

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

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

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

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

21 4. Accellion is a cybersecurity software and hardware company that offers secure
22 file sharing and collaboration systems. Accellion makes and sells the FTA file transfer
23 appliance. As of late 2020, the FTA was an outdated “legacy product” that was “nearing end-of-
24

1 life”¹ and was vulnerable to compromise. For several years prior to the Data Breach, Accellion
2 had been telling its customers to “upgrade” to Accellion’s newer, purportedly secure file
3 sharing program called kiteworks “to add a critical layer of security.”²

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

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

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

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

21 ¹ <https://www.accellion.com/company/press-releases/accellion-provides-update-to-recent-fta-security-incident/>

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

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.

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/>

1 21. Accellion even sells a product that it claims “prevents data breaches”: The
2 Accellion enterprise content firewall **prevents data breaches** and compliance violations from
3 third party cyber risk. **CIOs and CISOs rely on the Accellion platform for complete**
4 **visibility, security and control over the communication of IP, PII, PHI, and other sensitive**
5 **content** across email, **file sharing**, mobile, enterprise apps, web portals, SFTP, and automated
6 inter-business workflows. By consolidating security across third party communication
7 channels, the Accellion content firewall simplifies complex infrastructure and reduces costs,
8 while improving the user experience.⁴

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

11 **When employees click the Accellion button, they know it’s the safe, secure**
12 **way to share sensitive information with the outside world.**⁵

13 23. Until very recently, Accellion continued to offer its 20-year-old legacy file
14 transfer product, called Accellion FTA. “Accellion FTA helps worldwide enterprises . . .
15 transfer large and sensitive files securely using a 100% private cloud, on-premise or hosted.”⁶
16 Accellion FTA devices are standalone servers, managed by Accellion, that are used specifically
17 for encrypted file transfer.⁷ FTA could be used, in particular, for transferring large volumes of
18
19
20

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

22 ⁵ *Id.*

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

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

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

3 24. But Accellion itself recognizes that the FTA is inadequate to keep file
4 transfers secure, admitting that “in today’s breach-filled, over-regulated world, you need even
5 broader protection and control” than FTA can offer.⁹

6 25. In a recent interview, Joel York, Accellion’s Chief Marketing Officer, said
7 that the Data Breach involved FTA, which he described as a 20-year-old “legacy product.”
8 Mr. York said that the company has been encouraging customers to stop using FTA, stating: “It
9 just wasn’t designed for these types of threats”¹⁰

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

14 27. Accellion’s Chief Information Security Officer Frank Balonis stated: “Future
15 exploits of [FTA], however, are a constant threat. We have encouraged all FTA customers to
16 migrate to kiteworks for the last three years and have accelerated our FTA end-of-life plans in
17

18 ⁸ <https://www.cpmagazine.com/cyber-security/1-6-million-washington-state-unemployment-claimants-have-financial-information-exposed-in-hack-of-state-auditors-office/>

19 ⁹ *Id.*

20 ¹⁰ Jim Brunner & Paul Roberts, *Personal data of 1.6 million Washington unemployment*
21 *claimants exposed in hack of state auditor*, Seattle Times (Feb. 1, 2021),
22 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.

23 ¹¹ <https://www.accellion.com/company/security-updates/accellion-announces-end-of-life-eol-for-its-legacy-fta-product/>
24

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

3 28. In fact, FTA used the CentOS 6 operating system—despite the fact that in late
4 2019, CentOS announced that it would no longer support CentOS 6 after November 2020.¹³
5 Accellion informed its FTA customers of CentOS 6’s end-of-life in or around August 2020 and
6 informed its customers that Accellion would be less able to support the FTA software as a
7 result.¹⁴

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

11 **B. The Data Breach**

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

17 ¹² Press Release: Accellion Provides Update to Recent FTA Security Incident,
18 Accellion.com (Feb. 1, 2021), <https://www.accellion.com/company/press-releases/accellion-provides-update-to-recent-fta-security-incident/>

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

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

21 ¹⁵ <https://www.accellion.com/company/press-releases/accellion-provides-update-to-fta-security-incident-following-mandiant-preliminary-findings/>

22 ¹⁶ Press Release: Accellion Provides Update to Recent FTA Security Incident,
23 Accellion.com (Feb. 1, 2021), <https://www.accellion.com/company/press-releases/accellion-provides-update-to-recent-fta-security-incident/>.

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

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

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

18 33. Accellion did not detect the cyberattack on its own. It only learned of the
19 attack when one of the breached FTA users detected suspicious activity on or around December
20

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

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

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

1 16, 2020. Despite knowing that there were attacks underway, Accellion did not release security
2 patches to fix the exploited vulnerabilities until December 20 and December 23, 2020. Even
3 then, Accellion kept the attacks quiet and did not engage an independent forensic investigator
4 to probe the FTA for additional vulnerabilities.

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

9 35. Accellion learned of these attacks on January 22, 2021, and issued a critical
10 security alert, advising its FTA customers to shut down their FTA systems immediately.
11 Accellion released patches to fix the vulnerabilities involved in the January attack on January
12 25 and January 28, 2021.

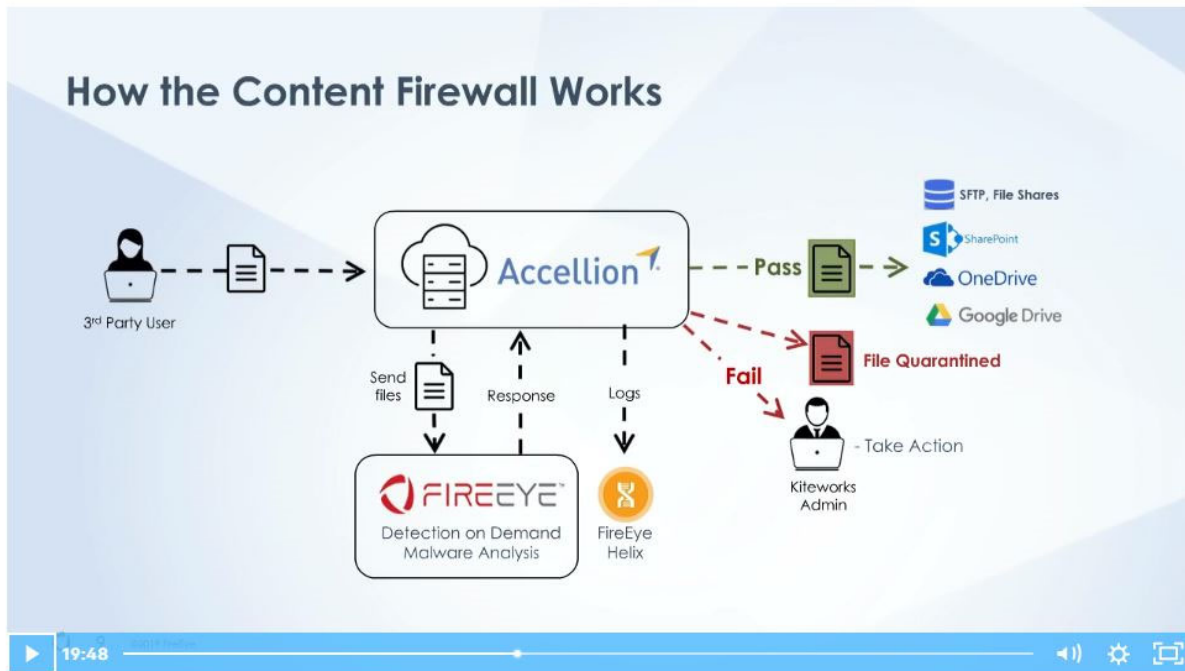
13 36. Following the January attack, Accellion engaged cyber security firm FireEye,
14 also known as Mandiant, to perform forensic analysis and a security assessment of the Data
15 Breach.²² Cyber security experts typically recommend best practices for responding to a data
16 breach include bringing in a third-party expert to manage the investigation and forensic
17 analysis.²³ FireEye, however, has a vested interest in convincing the world that the Accellion
18 breach was limited to the end-of-life FTA system and did not have broader ramifications for
19
20

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

23 ²² [https://www.accellion.com/sites/default/files/trust-center/accellion-fta-attack-](https://www.accellion.com/sites/default/files/trust-center/accellion-fta-attack-mandiant-report-full.pdf)
24 [mandiant-report-full.pdf](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-](http://www.experian.com/assets/data-breach/white-papers/data-breach-incidents-to-resolution.pdf)
[incidents-to-resolution.pdf](http://www.experian.com/assets/data-breach/white-papers/data-breach-incidents-to-resolution.pdf); [https://digitalguardian.com/blog/data-breach-experts-share-most-](https://digitalguardian.com/blog/data-breach-experts-share-most-important-next-step-you-should-take-after-data-breach-2014-2015)
[important-next-step-you-should-take-after-data-breach-2014-2015](https://digitalguardian.com/blog/data-breach-experts-share-most-important-next-step-you-should-take-after-data-breach-2014-2015)

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



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

20

21 ²⁴ Press Release: FireEye and Accellion Launch Joint 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>.

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

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

24

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

8 39. In addition to identifying the vulnerabilities exploited by hackers in the
9 December and January attacks, Mandiant’s assessment uncovered two additional vulnerabilities
10 which had not been previously identified by Accellion, including one ranked as “high
11 severity.”²⁸

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

18 While Accellion has announced the “end of life” for its legacy FTA effective on April 30,

20 ²⁷ [https://www.accellion.com/sites/default/files/trust-center/accellion-fts-attack-](https://www.accellion.com/sites/default/files/trust-center/accellion-fts-attack-mandiant-report-full.pdf)
21 mandiant-report-full.pdf

22 ²⁸ [https://www.accellion.com/sites/default/files/trust-center/accellion-fts-attack-](https://www.accellion.com/sites/default/files/trust-center/accellion-fts-attack-mandiant-report-full.pdf)
23 mandiant-report-full.pdf

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

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

1 2021, its states that it will continue to “honor its FTA contracts for the duration of its existing
2 licensing terms.”³¹

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

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

15 **C. Washington State Auditor**

16 43. The SAO audits state agencies, local governments, schools, and institutions of
17 higher education in Washington for compliance with state, federal, and local laws, including
18

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

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

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

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

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

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

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

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

20 ³⁵ <https://sao.wa.gov/breach2021/>

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

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

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

24 ³⁹ <https://sao.wa.gov/breach2021/>

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

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

8 **C. The Effect of the Data Breach on the Class**

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

14 50. As a result of the Data Breach, Plaintiffs and Class members will have to take
15 a variety of steps to monitor for and safeguard against identity theft, and they are at a much
16 greater risk of suffering such identity theft. In addition, these victims of the Data Breach are at
17 a heightened risk of potentially devastating financial identity theft. As the Bureau of Justice
18
19
20

21 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

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

1 Statistics reports, identity theft causes its victims out-of-pocket monetary losses and costs the
2 nation's economy billions of dollars every year.⁴²

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

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

22
23 ⁴² See U.S. Dept. of Justice, Bureau of Justice Statistics, *Victims of Identity Theft, 2012*
24 (Dec. 2013), available at <http://www.bjs.gov/content/pub/pdf/vit12.pdf> (last visited Mar. 30, 2015).

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

7 54. Exposure of this information to the wrong people can have serious
8 consequences. Identity theft can have ripple effects, which can adversely affect the future
9 financial trajectories of victims' lives. For example, the Identity Theft Resource Center reports
10 that respondents to their surveys in 2013–2016 described that the identity theft they
11 experienced affected their ability to get credit cards and obtain loans, such as student loans or
12 mortgages.⁴³ For some victims, this could mean the difference between going to college or not,
13 becoming a homeowner or not, or having to take out a high interest payday loan versus a lower-
14 interest loan.

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

17 In addition to the losses that result when identity thieves fraudulently open accounts
18 . . . individual victims often suffer indirect financial costs, including the costs
19 incurred in both civil litigation initiated by creditors and in overcoming the many
20 obstacles they face in obtaining or retaining credit. Victims of non-financial identity
21 theft, for example, health-related or criminal record fraud, face other types of harm
22 and frustration.

21 In addition to out-of-pocket expenses that can reach thousands of dollars for the
22 victims of new account identity theft, and the emotional toll identity theft can take,
23 some victims have to spend what can be a considerable amount of time to repair

23 ⁴³ Identity Theft Resource Center, *The Aftermath 2017*,
24 https://www.idtheftcenter.org/images/page-docs/Aftermath_2017.pdf (last visited Nov. 22,
2019).

1 the damage caused by the identity thieves. Victims of new account identity theft,
2 for example, must correct fraudulent information in their credit reports and monitor
3 their reports for future inaccuracies, close existing bank accounts and open new
4 ones, and dispute charges with individual creditors.⁴⁴

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

10 A new number probably will not solve all your problems. This is because other
11 governmental agencies (such as the Internal Revenue Service and state motor
12 vehicle agencies) and private businesses (such as banks and credit reporting
13 companies) likely will have records under your old number. Also, because credit
14 reporting companies use the number, along with other Personal Information, to
15 identify your credit record, using a new number will not guarantee you a fresh start.
16 This is especially true if your other Personal Information, such as your name and
17 address, remains the same.

18 If you receive a new Social Security Number, you will not be able to use the old
19 number anymore.

20 For some victims of identity theft, a new number actually creates new problems. If
21 the old credit card information is not associated with the new number, the absence
22 of any credit history under the new number may make it more difficult for you to
23 get credit.⁴⁵

24 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

21 ⁴⁴ FTC, *Combating Identity Theft A Strategic Plan* (April 2007), available at
22 [https://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-](https://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf)
23 [plan/strategicplan.pdf](https://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf) (last visited Nov. 22, 2019).

24 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).

1 explained recently: “The ubiquity of the SSN as an identifier makes it a primary target for both
2 hackers and identity thieves. . . . When data breaches expose SSNs, thieves can use these
3 numbers—usually combined with other pieces of data—to impersonate individuals and apply
4 for loans, housing, utilities, or government benefits. Additionally, this information may be sold
5 on the black market to other hackers.”⁴⁷

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

- 9 a. losing the inherent value of their Personal Information;
- 10 b. costs associated with the detection and prevention of identity theft and
11 unauthorized use of their financial accounts;
- 12 c. costs associated with purchasing credit monitoring, credit freezes, and
13 identity theft protection services;
- 14 d. lowered credit scores resulting from credit inquiries following fraudulent
15 activities;
- 16 e. costs associated with time spent and the loss of productivity or the
17 enjoyment of one’s life from taking time to address and attempt to mitigate
18 and address the actual and future consequences of the Data Breach,
19 including discovering fraudulent charges, cancelling and reissuing cards,
20 purchasing credit monitoring and identity theft protection services,
21 imposing withdrawal and purchase limits on compromised accounts, and
22 the stress, nuisance and annoyance of dealing with the repercussions of the
23 Data Breach; and
- 24 f. the continued imminent and certainly impending injury flowing from potential
fraud and identity 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).

1 significant time and effort associated with seeking reimbursement that is not refunded. The
2 Department of Justice’s Bureau of Justice Statistics found that identity theft victims “reported
3 spending an average of about 7 hours clearing up the issues” relating to identity theft or fraud.⁴⁸

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

7 [L]aw enforcement officials told us that in some cases, stolen data may be held
8 for up to a year or more before being used to commit identity theft. Further, once
9 stolen data have been sold or posted on the Web, fraudulent use of that
10 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

11 **D. Plaintiffs’ Individual Allegations**

12 **Jackie Stone:**

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

17 62. Plaintiff Stone has already experienced ID theft as a result of the Data Breach.
18 In January 2021, Plaintiff Stone received a call from the Washington Department of Licensing
19 (DOL) informing her that an unauthorized individual attempted to renew her driver license.
20

21 ⁴⁸ E. Harrell, U.S. Department of Justice, *Victims of Identity Theft, 2014* (revised Nov.
22 13, 2017), <http://www.bjs.gov/content/pub/pdf/vit14.pdf> (last visited Nov. 22, 2019).

23 ⁴⁹ U.S. Government Accountability Office Report to Congressional Requesters, *Data*
24 *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).

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

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

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

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

16 **Nervys Jones:**

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

20 67. Given the highly sensitive nature of the information stolen in the Data Breach,
21 Plaintiff Jones remains at a substantial and imminent risk of future harm, including identity
22 theft and theft from his bank accounts. Plaintiff Jones has expended and will be required to
23 expended time and effort monitoring his financial accounts and credit reports.
24

1 **Davina Kim:**

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

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

9 **Jean DeFond:**

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

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

19 **V. CLASS ACTION ALLEGATIONS**

20 72. Plaintiffs bring this action individually and on behalf of a class (the "Class")
21 preliminarily defined as:

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

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

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

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

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

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

13 c) **Typicality.** Plaintiffs' claims are typical of Class members' claims as
14 each arises from the same Data Breach, the same alleged negligence of and/or statutory
15 violations by Defendants, and the same unreasonable manner of notifying individuals
16 regarding the Data Breach.

17 d) **Adequacy.** Plaintiffs will fairly and adequately protect the interests of
18 the proposed Class. Their interests do not conflict with Class members' interests and
19 they have retained counsel experienced in complex class action litigation and data
20 privacy to vigorously prosecute this action on behalf of the Class, including in the
21 capacity as lead counsel.

22 e) **Commonality.** Plaintiffs' and Class members' claims raise
23 predominantly common factual and legal questions that can be answered for all Class
24

1 members through a single class-wide proceeding. For example, to resolve any Class
2 member's claims, it will be necessary to answer the following questions:

- 3 A. Whether Defendant Accellion sold a file transfer product that was
4 vulnerable to cyberattack and that was inadequate to protect the transfer
5 of sensitive files;
- 6 B. Whether Defendants failed to implement and maintain reasonable
7 security procedures and practices appropriate to the nature and scope of
8 the information compromised in the Data Breach;
- 9 C. Whether Defendants' conduct was negligent;
- 10 D. Whether Plaintiffs and the Class are entitled to damages, treble damages,
11 and/or injunctive relief.

12 75. In addition to satisfying the prerequisites of CR 23(a), Plaintiffs satisfy the
13 requirements for maintaining a class action under CR 23(b). Common questions of law and
14 fact predominate over any questions affecting only individual members, and a class action is
15 superior to individual litigation or any other available methods for the fair and efficient
16 adjudication of the controversy. The damages available to individual plaintiffs are insufficient
17 to make litigation addressing Defendants' privacy practices economically feasible in the
18 absence of the class action procedure.

19 76. In the alternative, class certification is appropriate because Defendants have
20 acted or refused to act on grounds generally applicable to the class, thereby making final
21 injunctive relief appropriate with respect to the members of the Class as a whole.
22
23
24

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

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

3 83. In addition, Defendant SAO had duties to use reasonable security measures
4 under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits
5 “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the
6 FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

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

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

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

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

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

6
7 **VII. SECOND CLAIM FOR RELIEF**
8 **Negligence**
9 **(On Behalf of Plaintiffs and the Class against Defendant Accellion)**

10 89. Plaintiffs incorporate by reference all foregoing factual allegations.

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

16 91. It was reasonably foreseeable to Defendant Accellion that its failure to
17 implement and maintain reasonable security procedures and practices appropriate to the nature
18 and scope of use of the FTA product could subject customers to breach of the sensitive
19 information, and could thus expose the owners of that information to harm.

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

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

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

8 95. In addition, Defendant Accellion had duties to use reasonable security
9 measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which
10 prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced
11 by the FTC, the unfair practice of failing to use reasonable measures to protect confidential
12 data.

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

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

19 98. By failing to use reasonable measures to secure its FTA product, by continuing
20 to offer the FTA product as a product for secure file transfers of Personal Information despite
21 its vulnerabilities, and by failing to cure those vulnerabilities, Defendant Accellion breached its
22 duties to Plaintiffs and the Class.

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

8
9 **VIII. THIRD CLAIM FOR RELIEF**
10 **Violation of the Washington Consumer Protection Act, RCW § 19.86, *et seq.***
11 **(On Behalf of Plaintiffs and Class against Defendant Accellion)**

12 100. Plaintiffs incorporate by reference all foregoing factual allegations.

13 101. Defendant Accellion is a "person" within the meaning of the Washington
14 Consumer Protection Act, RCW 19.86.010(1), and they conduct "trade" and "commerce"
15 within the meaning of RCW 19.86.010(2). Plaintiffs and other members of the Class are
16 "persons" within the meaning of RCW 19.86.010(1).

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

19 103. Defendant Accellion's failure to safeguard the Personal Information
20 compromised in the Data Breach caused substantial injury to Plaintiffs and Class members.
21 Defendant's failure is not outweighed by any countervailing benefits to consumers or
22 competitors, and it was not reasonably avoidable by consumers.

23 104. Defendant Accellion's failure to safeguard the Personal Information disclosed
24 in the Data Breach, and its failure to provide timely and complete notice of that Data Breach to

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

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

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

10 107. As a result of Defendant Accellion's conduct, Plaintiffs and members of the
11 Class have suffered actual damages, including the lost value of their Personal Information; the
12 lost value of their personal data and lost property in the form of their breached and
13 compromised Personal Information (which is of great value to third parties); ongoing,
14 imminent, and certainly impending threat of identity theft crimes, fraud, and abuse, resulting in
15 monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the
16 illegal sale of the compromised data on the dark web black market; expenses and/or time spent
17 on credit monitoring and identity theft insurance; time spent scrutinizing bank statements,
18 credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts;
19 decreased credit scores and ratings; lost work time; and other economic and non-economic
20 harm.

21 108. Plaintiffs and Class members are entitled to an order enjoining the conduct
22 complained of herein and ordering Defendant Accellion to take remedial measures to prevent
23
24

1 similar data breaches; actual damages; treble damages pursuant to RCW § 19.86.090; costs of
2 suit, including reasonable attorneys' fees; and such further relief as the Court may deem proper.

3 4 **IX. PRAYER FOR RELIEF**

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

- 7 A. An order certifying the proposed Class pursuant to Civil Rule 23 and appointing
8 Plaintiffs and their counsel to represent the Class;
- 9 B. An order awarding Plaintiffs and Class members monetary relief, including
10 actual and treble damages and penalties;
- 11 C. Equitable relief enjoining Defendants from engaging in the wrongful conduct
12 complained of herein and compelling Defendants to utilize appropriate methods
13 and policies with respect to maintaining the security of its file transfer products;
- 14 D. An award of costs of suit and attorneys' fees, as allowable by law;
- 15 E. An award of pre-judgment and post-judgment interest, as provided by law;
- 16 F. Leave to amend this Complaint to conform to the evidence produced at trial; and
- 17 G. Such other and further relief as this Court may deem just and proper.

18 Dated: April 8, 2021

Respectfully submitted,

19 TOUSLEY BRAIN STEPHENS PLLC

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

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

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

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

5 1700 Seventh Avenue, Suite 2200
6 Seattle, Washington 98101
7 Tel: 206.682.5600
Fax: 206.682.2992

8 GIBBS LAW GROUP LLP

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

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

13 505 14th St, Suite 1110
14 Oakland, CA 94612
Tel: (510) 350-9700
Fax: (510) 350-9701

15
16
17 4820-7781-1172, v. 4
18
19
20
21
22
23
24

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Nearly \\$3.1M Washington State Auditor Settlement Ends Lawsuit Over December 2020 Data Breach](#)
