HON. JOSEPHINE WIGGS-MARTIN

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

JACKIE STONE, NERYS JONES, DAVINA KIM, and JEAN DEFOND, individually and on behalf of all others similarly situated, Plaintiffs, v. ACCELLION USA LLC, a Washington limited liability company; and THE OFFICE OF THE WASHINGTON STATE AUDITOR, Defendants.	NO. 21-2-01439-5 SEA **FIRST AMENDED CLASS ACTION COMPLAINT FOR:** 1. Negligence; 2. Violation of the Washington Consumer Protection Act, RCW § 19.86, *et seq.*

Plaintiffs Jackie Stone, Nerys Jones, Davina Kim, and Jean DeFond, by and through their counsel, bring this Class Action Complaint against Defendants ACCELLION USA LLC, a Washington limited liability company and THE OFFICE OF THE WASHINGTON STATE AUDITOR ("SAO"), individually and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsel's investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Accellion is a cybersecurity company that until very recently marketed and sold an antiquated product named "FTA" or File Transfer Appliance. Since Accellion

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

introduced the FTA roughly 20 years ago, it boasted of FTA's ability to securely transfer files over the internet. But Accellion knew that the aging FTA product was no longer secure. And while it encouraged its customers to switch to a better system, it still allowed them to gamble with the security of the information stored in and transferred with the FTA. The Office of the Washington State Auditor was one of those customers. Not only did it ignore Accellion's warnings, it used the "end-of-life" FTA product to transfer incredibly sensitive personal information on over 1.5 million Washington residents. When hackers predictably compromised the FTA product in December 2020, they quickly exfiltrated those records and distributed them to active criminal identity theft rings. The State of Washington has already admitted that many of those records already are being used for fraud.

2. Plaintiffs bring this class action lawsuit individually and on behalf of a Class of similarly situated individuals, against Defendants for their failure to protect the sensitive, confidential information of individuals in the state of Washington—including their names, Social Security numbers, driver's license or state identification numbers, bank account numbers, bank routing numbers, and places of employment ("Personal Information").

3. On or about February 1, 2021, the SAO announced that Personal Information from approximately 1.6 million unemployment claims was compromised in a data security breach of the FTA product the SAO licensed from Accellion (the "Data Breach"). In addition, the SAO announced that data in its possession from other, unspecified, state agencies and local governments was included in the breach.

4. Accellion is a cybersecurity software and hardware company that offers secure file sharing and collaboration systems. Accellion makes and sells the FTA file transfer appliance. As of late 2020, the FTA was an outdated "legacy product" that was "nearing end-of

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

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 newer, purportedly secure file sharing program called kiteworks "to add a critical layer of security."[2]

5. At the time of the Data Breach, the SAO was in the process of migrating to the new kiteworks system. The Data Breach, however, affected data the SAO stored in the legacy FTA product despite the security risks.

6. By December 2020, and continuing into January 2021, attackers exploited vulnerabilities in the FTA to gain unauthorized access to files that were being transferred or stored using the FTA.

7. The attackers were able to exploit vulnerabilities in Accellion's FTA product to access SAO files containing Personal Information. Included among the SAO files compromised in the Data Breach were records from over 1.6 million unemployment insurance claims between 2017 and 2020.

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

---

[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

9. The SAO was aware that FTA was an inadequately secure product, having been advised for years that it was a legacy product and to upgrade to kiteworks. By continuing to use legacy software despite warnings about its vulnerabilities, the SAO fell short of its obligations, and also fell short of Plaintiffs' and other class members' reasonable expectations for protection of their information.

10. As a result of Defendants' conduct and the ensuing Data Breach, Plaintiffs 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, Plaintiffs bring suit, on their own behalf and on behalf of a Class of all others similarly situated, to seek redress for Defendants' unlawful conduct.

II. PARTIES

11. Plaintiff Jackie Stone is an individual and is a resident of King County, Washington. Plaintiff Stone filed for unemployment benefits with the State of Washington in 2020.

12. Plaintiff Nerys Jones is an individual and is a resident of King County, Washington. Plaintiff Jones filed for unemployment benefits with the State of Washington in 2020.

13. Plaintiff Davina Kim is an individual and is a resident of King County, Washington. Plaintiff Kim filed for unemployment benefits with the State of Washington in 2020.

14. Plaintiff Jane DeFond is an individual and is a resident of King County, Washington. Plaintiff DeFond's personal information was used by someone without authorization in a submission for unemployment benefits with the State of Washington in 2020.

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

15. 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.

16. Defendant OFFICE OF THE WASHINGTON STATE AUDITOR is a branch of the Washington State government with its main office located at 302 Sid Snyder Ave. SW, Olympia, Washington 98504.

III. JURISDICTION AND VENUE

17. Jurisdiction is appropriate in this Court pursuant to RCW 2.08.010 and RCW 4.92.090.

18. This Court has personal jurisdiction over Accellion because Accellion USA LLC is a resident of the State of Washington, and Accellion contracted to provide file transfer services in Washington to the Washington SAO. This Court has personal jurisdiction over the Washington State Auditor because it is a branch of the Washington State government.

19. Venue is proper in this Court pursuant to RCW 4.92.010(1) and RCW 4.12.020(3) because Plaintiffs reside in King County where the cause of action arose.

IV. FACTUAL BACKGROUND

A. Accellion

20. Accellion is a cybersecurity company that markets purportedly secure file transfer applications, among other products and services. Accellion offers a variety of file-sharing platforms to its customers, giving them "a simple, secure, private way to share confidential information."[3]

[3] https://www.accellion.com/platform/simple/secure-file-sharing/

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

21. Accellion even sells a product that it claims "prevents data breaches": 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]

22. 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]**

23. Until very recently, Accellion continued to offer its 20-year-old legacy file transfer product, called Accellion FTA. "Accellion FTA helps worldwide enterprises . . . transfer large and sensitive files securely using a 100% private cloud, on-premise or hosted."[6] Accellion FTA devices are standalone servers, managed by Accellion, that are used specifically for encrypted file transfer.[7] FTA could be used, in particular, for transferring large volumes of

---

[4] *About Accellion*, Accellion.com, https://www.accellion.com/company/ (last visited Feb. 1, 2021) (emphasis added).

[5] *Id.*

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

[7] https://blog.qualys.com/vulnerabilities-research/2021/04/02/qualys-update-on-accellion-fta-security-incident#original

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

data.[8] As a result, files on an FTA server were, by definition, designated as sensitive information requiring secure transmission.

24. But Accellion itself recognizes that the FTA is inadequate to keep file transfers secure, admitting that "in today's breach-filled, over-regulated world, you need even broader protection and control" than FTA can offer.[9]

25. 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 . . . ."[10]

26. Mr. York's recent statement was not the first of its kind. Because the FTA product was inadequately secure and subject to vulnerabilities and cyberattacks, Accellion had been encouraging its users to upgrade to Accellion's newer product, known as Kiteworks, for several years.[11]

27. 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

---

[8] https://www.cpomagazine.com/cyber-security/1-6-million-washington-state-unemployment-claimants-have-financial-information-exposed-in-hack-of-state-auditors-office/

[9] *Id.*

[10] 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.

[11] https://www.accellion.com/company/security-updates/accellion-announces-end-of-life-eol-for-its-legacy-fta-product/

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

light of these attacks. We remain committed to assisting our FTA customers, but strongly urge them to migrate to kiteworks as soon as possible."[12]

28. In fact, FTA used the CentOS 6 operating system—despite the fact that in late 2019, CentOS announced that it would no longer support CentOS 6 after November 2020.[13] Accellion informed its FTA customers of CentOS 6's end-of-life in or around August 2020 and informed its customers that Accellion would be less able to support the FTA software as a result.[14]

29. Despite the vulnerabilities in the FTA system, Accellion continued to provide the FTA platform to approximately 300 customers,[15] including to the SAO. And SAO continued to use Accellion's insecure product to transfer highly sensitive Personal Information.

B. The Data Breach

30. In mid-December 2020, "Accellion was made aware of a zero-day vulnerability in its legacy FTA software."[16] A zero-day vulnerability is one that was previously unknown to the software vendor and which it has no patch to fix.[17] Such a vulnerability can be exploited immediately by malicious actors.

---

[12] 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/

[13] https://www.techrepublic.com/article/kroger-data-breach-highlights-urgent-need-to-replace-legacy-end-of-life-tools/

[14] https://www.accellion.com/company/security-updates/accellion-announces-end-of-life-eol-for-its-legacy-fta-product/

[15] https://www.accellion.com/company/press-releases/accellion-provides-update-to-fta-security-incident-following-mandiants-preliminary-findings/

[16] 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/.

[17] https://us.norton.com/internetsecurity-emerging-threats-how-do-zero-day-vulnerabilities-work-30sectech.html

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

31. During the December 2020 attack, hackers exploited two zero-day vulnerabilities in FTA. One of the vulnerabilities used in the December 2020 attack involved SQL Injection.[18] SQL Injection is one of the most common attack mechanisms used by hackers, and it is most often used to attack websites.[19] In a SQL Injection attack, a malicious actor uses a vulnerability associated with a user input field, like a username or password field. Instead of inputting the text expected (like a username), the malicious actor inputs computer code. In a successful SQL Injection attack, the hacker-inputted code tricks the targeted system into running the hacker's code instead of the normal command, which can result in the hacker gaining access to other information on the server and even other systems on the same network.[20] Developers can take several steps to protect against SQL Injection attacks, including validating user input to ensure it is in the proper format and sanitizing it to remove any malicious code. These are standard precautions taught in undergraduate coding programs, which Accellion should have followed.

32. In the December 2020 attack, after gaining access to Accellion FTA servers via the SQL Injection attack, hackers were able to upload a web shell called DEWMODE, which gave the hackers broader access onto the affected FTA servers. DEWMODE is what the hackers used to extract information and download files from the FTA.

33. Accellion did not detect the cyberattack on its own. It only learned of the attack when one of the breached FTA users detected suspicious activity on or around December

[18] https://www.accellion.com/sites/default/files/trust-center/accellion-fta-attack-mandiant-report-full.pdf

[19] https://security.berkeley.edu/education-awareness/best-practices-how-tos/system-application-security/how-protect-against-sql

[20] https://security.berkeley.edu/education-awareness/best-practices-how-tos/system-application-security/how-protect-against-sql

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

16, 2020. Despite knowing that there were attacks underway, Accellion did not release security patches to fix the exploited vulnerabilities until December 20 and December 23, 2020. Even then, Accellion kept the attacks quiet and did not engage an independent forensic investigator to probe the FTA for additional vulnerabilities.

34. When Accellion took no action, the hackers struck again. On or around January 20, 2021, hackers began a second wave of attacks, exploiting brand new vulnerabilities. Through these vulnerabilities, hackers were again able to upload a variant of the DEWMODE web shell. DEWMODE was then used for the remainder of the January attack.[21]

35. Accellion learned of these attacks on January 22, 2021, and issued a critical security alert, advising its FTA customers to shut down their FTA systems immediately. Accellion released patches to fix the vulnerabilities involved in the January attack on January 25 and January 28, 2021.

36. Following the January attack, Accellion engaged cyber security firm FireEye, also known as Mandiant, to perform forensic analysis and a security assessment of the Data Breach.[22] Cyber security experts typically recommend best practices for responding to a data breach include bringing in a third-party expert to manage the investigation and forensic analysis.[23] FireEye, however, has a vested interest in convincing the world that the Accellion breach was limited to the end-of-life FTA system and did not have broader ramifications for

---

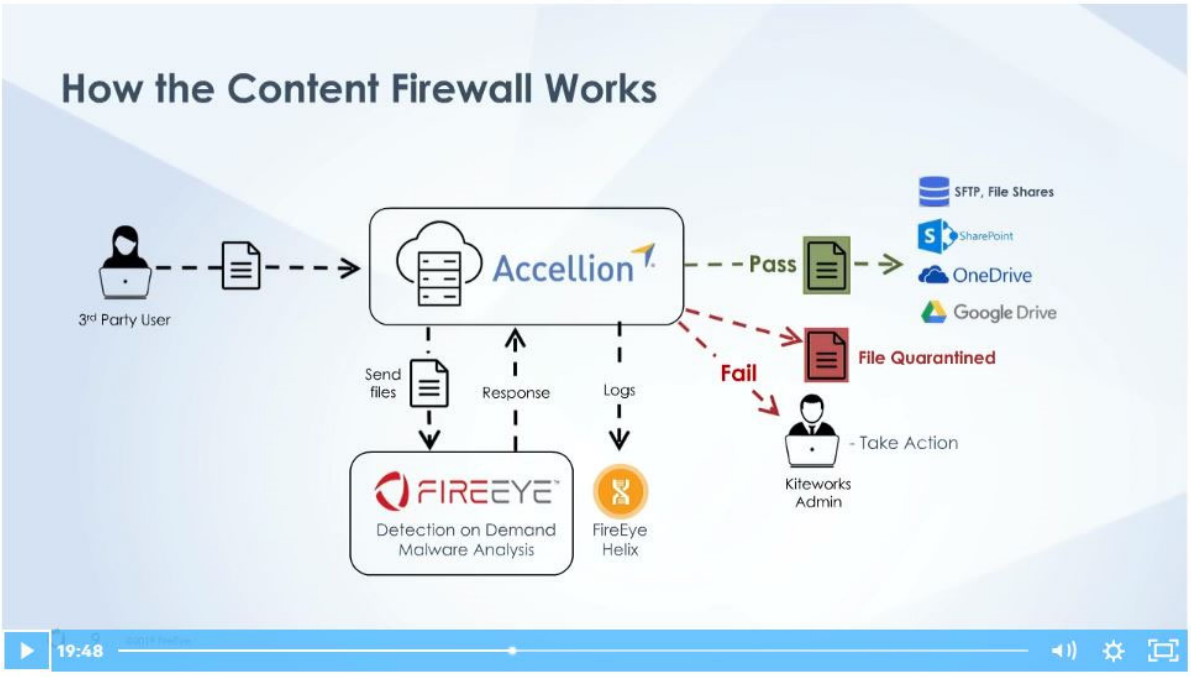
[21] https://security.berkeley.edu/education-awareness/best-practices-how-tos/system-application-security/how-protect-against-sql

[22] https://www.accellion.com/sites/default/files/trust-center/accellion-fta-attack-mandiant-report-full.pdf

[23] *See, e.g.*, http://www.experian.com/assets/data-breach/white-papers/data-breach-incidents-to-resolution.pdf; https://digitalguardian.com/blog/data-breach-experts-share-most-important-next-step-you-should-take-after-data-breach-2014-2015

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

Accellion's other products and services. In fact, FireEye jointly markets cybersecurity products and services with Accellion, as the promotional video from Accellion's website indicates.[24]



37. FireEye / Mandiant began the forensic analysis and security assessment on February 4, 2021. Mandiant's review relied on forensic images of just 10 instances in which Accellion's FTA was compromised, the majority of which reflected activity associated with the December 2020 cyberattack.[25] Mandiant's report concluded that the four vulnerabilities exploited in the January and December attacks were of critical severity because they allowed for unauthenticated remote code execution, that is the ability to execute malicious code on a remote system without being logged in (authenticated) as a valid user.[26]

---

[24] Press Release: FireEye and Accellion Launch Join Solution For Malware Protection (Mar. 19, 2020), https://www.fireeye.com/blog/products-and-services/2020/03/fireeye-accellion-launch-joint-solution-for-malware-protection.html.

[25] https://www.accellion.com/sites/default/files/trust-center/accellion-fta-attack-mandiant-report-full.pdf

[26] https://www.accellion.com/sites/default/files/trust-center/accellion-fta-attack-mandiant-report-full.pdf

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

38. Mandiant concluded that both the December and January attacks demonstrated familiarity with the inner workings of the FTA platform, likely obtained through reverse engineering. For example, the attackers knew how to navigate FTA's internal databases and how to utilize other internal scripts within the FTA platform. In addition, the malware used in both was programmed to run a cleanup routine, which would seek to remove forensic evidence of the attack by modifying or removing log files and other files that would track how the attack worked.[27]

39. In addition to identifying the vulnerabilities exploited by hackers in the December and January attacks, Mandiant's assessment uncovered two additional vulnerabilities which had not been previously identified by Accellion, including one ranked as "high severity."[28]

40. Following Mandiant's investigation, Accellion announced that it was "accelerat[ing] FTA's end-of-life to April 30, 2021[,] and [that they] continue[d] to strongly urge all FTA customers that have not done so already to upgrade to the [newer] platform as soon as possible."[29] In its end-of-life announcement, Accellion emphasized that FTA is a "20 year old legacy product [and] [f]or the past three years, Accellion has been attempting to move its existing FTA customers over to [their] modern and more secure platform, Kiteworks."[30] While Accellion has announced the "end of life" for its legacy FTA effective on April 30,

---

[27] https://www.accellion.com/sites/default/files/trust-center/accellion-fta-attack-mandiant-report-full.pdf

[28] https://www.accellion.com/sites/default/files/trust-center/accellion-fta-attack-mandiant-report-full.pdf

[29] https://www.accellion.com/company/press-releases/mandiant-issues-final-report-regarding-accellion-fta-attack/

[30] https://www.accellion.com/company/security-updates/accellion-announces-end-of-life-eol-for-its-legacy-fta-product/

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

2021, its states that it will continue to "honor its FTA contracts for the duration of its existing licensing terms."[31]

41. Beginning in late January 2021, organizations that had been affected by the data breaches began receiving extortion emails threatening to publish stolen data on the "CLOP^_- LEAKS" .onion website.[32] Since then, the hackers have continued to post parts of the data in phases.[33]

42. Mandiant has attributed the attack on Accellion's FTA to a criminal hacking cluster it refers to as UNC2546, and it has attributed the extortion activity to a cluster it calls UNC2582.[34] Mandiant has identified "compelling" overlaps between the two sets of malicious activities and previous attacks carried out by a group labeled FIN11, including similar targets and use of the same IP addresses and/or email accounts. The prefix "FIN" in FIN11 indicates that Mandiant believes FIN 11 is a financially motivated hacking group. In other words, FIN 11 and its associated hackers in UNC2546 and UNC2582 are looking for ways to make money off of the information they obtained, which means they are selling it to criminals.

C. Washington State Auditor

43. The SAO audits state agencies, local governments, schools, and institutions of higher education in Washington for compliance with state, federal, and local laws, including

---

[31] Rob Daughtry, FTA End of Life Effective April, 20, 2021 (Feb. 25, 2021), https://www.accellion.com/company/security-updates/accellion-announces-end-of-life-eol-for-its-legacy-fta-product/

[32] https://www.fireeye.com/blog/threat-research/2021/02/accellion-fta-exploited-for-data-theft-and-extortion.html

[33] https://blog.qualys.com/vulnerabilities-research/2021/04/02/qualys-update-on-accellion-fta-security-incident#original

[34] https://thehackernews.com/2021/02/hackers-exploit-accellion-zero-days-in.html; https://www.fireeye.com/blog/threat-research/2021/02/accellion-fta-exploited-for-data-theft-and-extortion.html

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

financial audits, special investigations of fraud, and performance audits. SAO issues annual reports regarding government agencies in Washington.

44. On January 12, 2021, SAO learned that data stored in its Accellion file-transfer account had been exfiltrated by malicious actors. SAO has acknowledged that the affected data included personal information regarding people who applied for unemployment benefits from the Employment Security Department (ESD) from 2017 to 2020. Specifically, the information may have included names, Social Security numbers, dates of birth, street and email addresses, and bank account and routing numbers.[35] News reports indicate that at least 1.3 million Washingtonians' Personal Information was compromised in the data breach.[36] This included people whose personal information was in the ESD files because of fraudulent unemployment claims submitted on their behalf in an unrelated incident last year.[37]

45. State Auditor Pat McCarthy stated that information from 100 local governments and 25 state agencies may have been compromised in the breach, but in addition to the ESD, only identified the Department of Children, Youth and Families by name.[38]

46. In late summer 2020, SAO began migrating from FTA to Kiteworks, Accellion's new platform which Accellion had been advising its clients to use.[39] According to SAO, it completed this process on December 31, 2020. Nonetheless, SAO failed to secure the millions of records it left vulnerable within the Accellion FTA.

---

[35] https://sao.wa.gov/breach2021/

[36] https://www.seattletimes.com/seattle-news/politics/washington-state-lawmakers-grill-auditor-aides-over-disclosure-of-massive-data-breach/

[37] https://www.king5.com/article/news/local/washington-state-auditor-accellion-security-breach/281-874c1a9c-e61c-4ca5-bec8-b27e621d676f

[38] https://www.seattletimes.com/seattle-news/politics/personal-data-of-1-6-million-washington-unemployment-claimants-exposed-in-hack-of-state-auditor/

[39] https://sao.wa.gov/breach2021/

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

47. Following the data breach, several Washington state senators questioned why SAO stored so much data as part of the audit. State Senator Karen Keiser asked, "Was it truly necessary for the audit of ESD to include all this personal financial data from ESD claimants?"[40] Other legislators have explained that cybersecurity experts recommend minimizing collection of sensitive data in order to reduce the harm posed by any potential breach.[41]

48. On February 1, 2021, SAO announced the Data Breach to the public.

C. The Effect of the Data Breach on the Class

49. 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 Plaintiffs and Class members now and into the indefinite future.

50. As a result of the Data Breach, Plaintiffs 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

[40] 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

[41] https://www.seattletimes.com/seattle-news/politics/washington-state-lawmakers-grill-auditor-aides-over-disclosure-of-massive-data-breach/

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.[42]

51. In fact, many victims of the Data Breach have 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. Plaintiffs 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.

52. 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.

---

[42] *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

53. 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.

54. 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.[43] 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.

55. 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

[43] 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.[44]

56. 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.[45]

57. According to the Attorney General of the United States, Social Security numbers "can be an identity thief's most valuable piece of consumer information."[46] Indeed, as

---

[44] 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).

[45] 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).

[46] *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."[47]

58. As the result of the Data Breach, Plaintiffs 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.

59. 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

[47] 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.[48]

60. 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.[49]

D. Plaintiffs' Individual Allegations

Jackie Stone:

61. Plaintiff Stone applied for unemployment benefits from the State of Washington in or around April 2020. As part of the application, Plaintiff Stone was required to provide sensitive Personal Information, including her Social Security number and banking information.

62. Plaintiff Stone has already experienced ID theft as a result of the Data Breach. In January 2021, Plaintiff Stone received a call from the Washington Department of Licensing (DOL) informing her that an unauthorized individual attempted to renew her driver license.

---

[48] 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).

[49] 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

DOL informed Plaintiff Stone that DOL had reason to believe that her information was included in the data breach, and that the information obtained in the data breach was used in the unauthorized attempt to renew her license. In addition, DOL told Plaintiff Stone that they knew of at least 500 other people whose data had been breached.

63. Plaintiff Stone was told that she would probably receive a bill in the mail for the fraudulent license renewal and did in fact receive that bill. In addition, as a result of the breach, DOL told Plaintiff Stone that she needed to obtain a new driver's license and close her credit cards, bank account, and freeze her credit. On the advice of DOL, Plaintiff Stone has spent her own time to close her credit cards, bank account, and freeze her credit.

64. In recent months, Plaintiff Stone noticed unauthorized charges on her credit card. Plaintiff Stone was forced to close that credit card.

65. Given the highly sensitive nature of the information stolen in the Data Breach, Plaintiff Stone remains at a substantial and imminent risk of future harm, including identity theft and theft from her bank accounts. Plaintiff Stone has expended and will be required to expended time and effort monitoring her financial accounts and credit reports.

Nerys Jones:

66. Plaintiff Jones applied for unemployment benefits from the State of Washington in 2020. As part of the application, Plaintiff Jones was required to provide sensitive Personal Information, including Social Security number and banking information.

67. Given the highly sensitive nature of the information stolen in the Data Breach, Plaintiff Jones remains at a substantial and imminent risk of future harm, including identity theft and theft from his bank accounts. Plaintiff Jones has expended and will be required to expended time and effort monitoring his financial accounts and credit reports.

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

Davina Kim:

68. Plaintiff Kim applied for unemployment benefits from the State of Washington in 2020. As part of the application, Plaintiff Kim was required to provide sensitive Personal Information, including Social Security number and banking information.

69. Given the highly sensitive nature of the information stolen in the Data Breach, Plaintiff Kim remains at a substantial and imminent risk of future harm, including identity theft and theft from his bank accounts. Plaintiff Kim has expended and will be required to expended time and effort monitoring her financial accounts and credit reports.

Jean DeFond:

70. In 2020, an unauthorized individual used Plaintiff DeFond's information to falsely, and without knowledge of Plaintiff DeFond, apply for unemployment benefits from the State of Washington in Plaintiff DeFond's name. Accordingly, the State of Washington held sensitive Personal Information of Plaintiff DeFond.

71. Given the highly sensitive nature of the information stolen in the Data Breach, Plaintiff DeFond remains at a substantial and imminent risk of future harm, including identity theft and theft from her bank accounts. Plaintiff DeFond has expended time to freeze her credit and change passwords as a result of the Data Breach. Plaintiff DeFond has expended and will be required to expended time and effort monitoring her financial accounts and credit reports.

V. CLASS ACTION ALLEGATIONS

72. Plaintiffs bring 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.

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

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.

73. Plaintiffs reserve the right to amend the class definition.

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

a) **Numerosity.** Plaintiffs are representatives of the proposed Class reportedly consisting of over one million members—far too many to join in a single action.

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

c) **Typicality.** Plaintiffs' 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 Defendants, and the same unreasonable manner of notifying individuals regarding the Data Breach.

d) **Adequacy.** Plaintiffs will fairly and adequately protect the interests of the proposed Class. Their interests do not conflict with Class members' interests and they have 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.** Plaintiffs' and Class members' claims raise predominantly common factual and legal questions that can be answered for all Class

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

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 Accellion sold a file transfer product that was vulnerable to cyberattack and that was inadequate to protect the transfer of sensitive files;

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

C. Whether Defendants' conduct was negligent;

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

75. In addition to satisfying the prerequisites of CR 23(a), Plaintiffs satisfy 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 Defendants' privacy practices economically feasible in the absence of the class action procedure.

76. In the alternative, class certification is appropriate because Defendants have 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.

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

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

77. Plaintiffs incorporate by reference all foregoing factual allegations.

78. Defendant Accellion sold a product that was vulnerable to a security breach and that was inadequate to safeguard sensitive information such that using its product could lead to attackers gaining access to sensitive information. Defendant Accellion informed its customers, such as Defendant SAO, that the FTA product was an end of life product and advised them to switch to a more secure product.

79. It was reasonably foreseeable to Defendant SAO that its failure to implement and maintain reasonable security procedures and practices, and its failure to use adequately secure file transfer and storage systems, would leave the sensitive information in its systems vulnerable to breach and could thus expose the owners of that information to harm.

80. 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), Plaintiffs 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.

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

82. Defendant SAO's duty of care arose as a result of Defendant's knowledge that individuals trusted the State to protect their confidential data that they provided to it. Only the

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

State was in a position to ensure that its own protocols were sufficient to protect against the harm to Plaintiffs and the members of the Class from a data breach of its own systems.

83. In addition, Defendant SAO had duties 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.

84. Defendant SAO also had duties to use reasonable care in protecting confidential data because it committed to comply with industry standards for the protection of Personal Information.

85. Defendant SAO knew, or should have known, of the risks inherent in the vulnerabilities in the FTA product, and the importance of adequate security to FTA users and the owners of sensitive data.

86. By using an inadequately secure file transfer and storage system for the transfer and storage of Plaintiffs' data, Defendant SAO breached its duties to Plaintiffs and the Class.

87. Plaintiffs and Class members have suffered harm as a result of Defendant SAO's negligence. These victims suffered diminished value of their sensitive information. Plaintiffs and members of the 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

88. Consistent with RCW 4.92.100, Plaintiffs Kim and Jones, on their own behalf and on behalf of the Class they seek to represent, presented Tort Claim Forms to the Washington Department of Enterprise Services, Office of Risk Management for the State's tortious conduct as set forth herein. More than sixty calendar days have elapsed after their claims were presented. *See* RCW 4.92.100.

VII. SECOND CLAIM FOR RELIEF
Negligence
(On Behalf of Plaintiffs and the Class against Defendant Accellion)

89. Plaintiffs incorporate by reference all foregoing factual allegations.

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

91. It was reasonably foreseeable to Defendant Accellion that its 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.

92. 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), Plaintiffs 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.

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

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

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

95. In addition, Defendant Accellion had duties 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.

96. Defendant Accellion also had duties to use reasonable care in protecting confidential data because it committed to comply with industry standards for the protection of Personal Information.

97. Defendant Accellion knew, or should have known, of the risks inherent in the vulnerabilities in the FTA product, and the importance of adequate security to FTA users and the owners of sensitive data.

98. 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 Accellion breached its duties to Plaintiffs and the Class.

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

99. Plaintiffs and Class members have suffered harm as a result of Defendant Accellion's negligence. These victims suffered diminished value of their sensitive information. Plaintiffs and members of the 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.

VIII. THIRD CLAIM FOR RELIEF
Violation of the Washington Consumer Protection Act, RCW § 19.86, *et seq.*
(On Behalf of Plaintiffs and Class against Defendant Accellion)

100. Plaintiffs incorporate by reference all foregoing factual allegations.

101. Defendant Accellion 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). Plaintiffs and other members of the Class are "persons" within the meaning of RCW 19.86.010(1).

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

103. Defendant Accellion's failure to safeguard the Personal Information compromised in the Data Breach caused substantial injury to Plaintiffs 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.

104. Defendant Accellion'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

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

the victims, is unfair because these acts and practices are immoral, unethical, oppressive, and/or unscrupulous.

105. Defendant Accellion'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 Accellion'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.

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

107. As a result of Defendant Accellion's conduct, Plaintiffs 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.

108. Plaintiffs and Class members are entitled to an order enjoining the conduct complained of herein and ordering Defendant Accellion to take remedial measures to prevent

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

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.

IX. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs makes the following prayer for relief, individually and on behalf of the proposed Class:

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

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

C. Equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein and compelling Defendants 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: April 8, 2021

Respectfully submitted,

TOUSLEY BRAIN STEPHENS PLLC

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

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

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

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

By: *s/ Kaleigh N. Powell*
Kaleigh N. Powell, WSBA #52684
kpowell@tousley.com

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

GIBBS LAW GROUP LLP

By: *s/ David M. Berger*
David M. Berger (*pro hac vice forthcoming*)
dmb@classlawgroup.com

By: *s/ Jeffrey Kosbie*
Jeffrey Kosbie (*pro hac vice forthcoming*)
jbk@classlawgroup.com

505 14th St, Suite 1110
Oakland, CA 94612
Tel: (510) 350-9700
Fax: (510) 350-9701

4820-7781-1172, v. 4