MICHAEL F. RAM (SBN 104805)
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
711 Van Ness Avenue, Suite 500
San Francisco, CA 94102
Telephone: (415) 358-6913
Facsimile: (415) 358-6923
mram@forthepeople.com

JOHN A. YANCHUNIS
(*Pro Hac Vice application forthcoming*)
RYAN D. MAXEY
(*Pro Hac Vice application forthcoming*)
MORGAN & MORGAN COMPLEX
LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505
jyanchunis@ForThePeople.com
rmaxey@ForThePeople.com

M. ANDERSON BERRY (SBN 262879)
LESLIE GUILLON (SBN 222400)
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829
aberry@justice4you.com
lguillon@justice4you.com

Attorneys for Plaintiff

THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

SUSAN ZEBELMAN,
on behalf of herself and all others similarly situated,

Plaintiff,

v.

ACCELLION, INC.,
a Delaware limited liability company,

Defendant.

Case No.:

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff Susan Zebelman, individually and on behalf of all others similarly situated, brings this Class Action Complaint against Defendant Accellion, Inc., and alleges, upon personal knowledge as to her own actions and her counsel's investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard personally identifiable information that was stored on and/or shared with Defendant's "Accellion FTA" file transfer service, including, without limitation, names, social security numbers and/or driver's license or state identification numbers, dates of birth, bank account numbers and bank routing numbers, and/or places of employment (collectively, "personally identifiable information" or "PII").[1]

2. According to Defendant's website, Accellion FTA "helps worldwide enterprises . . . ***transfer large and sensitive files securely*** using a 100% private cloud, on-premise or hosted."[2]

3. Defendant knew or should have known that its customers included law firms, government agencies, and universities and that these customers could and would use Accellion FTA as advertised, namely, "to transfer large and sensitive files," including sensitive files containing PII, and that it was important and necessary that such large and sensitive files be transferred "securely."

4. Notwithstanding Defendant's representation that Accellion FTA would transfer large and sensitive files securely, in December 2020, an unauthorized person accessed files and data that numerous customers of Defendant had stored on or shared with Accellion FTA (the "Data

[1] Personally identifiable information 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 their face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security number, passport number, driver's license number, financial account number).

[2] *See* https://www.accellion.com/products/fta/ (last visited Feb. 10, 2021).

Breach").[3]

5. The compromised files and data contained the PII of Plaintiff and Class Members, including, but not limited to, names, social security numbers and/or driver's license or state identification numbers, dates of birth, bank account numbers and bank routing numbers, and/or places of employment.

6. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties to those individuals.

7. The exposed PII of Plaintiff and Class Members can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. Plaintiff and Class Members face a lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers.

8. This PII was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect PII of Plaintiff and Class Members.

9. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of its inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates federal and state statutes.

10. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and significantly (iv) the continued increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's

[3] *See* https://www.accellion.com/company/press-releases/accellion-provides-update-to-recent-fta-security-incident/ (last visited Feb. 10, 2021).

possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

11. Defendant 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 an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party. 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.

II. PARTIES

12. Plaintiff Susan Zebelman is a citizen of Colorado residing in Boulder County, Colorado. Plaintiff's PII was exposed in the Data Breach because the University of Colorado used Accellion FTA to store and/or share Plaintiff's PII.

13. Defendant Accellion, Inc. is a corporation organized under the laws of Delaware, headquartered at 1804 Embarcadero Road, Suite 200, Palo Alto, California.

14. 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 other responsible parties when their identities become known.

15. All of Plaintiff's claims are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

16. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action where the amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one other Class Member (including named Plaintiff Susan Zebelman,

a citizen of Colorado) is a citizen of a state different from Defendant.

17. The Northern District of California has personal jurisdiction over Defendant because Defendant is headquartered in this District and Defendant conducts substantial business in California and this District through its headquarters, offices, parents, and affiliates.

18. Venue is proper in this District under 28 U.S.C. §1391(b) because a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District, including that Defendant implemented and managed Accellion FTA from its headquarters in this District and the breach of Accellion FTA occurred at Defendant's headquarters in this District.

IV. FACTUAL ALLEGATIONS

Background

19. Accellion FTA purportedly allows users to "transfer large and sensitive files securely."

20. Accellion FTA was used to transfer some of Plaintiff's and Class Members most sensitive and confidential information, including names, social security numbers and/or driver's license or state identification numbers, dates of birth, bank account numbers and bank routing numbers, places of employment, and other personal identifiable information, which is static, does not change, and can be used to commit myriad financial crimes.

21. Plaintiff and Class Members relied on this sophisticated Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand security to safeguard their PII.

22. Defendant had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' PII from involuntary disclosure to third parties.

The Data Breach

23. The Data Breach occurred on or around December 20, 2020.[4]

24. Defendant claims it notified its Accellion FTA customers of the Data Breach on

[4] *Id.*

December 23, 2020.[5]

25. On January 12, 2021, Defendant issued a press release stating that it had resolved a vulnerability in Accellion FTI and "released a patch within 72 hours to the less than 50 customers affected."[6]

26. On or around January 15, 2021, the Reserve Bank of New Zealand announced that it was one of the Accellion FTA customers affected by the Data Breach.[7]

27. On or around January 25, 2021, The Australian Securities and Investments Commission ("ASIC") announced that it was one of the Accellion FTA customers affected by the Data Breach.[8]

28. In its announcement, ASIC stated that it learned of the Data Breach on January 15, 2021, raising doubt as to Defendant's claim that it notified all Accellion FTA customers of the Data Breach on December 23, 2020.

29. On or around February 1, 2021, the Office of the Washington State Auditor ("SAO") announced that it was one of the Accellion FTA customers affected by the Data Breach.[9]

30. The SAO's announcement included the following:

> What you need to know
>
> The Office of the Washington State Auditor (SAO) used the online services company Accellion to transfer data. A security incident at Accellion may have allowed unauthorized access to data being used by SAO. Navigate this page using the links below to learn about the incident, what you can do to protect your data, and about our next steps.
>
> ***
>
> Legal notice about the data incident

[5] *Id.*
[6] *See* https://www.accellion.com/company/press-releases/accellion-responds-to-recent-fta-security-incident/ (last visited Feb. 10, 2021).
[7] *See* https://www.itnews.com.au/news/reserve-bank-of-nz-governor-apologises-for-serious-data-breach-559802 (last visited Feb. 10, 2021).
[8] *See* https://asic.gov.au/about-asic/news-centre/news-items/accellion-cyber-incident/ (last visited Feb. 10, 2021).
[9] *See* https://sao.wa.gov/breach2021/ (last visited Feb. 10, 2021).

> The Office of the Washington State Auditor ("SAO") was recently made aware of a security breach involving Accellion, a third party provider of hosted file transfer services. During the week of January 25, 2021, Accellion confirmed that an unauthorized person gained access to SAO files by exploiting a vulnerability in Accellion's file transfer service. Some of the SAO data files contained personal information of Washington state residents who filed unemployment insurance claims in 2020. The compromised files may also include the personal information of other Washington residents who have not yet been identified but whose information was in state agency or local government files under review by the SAO.
>
> This matter is under ongoing investigation by SAO. SAO is committed to providing timely and accurate information about what happened and who is affected when available, as permitted and appropriate. As such, this page will be updated from time to time on the SAO website as SAO obtains additional information.
>
> **What happened:** SAO is advised that an unauthorized person was able to exploit a software vulnerability in Accellion's file transfer service and gain access to files that were being transferred using Accellion's service. Accellion stated that they believe the unauthorized access occurred in late December of 2020. Other customers of this Accellion service were similarly impacted. SAO is currently seeking a full understanding of the timeline of the incident and the status of Accellion's investigation and the investigation by law enforcement. At this time, SAO does not have enough information to draw conclusions about the timing or full scope of what took place. It was not until the week of January 25, 2021, that Accellion confirmed to SAO that SAO files were subject to this attack and provided the information needed for SAO to begin to identify which data files were impacted and individuals whose personal information is in those files.
>
> **What information was involved?** The data files are voluminous and SAO is in the process of reviewing the impacted files to identify the types of data, agencies, and individuals involved. SAO will provide updates about the types of information involved as soon as that information becomes available through the investigation. At this time, SAO has determined that data files from the Employment Security Department (ESD) were impacted. These ESD data files contained unemployment compensation claim information including the person's name, social security number and/or driver's license or state identification number, date of birth, bank account number and bank routing number, and place of employment.
>
> Data files from some local governments and other state agencies were also affected. SAO is diligently reviewing all potentially

> accessed data files to identify which agencies' and local governments' files were impacted and to determine whether those data files contained personal information. SAO will provide updates on these efforts and notify the individuals, agencies, and local governments as soon as possible.
>
> **Resources SAO will provide:** SAO will make resources available to help each affected individual take measures to protect their identity. SAO is currently in the process of arranging for such services and will post that information as soon as it is available.[10]

31. The SAO explained that, prior to the Data Breach, it used Accellion FTA to transfer data files from the Washington State Employment Security Department, which contained the personal information of approximately 1.6 million Washington state residents who filed unemployment insurance claims in 2020 (the "ESD Data Files").[11]

32. The ESD Data Files included PII such as names, social security numbers and/or driver's license or state identification numbers, dates of birth, bank account numbers and bank routing numbers, and places of employment.[12]

33. In its announcement, the SAO stated that "[d]uring the week of January 25, 2021," Defendant confirmed that the ESD Data Files were exposed in the Data Breach, raising doubt as to Defendant's claim that it notified all Accellion FTA customers of the Data Breach on December 23, 2020.[13]

34. On or around February 9, 2021, the University of Colorado (which used Accellion FTA to store and/or share Plaintiff's PII) announced that it was affected by the Data Breach; that PII from prospective and enrolled students, employees, and others may have been compromised; and that the compromised data could include "limited health and clinical data . . . and study and research data."[14]

35. In its announcement, the University of Colorado stated that it was "one of some 300 Accellion customers that were affected by the attack," raising doubt as to Defendant's claim

[10] *See* https://sao.wa.gov/breach2021/ (last visited Feb. 10, 2021).
[11] *Id.*
[12] *Id.*
[13] *Id.*
[14] Ex. A.

that less than 50 customers were affected.[15] Of course, many Accellion customers entrusted Accellion with data from a great number of Class Members.

36. In its announcement, the University of Colorado stated that Defendant notified it of the Data Breach in "late January [2021]," raising doubt as to Defendant's claim that it notified all Accellion FTA customers of the Data Breach on December 23, 2020.[16]

37. On or around February 11, 2021, Singtel, a Singapore telephone company, and QIMR Berghofer, an Australian medical research institute, announced that they were also affected by the Data Breach.

38. On February 16, 2021, the Wall Street Journal reported that the law firm Jones Day was affected by the Data Breach.[17]

39. Plaintiff's and Class Members' unencrypted information may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII of Plaintiff and Class Members.

40. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiff and Class Members, causing their PII to be exposed.

Defendant Acquires, Collects and Stores Plaintiff's and Class Members' PII.

41. Defendant acquired, collected, and stored Plaintiff's and Class Members' PII.

42. At all relevant times, Defendant knew or should have known that its Accellion FTA customers included law firms, government agencies, and universities and that these customers could and would use Accellion FTA to store and/or share sensitive data, including highly confidential PII, because Defendant marketed Accellion FTA as a tool to "transfer large and sensitive files securely."

43. By obtaining, collecting, and storing Plaintiff's and Class Members' PII, Defendant

---

[15] *Id.*

[16] *Id.*

[17] *See* https://www.wsj.com/articles/hacker-claims-to-have-stolen-files-belonging-to-prominent-law-firm-jones-day-11613514532 (last visited Feb. 16, 2021).

assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

44. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiff and the Class Members relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Securing PII and Preventing Breaches

45. Defendant could have prevented this Data Breach by properly securing and encrypting Plaintiff's and Class Members' PII.

46. Defendant's negligence in safeguarding Plaintiff's and Class Members' PII is exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data.

47. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect Plaintiff's and Class Members' PII from being compromised.

48. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[18] 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."[19]

49. The ramifications of Defendant's failure to keep secure Plaintiff's and Class Members' PII are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Value of Personal Identifiable Information

50. The PII of individuals remains of high value to criminals, as evidenced by the prices

[18] 17 C.F.R. § 248.201 (2013).
[19] *Id*.

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.[20] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[21] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[22]

51. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[23]

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

53. Even then, a new Social Security number may not be effective. According to Julie

---

[20] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Jan. 25, 2021).

[21] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed Jan. 25, 2021).

[22] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed Jan. 25, 2021).

[23] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Jan. 25, 2021).

Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[24]

54. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security number, driver's license number or government-issued identification number, name, and date of birth.

55. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[25]

56. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

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

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

> [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.

[24] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last accessed Jan. 25, 2021).

[25] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Jan. 25, 2021).

> As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[26]

59. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding Plaintiff's and Class Members' PII, including social security numbers, driver's license or state identification numbers, and/or dates of birth, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members a result of a breach.

60. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

61. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

Plaintiff Susan Zebelman's Experience

62. In or around 1987, Plaintiff attended graduate school at the University of Colorado. For the past several years, Plaintiff has participated in the University of Colorado's "mini law school." Plaintiff has also participated in a "beetroot juice study" at the University of Colorado. Through these interactions with the University of Colorado, Plaintiff shared her PII. The University of Colorado, in turn, used Accellion FTA to store and/or share Plaintiff's PII.

63. On or around February 13, 2021, Plaintiff learned of the Data Breach via news sources.

64. As a result of learning of the Data Breach, Ms. Zebelman spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the news reports of the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

65. Additionally, Ms. Zebelman is very careful about sharing her PII. She has never

[26] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf (last accessed Jan. 25, 2021).

knowingly transmitted unencrypted PII over the internet or any other unsecured source.

66. Ms. Zebelman stores any documents containing her PII in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

67. Ms. Zebelman suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property that Ms. Zebelman entrusted to Defendant for the purpose of her employment, which was compromised in and as a result of the Data Breach.

68. Ms. Zebelman suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

69. Ms. Zebelman has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially her Social Security number, in combination with her name and bank account information, being placed in the hands of unauthorized third-parties and possibly criminals.

70. Ms. Zebelman has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

71. Plaintiff brings this nationwide class action on behalf of herself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

72. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

> All individuals in the United States whose PII was exposed to unauthorized third parties as a result of the compromise of Accellion FTA on or around December 20, 2020 (the "Nationwide Class").

73. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their 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 their immediate family members.

74. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

75. Numerosity, Fed R. Civ. P. 23(a)(1): The Nationwide Class (the "Class") are so numerous that joinder of all members is impracticable. The ESD Data Files alone contain the PII of approximately 1.6 million individuals. The University of Colorado likely has tens of thousands of current and former students, prospective students, and employees.

76. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class Members;

b. Whether Defendant had a duty not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant had a duty not to use the PII of Plaintiff and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;

e. Whether and when Defendant actually learned of the Data Breach;

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

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

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

i. Whether Defendant adequately addressed and fixed the vulnerabilities which

permitted the Data Breach to occur;

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

k. Whether Plaintiff and Class Members are entitled to actual, damages, and/or statutory damages as a result of Defendant's wrongful conduct;

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

m. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

77. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendant's misfeasance.

78. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members, and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

79. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that she has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

80. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action

treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

81. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

82. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

83. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

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

85. Further, Defendant has acted or refused to act on grounds generally applicable to

the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

86. 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 Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

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

d. Whether Plaintiff and Class Members are third-party beneficiaries of contracts between Defendant and its Accellion FTA customers;

e. Whether Defendant breached the contracts with its Accellion FTA customers and thereby damaged Plaintiff and Class Members;

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

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

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

i. Whether Class Members are entitled to actual damages, statutory damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

\\\

\\\

COUNT I
Negligence
(On Behalf of Plaintiff and the Nationwide Class)

87. Plaintiff and Class Members re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 86.

88. In the course of using Accellion FTA, Defendant's customers stored and shared certain PII, including names, social security numbers and/or driver's license or state identification numbers, dates of birth, bank account numbers and bank routing numbers, and/or places of employment.

89. Plaintiff and the Class Members entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

90. Defendant has or should have knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

91. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII involved an unreasonable risk of harm to Plaintiff and Class Members, even if the harm occurred through the criminal acts of a third party.

92. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that Plaintiff's and Class Members' information in Defendant's possession was adequately secured and protected.

93. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's and Class Members' PII.

94. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and Class Members. That special relationship arose because Defendant knew or should have known that its customers included law firms, government agencies, and universities and that these customers could and would use

Accellion FTA to store and share sensitive information, including Plaintiffs' and Class Members' PII.

95. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or Class Members.

96. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class Members was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

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

98. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and Class Members. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decision not to comply with industry standards for the safekeeping of Plaintiff's and Class Members' PII.

99. Plaintiff and the Class Members had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

100. Defendant was in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

101. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiff and Class Members within Defendant's possession might have been compromised, how it was compromised, and when. Such notice was necessary to allow Plaintiff and the Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

102. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and Class Members.

103. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiff and Class Members during the time the PII was within Defendant's possession or control.

104. Defendant improperly and inadequately safeguarded the PII of Plaintiff and Class Members in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

105. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect its Plaintiff's and Class Members' PII in the face of increased risk of theft.

106. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff's and Class Members' PII.

107. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and Class Members the existence and scope of the Data Breach.

108. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and Class Members, the PII of Plaintiff and Class Members would not have been compromised.

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

110. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

111. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures

to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and Class Members.

112. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

113. Plaintiff and Class Members are within the class of persons that the FTC Act was intended to protect.

114. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

115. As a direct and proximate result of Defendant's 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 is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which may remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII in its continued possession; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

116. As a direct and proximate result of Defendant's 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.

117. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and Class members have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

COUNT II
Third-Party Beneficiary Claim
(On Behalf of Plaintiff and the Nationwide Class)

118. Plaintiff and Class Members re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 86.

119. Defendant and its Accellion FTA customers entered into contracts related to the use of Accellion FTA.

120. As evidenced by Defendant's marketing of Accellion FTA, these contracts required Defendant to keep secure and confidential information stored on and/or shared through Accellion FTA.

121. Plaintiff and Class Members were not parties to these contracts; however, a motivating purpose of Accellion and its Accellion FTA customers was for Plaintiff and Class Members to benefit from these contracts.

122. Defendant knew or should have known that its Accellion FTA customers included law firms, government agencies, and universities and that these customers could and would use Accellion FTA "to transfer large and sensitive files," including sensitive files containing PII, and that it was important such large and sensitive files be transferred "securely" as Defendant advertised.

123. Defendant knew or should have known that its Accellion FTA customers could and would use Accellion FTA to transfer PII of, among others, law firm clients; citizens of the State of Washington; and students and employees of the University of Colorado, such as Plaintiff.

124. Defendant breached the contracts with its Accellion FTA customers by failing to

keep secure and confidential the PII of Plaintiff and Class Members.

125. As a direct and proximate result of Defendant's above-described breach of contract, 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; the illegal sale of the compromised data on the dark web; 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.

COUNT III
Invasion of Privacy
(On Behalf of Plaintiff and the Nationwide Class)

126. Plaintiff and Class Members re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 86.

127. Plaintiff and Class Members had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

128. Defendant owed a duty to Plaintiffs and Class Members to keep their PII contained as a part thereof, confidential.

129. Defendant failed to protect and released to unknown and unauthorized third parties the PII of Plaintiff and Class Members.

130. Defendant allowed unauthorized and unknown third parties access to and examination of the PII of Plaintiff and Class Members, by way of Defendant's failure to protect the PII.

131. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiff and Class Members is highly offensive to a reasonable person.

132. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and Class Members disclosed their PII to Defendant as part of obtaining services from Defendant's customers, but privately with an intention that the PII would be kept confidential

and would be protected from unauthorized disclosure. Plaintiff and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

133. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiff's and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

134. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it was with actual knowledge that their information security practices were inadequate and insufficient.

135. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and Class Members.

136. As a proximate result of the above acts and omissions of Defendant, the PII of Plaintiff and Class Members was disclosed to third parties without authorization, causing Plaintiff and Class Members to suffer damages.

137. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that the PII maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Class.

COUNT IV
Breach of Confidence
(On Behalf of Plaintiff and the Nationwide Class)

138. Plaintiff and Class Members re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 86.

139. At all times during Plaintiff's and Class Members' interactions with Defendant through Defendant's customers, Defendant was fully aware of the confidential and sensitive nature

of Plaintiff's and Class Members' PII that Plaintiff and Class Members provided to Defendant.

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

141. Plaintiff and Class Members provided their PII to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the PII to be disseminated to any unauthorized third parties.

142. Plaintiff and Class Members also provided their PII to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that PII from unauthorized disclosure.

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

144. Due to Defendant's failure to prevent and avoid the Data Breach from occurring, Plaintiff's and Class Members' PII was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

145. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and Class Members have suffered damages.

146. But for Defendant's disclosure of 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. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' PII as well as the resulting damages.

147. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and Class Members' PII. Defendant knew or should have known its methods of accepting and securing Plaintiff's and Class Members' PII was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiff's and Class Members' PII.

148. As a direct and proximate result of Defendant's breach of their confidence with Plaintiff and Class Members, 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 how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which may remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiff and Class Members; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

149. As a direct and proximate result of Defendant's breaches of confidence, 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.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Nationwide Class as defined herein, and appointing Plaintiff and their Counsel to represent the Class;

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

C. 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:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

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

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant 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;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiff's and Class Members' personal identifying information;

v. prohibiting Defendant from maintaining Plaintiff's and Class Members' personal identifying information on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls

and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant 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 personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant 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 Defendant's policies, programs, and systems for protecting personal identifying information;

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

xv. requiring Defendant 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;

xvi. requiring Defendant to implement logging and monitoring programs sufficient

to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment; For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

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

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

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: February 18, 2021

Respectfully Submitted,

/s/ Michael F. Ram

MICHAEL RAM

MICHAEL F. RAM (SBN 104805)
mram@forthepeople.com
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
711 Van Ness Avenue, Suite 500
San Francisco, CA 94102
Telephone: (415) 358-6913
Facsimile: (415) 358-6923

JOHN A. YANCHUNIS
(*Pro Hac Vice application forthcoming*)
RYAN D. MAXEY
(*Pro Hac Vice application forthcoming*)
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505
jyanchunis@ForThePeople.com

rmaxey@ForThePeople.com

M. ANDERSON BERRY (SBN 262879)
LESLIE GUILLON (SBN 222400)
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829
aberry@justice4you.com
lguillon@justice4you.com

Attorneys for Plaintiff