IN THE SUPERIOR COURT FOR THE STATE OF WASHINGTON
IN AND FOR KING COUNTY

JASON STAHL, individually and on behalf of all others similarly situated, Plaintiff, v. ACCELLION USA LLC, a Washington limited liability company, Defendants.	NO. **CLASS ACTION COMPLAINT FOR:** 1. Negligence; 2. Violation of the Washington Consumer Protection Act, RCW § 19.86, *et seq.*

Plaintiff Jason Stahl, by and through his counsel, brings this Class Action Complaint against Defendant ACCELLION USA LLC, a Washington limited liability company ("Accellion") on behalf of himself and all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsel's investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiff brings this class action lawsuit his own behalf, and on behalf of a Class of similarly situated individuals, against Defendant for its failure to protect the sensitive, confidential information of individuals in the state of Washington—including such information as the person's name, social security number and/or driver's license or state identification

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

number, bank account number and bank routing number, and place of employment ("Personal Information").

2. On or about February 1, 2021, the Office of the Washington State Auditor ("SAO") announced that the Personal Information of approximately 1.6 million individuals in the State of Washington was compromised in a data security breach of its file transfer software vendor, Accellion (the "Data Breach").

3. Accellion is a software company that provides hosted file transfer services. Accellion makes and sells a file transfer service product called "FTA." However, as of late 2020, the FTA program was an outdated "legacy product" that was "nearing end-of life"[1] and was vulnerable to compromise. For several years prior to the Data Breach, Accellion had been telling its customers to "upgrade" to Accellion's new, secure file sharing program called kiteworks "to add a critical layer of security."[2]

4. At the time of the Data Breach, the SAO used the legacy FTA program to transfer files.

5. Beginning as early as December 2020, and continuing into January 2021, attackers exploited vulnerabilities in the FTA software to gain unauthorized access to files that were being transferred using the FTA product.

6. The attackers were able to exploit vulnerabilities in Accellion's FTA product to access SAO files containing Personal Information. Included among the SAO files

---

[1] https://www.accellion.com/company/press-releases/accellion-provides-update-to-recent-fta-security-incident/

[2] Accellion, *Upgrade to Accellion kiteworks: Introducing Accellion's Secure and Compliant File Sharing Program*, available at https://www.accellion.com/sites/default/files/resources/datasheet-upgrade-fta-to-kiteworks.pdf (last visited Feb. 1, 2021).

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

compromised in the Data Breach were claims records of over 1.6 million Washington residents who filed unemployment insurance claims between January and December 2020.

7. Defendant was aware that FTA was an inadequately secure product, yet sold this vulnerable product to SAO for the transfer of Personal Information. Defendant's failure to ensure that the FTA provided adequate security protocols jeopardized the Personal Information of millions of Washington residents, including Plaintiff and the Class, fell well short of Defendant's obligations, and also fell short of Plaintiff's and other Class members' reasonable expectations for protection of their information.

8. As a result of Defendant's conduct and the ensuing Data Breach, Plaintiff and the members of the proposed Class have suffered actual damages, and are at imminent risk of future harm, including identity theft and fraud that would result in monetary loss. Accordingly, Plaintiff brings suit, on behalf of himself and Class of all others similarly situated, to seek redress for Defendant's unlawful conduct.

II. PARTIES

9. Plaintiff Stahl is an individual and is a resident of Seattle, King County, Washington. Plaintiff filed for unemployment benefits with the State of Washington in 2020.

10. Defendant ACCELLION USA LLC is a Washington limited liability company, with its main office located at 1804 Embarcadero Rd, Ste 200, Palo Alto, California 94303.

III. JURISDICTION AND VENUE

11. Jurisdiction is appropriate in this Court pursuant to RCW 2.08.010.

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

12. This Court has personal jurisdiction over Defendant because Accellion USA LLC is a resident of the state of Washington that provided file transfer services to the Washington SAO.

13. Venue is proper in this Court pursuant to RCW 4.12.020(3) because, *inter alia*, Plaintiffs reside in King County where the cause of action arose.

IV. FACTUAL BACKGROUND

A. Accellion

14. Accellion is software company that offers a variety of file-sharing platforms to its customers, giving its customers "a simple, secure, private way to share confidential information."[3]

15. Accellion describes itself as a providing a product that "prevents data breaches" and allows its users to transfer files securely:

> The Accellion enterprise content firewall **prevents data breaches** and compliance violations from third party cyber risk. **CIOs and CISOs rely on the Accellion platform for complete visibility, security and control over the communication of IP, PII, PHI, and other sensitive content** across email, **file sharing,** mobile, enterprise apps, web portals, SFTP, and automated inter-business workflows. By consolidating security across third party communication channels, the Accellion content firewall simplifies complex infrastructure and reduces costs, while improving the user experience.[4]

[3] https://www.accellion.com/platform/simple/secure-file-sharing/
[4] *About Accellion*, Accellion.com, https://www.accellion.com/company/ (last visited Feb. 1, 2021) (emphasis added).

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

16. Accellion markets its products as a means by which to safely transfer Personal Information and sensitive content across file sharing:

When employees click the Accellion button, they know it's the safe, secure way to share sensitive information with the outside world.[5]

17. One of Accellion's file transfer products is Accellion FTA. "Accellion FTA helps worldwide enterprises . . . transfer large and sensitive files securely using a 100% private cloud, on-premise or hosted."[6]

18. But even Accellion itself recognizes that its FTA program is inadequate to keep files transfers secure, admitting that "in today's breach-filled, over-regulated world, you need even broader protection and control" than FTA can offer.[7]

19. In a recent interview, Joel York, Accellion's Chief Marketing Officer, said that the Data Breach involved FTA, which he described as a 20-year-old "legacy product." Mr. York said that the company has been encouraging customers to stop using FTA, stating: "It just wasn't designed for these types of threats . . . ."[8]

20. Mr. York's recent statement was not the first of its kind. Although the FTA product was inadequately secure and subject to vulnerabilities and cyberattack threats,

---

[5] *Id.*

[6] *About Accellion*, Accellion.com, https://www.accellion.com/products/fta/ (last visited Feb. 1, 2021)

[7] *Id.*

[8] Jim Brunner & Paul Roberts, *Personal data of 1.6 million Washington unemployment claimants exposed in hack of state auditor*, Seattle Times (Feb. 1, 2021), https://www.seattletimes.com/seattle-news/politics/personal-data-of-1-6-million-washington-unemployment-claimants-exposed-in-hack-of-state-auditor/?utm_source=marketingcloud&utm_medium=email&utm_campaign=BNA_020121185309+BREAKING+Data+compromised+for+1.6+million+Washingtonians_2_1_2021&utm_term=Registered%20User.

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Accellion had been encouraging its users to upgrade to Accellion's newer product, known as kiteworks, for several years.

21. Accellion's Chief Information Security Officer Frank Balonis stated: "Future exploits of [FTA], however, are a constant threat. We have encouraged all FTA customers to migrate to kiteworks for the last three years and have accelerated our FTA end-of-life plans in light of these attacks. We remain committed to assisting our FTA customers, but strongly urge them to migrate to kiteworks as soon as possible."[9]

22. Despite the vulnerabilities in the FTA system, Accellion continued to provide the FTA platform to its customers, including to the SAO. And SAO continued to use Accellion's insecure product to transfer highly sensitive Personal Information.

B. The Data Breach

23. In mid-December 2020, "Accellion was made aware of a zero-day vulnerability in its legacy FTA software."[10]

24. While Accellion made attempts to patch the vulnerability it initially identified, "Accellion identified additional exploits in the ensuing weeks and rapidly developed and released patches to close each vulnerability." *Id.* The cyberattack continued from at least mid-December and into January 2021, as cyber attackers continued to exploit vulnerabilities in the FTA product.

25. During the December 2020 cyber-attack, an unauthorized person was able to exploit a software vulnerability in Accellion's FTA product and gain access to files that were

---

[9] https://www.accellion.com/company/press-releases/accellion-provides-update-to-recent-fta-security-incident/

[10] Press Release: Accellion Provides Update to Recent FTA Security Incident, Accellion.com (Feb. 1, 2021), https://www.accellion.com/company/press-releases/accellion-provides-update-to-recent-fta-security-incident/.

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

being transferred using Accellion's service. SAO was one of Accellion's customers targeted in the attack, along with 50 others.

26. SAO determined that data files from the Washington State Employment Security Department were impacted, including unemployment compensation claim information for more than 1.6 million Washington residents filed between January and December 2020. The unemployment compensation claim information included the person's name, social security number and/or driver's license or state identification number, bank account number and bank routing number, and place of employment.[11]

> "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." *Id.*

C. The Effect of the Data Breach on the Class

27. Given the sensitive nature of the Personal Information stolen in the Data Breach—including names, Social Security numbers, taxpayer identification numbers, and bank account and routing numbers—hackers have the ability to commit identity theft, financial fraud, and other identity-related fraud against Plaintiff and Class members now and into the indefinite future.

28. As a result of the Data Breach, Plaintiff and Class members will have to take a variety of steps to monitor for and safeguard against identity theft, and they are at a much greater risk of suffering such identity theft. In addition, these victims of the Data Breach are at a heightened risk of potentially devastating financial identity theft. As the Bureau of Justice

---

[11] About the Accellion data security breach, Office of the Washington State Auditor, https://sao.wa.gov/breach2021/ (last updated Feb 1, 2021)

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Statistics reports, identity theft causes its victims out-of-pocket monetary losses and costs the nation's economy billions of dollars every year.[12]

29. In fact, many victims of the Data Breach have likely already experienced harms as a result of the Data Breach, including, but not limited to, identity theft, financial fraud, tax fraud, unauthorized lines of credit opened in their names, medical and healthcare fraud, and unauthorized access to their bank accounts. Plaintiff and Class members have spent and will spend time, money, and effort dealing with the fallout of the Data Breach, including purchasing credit protection services, contacting their financial institutions, checking credit reports, and spending time and effort searching for unauthorized activity.

30. The Personal Information exposed in the Data Breach is highly coveted and valuable on underground or black markets. For example, a cyber "black market" exists in which criminals openly post and sell stolen consumer information on underground internet websites known as the "dark web"—exposing consumers to identity theft and fraud for years to come. Identity thieves can use the Personal Information to: (a) create fake credit cards that can be swiped and used to make purchases as if they were the real credit cards; (b) reproduce stolen debit cards and use them to withdraw cash from ATMs; (c) commit immigration fraud; (d) obtain a fraudulent driver's license or ID card in the victim's name; (e) obtain fraudulent government benefits; (f) file a fraudulent tax return using the victim's information; (g) commit medical and healthcare-related fraud; (h) access financial accounts and records; or (i) commit any number of other frauds, such as obtaining a job, procuring housing, or giving false information to police during an arrest.

---

[12] *See* U.S. Dept. of Justice, Bureau of Justice Statistics, *Victims of Identity Theft, 2012* (Dec. 2013), *available at* http://www.bjs.gov/content/pub/pdf/vit12.pdf (last visited Mar. 30, 2015).

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

31. Consumers are injured every time their data is stolen and placed on the dark web—even if they have been victims of previous data breaches. Not only is the likelihood of identity theft increased, but the dark web is not like Google or eBay. It is comprised of multiple and discrete repositories of stolen information. Each data breach puts victims at risk of having their information uploaded to different dark web databases and viewed and used by different criminal actors.

32. Exposure of this information to the wrong people can have serious consequences. Identity theft can have ripple effects, which can adversely affect the future financial trajectories of victims' lives. For example, the Identity Theft Resource Center reports that respondents to their surveys in 2013–2016 described that the identity theft they experienced affected their ability to get credit cards and obtain loans, such as student loans or mortgages.[13] For some victims, this could mean the difference between going to college or not, becoming a homeowner or not, or having to take out a high interest payday loan versus a lower-interest loan.

33. Annual monetary losses from identity theft are in the billions of dollars. According to a Presidential Report on identity theft produced in 2007:

> In addition to the losses that result when identity thieves fraudulently open accounts . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair

[13] Identity Theft Resource Center, *The Aftermath 2017*, https://www.idtheftcenter.org/images/page-docs/Aftermath_2017.pdf (last visited Nov. 22, 2019).

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

> the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.[14]

34. The unauthorized disclosure of Social Security Numbers can be particularly damaging because Social Security Numbers cannot easily be replaced. In order to obtain a new number, a person must prove, among other things, that he or she continues to be disadvantaged by the misuse. Thus, under current rules, no new number can be obtained until damage has been done. Furthermore, as the Social Security Administration warns:

> A new number probably will not solve all your problems. This is because other governmental agencies (such as the Internal Revenue Service and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Also, because credit reporting companies use the number, along with other Personal Information, to identify your credit record, using a new number will not guarantee you a fresh start. This is especially true if your other Personal Information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you will not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit card information is not associated with the new number, the absence of any credit history under the new number may make it more difficult for you to get credit.[15]

35. According to the Attorney General of the United States, Social Security numbers "can be an identity thief's most valuable piece of consumer information."[16] Indeed, as

---

[14] FTC, *Combating Identity Theft A Strategic Plan* (April 2007), available at https://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf (last visited Nov. 22, 2019).

[15] Social Security Administration, *Identity Theft and Your Social Security Number* (June 2017), available at http://www.ssa.gov/pubs/10064.html (last visited Nov. 22, 2019).

[16] *Fact Sheet: The Work of the President's Identity Theft Task Force*, DOJ 06-636, 2006 WL 2679771 (Sep. 19, 2006).

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

explained recently: “The ubiquity of the SSN as an identifier makes it a primary target for both hackers and identity thieves. . . . When data breaches expose SSNs, thieves can use these numbers—usually combined with other pieces of data—to impersonate individuals and apply for loans, housing, utilities, or government benefits. Additionally, this information may be sold on the black market to other hackers.”[17]

36. As the result of the Data Breach, Plaintiff and Class members are likely to suffer economic loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

a. losing the inherent value of their Personal Information;

b. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

c. costs associated with purchasing credit monitoring, credit freezes, and identity theft protection services;

d. lowered credit scores resulting from credit inquiries following fraudulent activities;

e. costs associated with time spent and the loss of productivity or the enjoyment of one’s life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including discovering fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with the repercussions of the Data Breach; and

f. the continued imminent and certainly impending injury flowing from potential fraud and identify theft posed by their Personal Information being in the possession of one or many unauthorized third parties.

37. Even in instances where a consumer is reimbursed for a financial loss due to identity theft or fraud, that does not make that individual whole again, as there is typically

[17] Daniel J. Marcus, *The Data Breach Dilemma: Proactive Solutions for Protecting Consumers' Personal Information*, 68 Duke L.J. 555, 564–65 (2018).

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

significant time and effort associated with seeking reimbursement that is not refunded. The Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" relating to identity theft or fraud.[18]

38. There may also be a significant time lag between when personal information is stolen and when it is actually misused. According to the GAO, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[19]

D. Plaintiff's Individual Allegations

39. Plaintiff Stahl applied for unemployment benefits from the State of Washington in 2020. As part of his application, Plaintiff Stahl was required to provide sensitive Personal Information, including his Social Security number and banking information. Given the highly sensitive nature of the information stolen in the Data Breach, Plaintiff Stahl remains at a substantial and imminent risk of future harm, including identity theft and theft from his bank accounts. Plaintiff Stahl has expended and will be required to expended time and effort monitoring his financial accounts and credit reports.

---

[18] E. Harrell, U.S. Department of Justice, *Victims of Identity Theft, 2014* (revised Nov. 13, 2017), http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited Nov. 22, 2019).

[19] U.S. Government Accountability Office Report to Congressional Requesters, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), http://www.gao.gov/new.items/d07737.pdf (last visited Nov. 22, 2019).

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

V. CLASS ACTION ALLEGATIONS

40. Plaintiff brings this action individually and on behalf of a class (the "Class") preliminarily defined as:

> All individuals residing in the United States whose personal information was compromised in the data breach disclosed by the Washington State Auditor in January 2021.

Excluded from the Class are Defendants; any agent, affiliate, parent, or subsidiary of any Defendant; any entity in which any Defendant has a controlling interest; any officer or director of any Defendant; any successor or assign of any Defendant; and any Judge to whom this case is assigned as well as his or her staff and immediate family.

41. Plaintiff reserves the right to amend the class definition.

42. This action satisfies the numerosity, commonality, typicality, and adequacy requirements of CR 23.

a) **Numerosity.** Plaintiff is a representative of the proposed Class reportedly consisting of approximately one million members—far too many to join in a single action.

b) **Ascertainability.** Class members are readily identifiable from information in Defendant's possession, custody, or control.

c) **Typicality.** Plaintiff's claims are typical of Class members' claims as each arises from the same Data Breach, the same alleged negligence of and/or statutory violations by Defendant, and the same unreasonable manner of notifying individuals regarding the Data Breach.

d) **Adequacy.** Plaintiff will fairly and adequately protect the interests of the proposed Class. His interests do not conflict with Class members' interests and he

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

has retained counsel experienced in complex class action litigation and data privacy to vigorously prosecute this action on behalf of the Class, including in the capacity as lead counsel.

e) **Commonality.** Plaintiff's and Class members' claims raise predominantly common factual and legal questions that can be answered for all Class members through a single class-wide proceeding. For example, to resolve any Class member's claims, it will be necessary to answer the following questions:

A. Whether Defendant sold a file transfer product that was vulnerable to cyberattack and that was inadequate to protect the transfer of sensitive files;

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

C. Whether Defendant's conduct was negligent;

D. Whether Plaintiff and the Class are entitled to damages, treble damages, and/or injunctive relief.

43. In addition to satisfying the prerequisites of CR 23(a), Plaintiff satisfies the requirements for maintaining a class action under CR 23(b). Common questions of law and fact predominate over any questions affecting only individual members, and a class action is superior to individual litigation or any other available methods for the fair and efficient adjudication of the controversy. The damages available to individual plaintiffs are insufficient to make litigation addressing Defendant's privacy practices economically feasible in the absence of the class action procedure.

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

44. In the alternative, class certification is appropriate because Defendant has acted or refused to act on grounds generally applicable to the class, thereby making final injunctive relief appropriate with respect to the members of the Class as a whole.

VI. FIRST CLAIM FOR RELIEF
Negligence
(On Behalf of Plaintiffs and the Class)

45. Plaintiff incorporates by reference all foregoing factual allegations.

46. Defendant negligently sold a product that was vulnerable to a security breach and that was inadequate to safeguard sensitive information and that using its product could lead to attackers gaining access to sensitive information. Defendants did so despite marketing and selling the FTA product as a means by which its customers could to securely transfer sensitive files, including personally identifiable information.

47. It was reasonably foreseeable to Defendant that their failure to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of use of the FTA product could subject customers to breach of the sensitive information, and could thus expose the owners of that information to harm.

48. Furthermore, given the known risk of major data breaches and the knowledge that FTA contained vulnerabilities that could be exploited by hackers to expose sensitive information (as described above), Plaintiff and the Class members are part of a well-defined, foreseeable, finite, and discernible group that was at high risk of having their Personal Information stolen.

49. Defendant owed a duty to Plaintiff and members the Class to ensure that its systems and networks—and the personnel responsible for them—adequately protected their Personal Information.

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

50. Defendant's duty of care arose as a result of Defendant's knowledge that customers trusted its product to protect confidential data. Only Defendant was in a position to ensure that its systems were sufficient to protect against the harm to Plaintiff and the members of the Class from a data breach of explanting FTA's vulnerabilities.

51. In addition, Defendant had a duty to use reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

52. Defendant also had a duty to use reasonable care in protecting confidential data because they committed to comply with industry standards for the protection of Personal Information.

53. Defendant knew, or should have known, of the risks inherent in the vulnerabilities in in the FTA product, and the importance of adequate security to FTA users.

54. By failing to use reasonable measures to secure its FTA product, by continuing to offer the FTA product as a product for secure file transfers of Personal Information despite its vulnerabilities, and by failing to cure those vulnerabilities, Defendant breached its duties to Plaintiff and the Class.

55. Plaintiff and Class members have suffered harm as a result of Defendant's negligence. These victims suffered diminished value of their sensitive information. Plaintiff and Class also lost control over the Personal Information exposed, which subjected each of them to a greatly enhanced risk of identity theft, medical identity theft, credit and bank fraud, Social Security fraud, tax fraud, and myriad other types of fraud and theft, in addition to the time and expenses spent mitigating those injuries and preventing further injury.

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

VII. SECOND CLAIM FOR RELIEF
Violation of the Washington Consumer Protection Act, RCW § 19.86, *et seq.*
(On Behalf of Plaintiff and Class)

56. Plaintiff incorporates by reference all foregoing factual allegations.

57. Defendant is a "person" within the meaning of the Washington Consumer Protection Act, RCW 19.86.010(1), and they conduct "trade" and "commerce" within the meaning of RCW 19.86.010(2).

58. Plaintiff and other members of the Class are "persons" within the meaning of RCW 19.86.010(1).

59. Defendant's failure to safeguard the Personal Information exposed in the Data Breach constitutes an unfair act that offends public policy.

60. Defendant's failure to safeguard the Personal Information compromised in the Data Breach caused substantial injury to Plaintiff and Class members. Defendant's failure is not outweighed by any countervailing benefits to consumers or competitors, and it was not reasonably avoidable by consumers.

61. Defendant's failure to safeguard the Personal Information disclosed in the Data Breach, and its failure to provide timely and complete notice of that Data Breach to the victims, is unfair because these acts and practices are immoral, unethical, oppressive, and/or unscrupulous.

62. Defendant's unfair acts or practices occurred in its trade or business and have and injured and are capable of injuring a substantial portion of the public. Defendant's general course of conduct as alleged herein is injurious to the public interest, and the acts complained of herein are ongoing and/or have a substantial likelihood of being repeated.

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

63. As a direct and proximate result of Defendant's unfair acts or practices, Plaintiff and Class members suffered injury in fact.

64. As a result of Defendant's conduct, Plaintiff and members of the Class have suffered actual damages, including the lost value of their Personal Information; the lost value of their personal data and lost property in the form of their breached and compromised Personal Information (which is of great value to third parties); ongoing, imminent, and certainly impending threat of 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 black market; 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.

65. Plaintiff and Class members are entitled to an order enjoining the conduct complained of herein and ordering Defendant to take remedial measures to prevent similar data breaches; actual damages; treble damages pursuant to RCW § 19.86.090; costs of suit, including reasonable attorneys' fees; and such further relief as the Court may deem proper.

VIII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff makes the following prayer for relief, on behalf of himself and the proposed Class:

A. An order certifying the proposed Class pursuant to Civil Rule 23 and appointing Plaintiff and his counsel to represent the Class;

B. An order awarding Plaintiff and Class members monetary relief, including actual and treble damages and penalties;

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

C. Equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein and compelling Defendant to utilize appropriate methods and policies with respect to maintaining the security of its file transfer products;

D. An award of costs of suit and attorneys' fees, as allowable by law;

E. An award of pre-judgment and post-judgment interest, as provided by law;

F. Leave to amend this Complaint to conform to the evidence produced at trial; and

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

Dated: February 2, 2021

Respectfully submitted,

TOUSLEY BRAIN STEPHENS PLLC

By: *s/ Kim D. Stephens*
Kim D. Stephens, WSBA #11984
kstephens@tousley.com

By: *s/ Jason T. Dennett*
Jason T. Dennett, WSBA #30686
jdennett@tousley.com

By: *s/ Cecily C. Shiel*
Cecily C. Shiel, WSBA #50061
cshiel@tousley.com

1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
Tel: 206.682.5600
Fax: 206.682.2992

4820-1738-9274, v. 2