Plaintiffs hereby reserve the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery. The proposed class meets the criteria for certification under Rule 23(a), 23(b)(2), 23(b)(3), and 23(c)(4).

64. Numerosity. The number of Class Members is so numerous that joinder of all of them is impracticable. For example, Presidio disclosed that 3,324 current and former employees were victim of the Data Breach. Thus, the proposed class is so numerous that joinder of all Class Members is impracticable.

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

a. Whether Defendants unlawfully used, maintained, lost, or disclosed Class Members' PII;

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

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

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

e. Whether Defendants owed a duty to Class Members to safeguard their PII;

f. Whether Defendants breached their duties to Class Members to safeguard their PII;

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

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

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

j. Whether an implied contract existed between Defendants on one hand, and Class Members on the other hand, and the terms of that implied contract;

k. Whether Defendants adequately and accurately informed Plaintiffs and Class Members that their PII had been compromised;

l. Whether Class Members suffered legally cognizable damages as a result of Defendants' misconduct;

m. Whether Defendants' conduct was negligent;

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

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

66. Typicality. Named Plaintiff's claims are typical of those of other Class Members because Named Plaintiff's PII, like that of every other Class Member, was compromised in the Data Breach.

67. Adequacy of Representation. Named Plaintiff and his counsel, Thomas & Solomon LLP, will fairly and adequately protect the interests of the class. Named Plaintiff has no interest antagonistic to Class Members, and has retained counsel experienced in class action litigation. Thomas & Solomon LLP is qualified and experienced in litigating class action cases, including data privacy litigation of this kind.

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

69. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

70. Defendants have acted on grounds that apply generally to Class Members as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

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

a. Whether Defendants owed a legal duty to Class Members to exercise due care in collecting, storing, and safeguarding their PII;

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

c. Whether Defendants' failure to institute adequate protective security measures amounted to negligence;

d. Whether Defendants failed to take commercially reasonable steps to safeguard consumer PII; and

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

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

73. Defendants' wrongful actions, inaction, and omissions are generally applicable to the class as a whole and therefore, Plaintiffs also seek equitable remedies for the class.

74. Defendants' systemic policies and practices regarding the protection of PII also make injunctive relief for the class appropriate.

FIRST CAUSE OF ACTION
Negligence

75. Named Plaintiff and Class Members re-allege the above paragraphs as if fully restated herein.

76. As a condition of their employment, Named Plaintiff and Class Members were obligated to provide Defendants with their PII.

77. As a sophisticated company with particular expertise in cyber security, Defendants had full knowledge of the sensitivity of their employees' PII, as well as the types

of harm Named Plaintiff and Class Members would suffer if their PII were to be exposed to cyber criminals.

78. Defendants owed a common law duty to Named Plaintiff and Class Members to exercise reasonable care in adequately safeguarding and protecting Named Plaintiff's and Class Members' PII in Defendants' possession.

79. Defendants assumed a duty of care to use reasonable means to secure and safeguard Named Plaintiff's and Class Members' PII, to prevent its disclosure, to guard it from theft, and to detect any attempted or actual breach of their servers or systems holding the PII.

80. Defendants breached their duty of care by failing to adequately secure and safeguard Named Plaintiff's and Class Members' PII by negligently storing and/or maintaining their servers and systems holding the PII.

81. As a result of Defendants' negligence, Named Plaintiff and Class Members have been forced or incur out of pocket costs, including for additional credit monitoring services incurred as a result of the Data Breach.

82. Named Plaintiff and Class Members have suffered harm as a result of Defendants' negligence.

83. Named Plaintiff not only suffered a concrete harm in the form of lost time and an invasion of privacy from the Data Breach as described above, but will also continue to suffer an imminent and continuing injury of heightened risk of identity theft and/or unauthorized use of his PII.

84. Named Plaintiff and Class Members will forever be subject to an increased risk that cyber criminals will use their PII as a result of Defendants' failure to adequately safeguard their PII. As a result, Named Plaintiff and Class Members have incurred, and will continue to

incur, damages in the form of, among other things, time and expense in mitigating harms caused by Defendants' conduct, diminished value of their PII, loss of privacy, and/or additional damages as set forth herein.

85. It was reasonably foreseeable that Defendants' failure to adequately safeguard Named Plaintiff and Class Members' PII would result in a cyber security breach and unauthorized disclosure of their PII by third-parties who would use and/or disseminate such PII for no lawful purpose.

86. A breach of security, unauthorized access, and resulting injury to Named Plaintiff and Class Members was reasonably foreseeable, particularly in light of Defendants' inadequate security practices.

87. Named Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the PII of Named Plaintiff and Class Members, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendants' systems.

88. Defendants as much as admit such foreseeability in their annual 10-K report identifying "[d]isruptions or breaches of security in our information technology systems and the misappropriation of our clients' data could impair our reputation, expose us to liability and adversely impact our business" as a risk factor to its business. As such, Presidio was well aware of the risk that security breaches by "hackers and cyberterrorists . . . could [] expose [Presidio] to legal claims, investigations, proceedings and liability and to regulatory penalties under laws that protect the privacy of personal information[.]"

89. But for Defendants' negligent and wrongful breach of their duty of care owed to

Named Plaintiff and Class Members, their PII would not have been compromised.

90. As a direct and proximate result of Defendants' negligent conduct, Named Plaintiff and Class Members have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

91. Plaintiffs are also entitled to injunctive relief as well as actual and punitive damages.

92. Accordingly, Named Plaintiff and Class Members respectfully request that this Court award all relevant damages for Defendants' negligent failure to adequately safeguard PII.

SECOND CAUSE OF ACTION
Breach of Implied Contract

93. Named Plaintiff and Class Members re-allege the above paragraphs as if fully restated herein.

94. Defendants required Named Plaintiff and Class Members to provide their personal information, including names, addresses, and Social Security numbers, and other personal information, as a condition of their employment.

95. As a condition of Named Plaintiff's and Class Members' employment with Defendants, Named Plaintiff and Class Members provided their PII to Defendants. In so doing, Named Plaintiff and Class Members entered into implied contracts with Defendants.

96. Defendants agreed to safeguard and protect such information, to keep such information adequately secure and confidential, and to timely and accurately notify Named Plaintiff and Class Members if their data had been breached and compromised or stolen.

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

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

99. Had Defendants disclosed that their security was inadequate, neither the Named Plaintiff, Class Members, nor any reasonable person would have entered into such contracts with Defendants.

100. As a direct and proximate result of Defendants' above-described breach of implied contracts, Named Plaintiff and Class Members have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

101. Further, due to Defendants' conduct, Named Plaintiff and Class Members did not receive the full benefit of the bargain.

102. The Data Breach was reasonably foreseeable consequence of Defendants' actions in breach of the contracts.

103. Accordingly, Named Plaintiff and Class Members respectfully request that this Court award all relevant damages for Defendants' breach of implied contracts.

THIRD CAUSE OF ACTION
Unjust Enrichment

104. Named Plaintiff and Class Members re-allege the above paragraphs as if fully restated herein.

105. Named Plaintiff and Class Members conferred benefits on Defendants.

106. Specifically, Named Plaintiff and Class Members provided services to Defendants through their employment, as well as providing Defendants with their private information.

107. In exchange, Named Plaintiff and Class Members should have received from Defendants the goods and services that were the subject of the transaction and should have been entitled to have Defendants protect their PII with adequate data security.

108. Defendants knew that Named Plaintiff and Class Members conferred a benefit on them and accepted and has accepted or retained that benefit. Defendants profited from Named Plaintiff's and Class Members' services, and used Named Plaintiff's and Class Members' PII for business purposes.

109. Defendants acquired the PII through inequitable means as they failed to disclose the inadequate security practices previously alleged.

110. If Named Plaintiff and Class Members knew that Defendants would not secure their PII using adequate security, they would not have entered into employment with Defendants.

111. Named Plaintiff and Class Members have no adequate remedy at law.

112. Under the circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Named Plaintiff and Class Members conferred on them.

113. As a direct and proximate result of Defendants' decision to profit rather than provide adequate security measures to safeguard Named Plaintiff's and Class Members' PII, Named Plaintiff and Class Members have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

114. Accordingly, Named Plaintiff and Class Members respectfully request this Court award relief in the form of restitution and/or compensatory damages.

FOURTH CAUSE OF ACTION
Violation of the Applicable State Laws

115. Named Plaintiff and Class Members re-allege the above paragraphs as if fully restated herein.

116. As a direct and proximate result of Defendants' actions and/or omissions described herein, and the resulting Data Breach exposing Named Plaintiff and Class Members' PII, Defendants are in violation of the following state laws similarly designed to protect Named Plaintiff and Class Members from the unauthorized disclosure of their PII:

- Cal. Bus. & Prof. Code § 17200 *et seq.*

- Cal. Civil Code §§ 56.06, 1785.11.2, 1797.29, 1798.80, 1798.81.5, 1798.82, 1798.84
- Mass. Gen. Laws ch. 93A § 9, ch. 93H
- Tex. Bus. & Com. Code Ann. § 521.052
- Utah Code §§ 13-44-101, 102, 202, 301
- Minn. Stat. §§ 325E.61, 325E.64
- Wis. Stat. § 895.507
- 815 ILCS 530/1 *et seq.*
- Ind. Code §§ 24-4.0 *et seq.*, 4-1-11 *et seq.*
- Ga. Code §§ 10-1-910, 912
- Fla. Stat. § 817.5681
- Md. Code Com. Law § 14-3501
- N.J. Stat. 56:8-163
- N.Y. Gen. Bus. Law § 899-aa

FIFTH CAUSE OF ACTION
Breach of Confidence

117. Named Plaintiff and Class Members re-allege the above paragraphs as if fully restated herein.

118. At all times during Named Plaintiff's and Class Members' interactions with Defendants, Defendants were fully aware of the confidential, novel, and sensitive nature of Named Plaintiff's and Class Members' PII that Named Plaintiff and Class Members provided to Defendants.

119. As alleged herein and above, Defendants' relationship with Named Plaintiff and Class Members was governed by expectations that Named Plaintiff's and Class Members' PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

120. Named Plaintiff's and Class Members provided their respective PII to Defendants with the explicit and implicit understandings that Defendants would protect and not permit the PII to be disseminated to any unauthorized parties.

121. Named Plaintiff and Class Members also provided their respective PII to

Defendants with the explicit and implicit understanding that Defendants would take precautions to protect that PII from unauthorized disclosure, such as following basic principles of information security practices.

122. Defendants voluntarily received in confidence Named Plaintiff's and Class Members' PII with the understanding that the PII would not be disclosed or disseminated to the public or any unauthorized third parties.

123. Due to Defendants' failures to prevent, detect, and/or avoid the Data Breach from occurring by, *inter alia*, failing to follow best information security practices to secure Named Plaintiff's and Class Members' PII, Named Plaintiff's and Class Members' PII was disclosed and misappropriated to unauthorized third parties beyond Named Plaintiff's and Class Members' confidence, and without their express permission.

124. But for Defendants' disclosure of Named Plaintiff's and Class Members' PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendants' Data Breach was the direct and legal cause of the theft of Named Plaintiff's and Class Members' PII, as well as the resulting damages.

125. The injury and harm Named Plaintiff and Class Members suffered was the reasonably foreseeable result of Defendants' unauthorized disclosure of Named Plaintiff's and Class Members' PII. Defendants knew or should have known their security systems were insufficient to protect the PII that is coveted by cybercriminals. Defendants also failed to observe industry standard information security practices.

126. As a direct and proximate cause of Defendants' conduct, Named Plaintiff and Class Members suffered damages as alleged above.

SIXTH CAUSE OF ACTION
Bailment

127. Named Plaintiff and Class Members re-allege the above paragraphs as if fully restated herein.

128. Named Plaintiff and Class Members delivered and entrusted their PII to Defendants for the purposes of employment with Defendants.

129. In delivering their PII to Defendant, Named Plaintiff and Class Members intended and understood that Defendants would adequately safeguard their personal and financial information.

130. Defendants accepted possession of Named Plaintiff's and Class Members' PII. By accepting possession, Defendants understood that Named Plaintiff and Class Members expected Defendants to safeguard their personal and financial information adequately. Accordingly, a bailment was established for the mutual benefit of the parties.

131. During the bailment, Defendants owed a duty to Named Plaintiff and Class Members to exercise reasonable care, diligence, and prudence in protecting their PII.

132. Defendants breached their duty of care by failing to take appropriate measures to safeguard and protect Named Plaintiff's and Class Members' PII, resulting in the unlawful and unauthorized access to and misuse of such information.

133. Defendants further breached their duty to safeguard Named Plaintiff's and Class Members' PII by failing to notify them individually in a timely and accurate manner that their information had been breached and compromised.

134. As a direct and proximate result of Defendants' breach of duty, Named Plaintiff and Class Members suffered consequential damages that were reasonably foreseeable to Defendants, including but not limited to the damages set forth herein.

SEVENTH CAUSE OF ACTION
Breach of Fiduciary Duty

135. Named Plaintiff and Class Members re-allege the above paragraphs as if fully restated herein.

136. In light of the special relationship between Defendants, and Named Plaintiff and Class Members, whereby Defendants became guardians of Named Plaintiff's and Class Members' PII, Defendants became a fiduciary by undertaking guardianship of the PII, to act primarily for the benefit of Defendants' employees and former employees, including Named Plaintiff and Class Members: (1) for the safeguarding of Named Plaintiff's and Class Members' PII; (2) to timely notify Named Plaintiff and Class Members of a data breach and disclosure; and (3) maintain complete and accurate records of what information (and where) Defendants did and does store.

137. Defendants have a fiduciary duty to act for the benefit of Named Plaintiff and Class Members upon matters within the scope of Defendants' relationship with their employees and former employees, in particular, to keep secure their PII.

138. Defendants breached their fiduciary duties to Named Plaintiff and Class Members by failing to diligently discovery, investigate, and give notice of the Data Breach in a reasonable and practicable period of time.

139. Defendants breached their fiduciary duties to Named Plaintiff and Class Members by failing to protect Named Plaintiff's and Class Members' PII.

140. Defendants breached their fiduciary duties owed to Named Plaintiff and Class Members by failing to timely notify and/or warn Named Plaintiff and Class Members of the Data Breach.

141. Defendants breached their fiduciary duties to Named Plaintiff and Class

Members by otherwise failing to safeguard Named Plaintiff's and Class Members' PII.

142. As a direct and proximate result of Defendants' breaches of their fiduciary duties, Named Plaintiff and Class Members have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

143. As a direct and proximate result of Defendants' breaches of its fiduciary duties, Named Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

WHEREFORE, Named Plaintiff and the Class demand judgment against Defendants in their favor and that they be given the following relief:

(a) an order certifying the Class as requested and designating Thomas & Solomon LLP as class counsel;

(b) designation of Named Plaintiff Eric LaPrairie as the representative of the Class;

(c) holding that Defendants breached their duty to safeguard and protect Named Plaintiff's and Class Members' PII;

(d) awarding Named Plaintiff and Class Members appropriate relief, including actual, compensatory, statutory, punitive, and any other such damages as permitted by law;

(e) awarding equitable, injunctive, and declaratory relief as appropriate, including an Order requiring Defendants to immediately secure and fully encrypt all confidential information, to properly secure computers containing PII, to crease

negligently storing, handling, and securing Plaintiffs' PII, and to provide additional years of identity theft monitoring;

(f) awarding reasonable attorneys' fees, expenses, expert fees, and costs incurred in vindicating Named Plaintiff's and Class Members' rights;

(g) an award of pre- and post-judgment interest;

(h) awarding a service payment for Named Plaintiff Eric LaPrairie; and

(i) such other and further legal or equitable relief as this Court deems just and appropriate.

JURY DEMAND

Plaintiffs demand a jury to hear and decide all issues of fact in accordance with Federal Rule of Civil Procedure 38(b).

Dated: December 20, 2021

THOMAS & SOLOMON LLP

By: **/s/ Jonathan W. Ferris**

J. Nelson Thomas, Esq.
Jessica L. Lukasiewicz, Esq.
Jonathan W. Ferris, Esq.
Attorneys for Plaintiff
693 East Avenue
Rochester, New York 14607
Telephone: (585) 272-0540
nthomas@theemploymentattorneys.com
jlukasiewicz@theemploymentattorneys.com
jferris@theemploymentattorneys.com