Julian Hammond (SBN 268489)
jhammond@hammondlawpc.com
Polina Brandler (SBN 269086)
pbrandler@hammondlawpc.com
Ari Cherniak (SBN 290071)
acherniak@hammondlawpc.com
Steven Resnick (*pro hac vice pending*)
sresnick@hammondlawpc.com
HAMMONDLAW, PC
11780 W. Sample Road, Suite 1103
Coral Springs, FL 33065
Tel: (310) 601-6766
Fax: (310) 295-2385

Attorneys for Plaintiff and the Putative Class

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

MADALYN BROWN, individually and on behalf of all others similarly situated,

Plaintiff,

vs.

ACCELLION, INC., a Delaware Corporation,

Defendant.

Case No.: 5:21-1155

CLASS ACTION COMPLAINT FOR:

1. Negligence;
2. Violation of Washington State Consumer Protection Act, RCW 19.86.010;

DEMAND FOR JURY TRIAL

Plaintiff Madalyn Brown ("Plaintiff"), on behalf of herself and all others similarly situated (hereinafter "Class Members"), complains and alleges as follows:

OVERVIEW OF CLAIMS

1. This is a class action, under Federal Rule of Civil Procedure 23, brought on behalf of individuals whose private information, including names, dates of birth, Social Security numbers, driver's license numbers and/or state identification numbers, bank account information, and employment information (collectively "Personally Identifiable Information" or "PII") was exposed because of the failure of Accellion, Inc. ("Accellion" or "Defendant") to safeguard and protect the sensitive information of Plaintiff and the Class Members.

2. In January 2021, Accellion, a software company, providing services to the Washington State Auditor's Office (the "SAO"), announced that unauthorized individuals gained access to SAO files by exploiting a vulnerability in Accellion's file transfer service. This unauthorized access began in December 2020 and continued into January 2021 (the "Data Breach"). The SAO files contained the PII of Washington residents who filed unemployment insurance claims in 2020. In addition, the compromised files may have included the PII of other Washington residents whose information was contained in state agency and/or local government files.

3. On February 1, 2021, the Washington State Auditor's Office confirmed that PII belonging to approximately 1.6 million people in Washington was compromised as a result of the Data Breach.

4. Accellion is a cloud computing company focused on file sharing and collaboration solutions.[1] Accellion developed, marketed, and sold a file sharing transfer product called "File Transfer Appliance" ("FTA") for use in overcoming limits imposed on the size of email attachments.[2] Rather than transferring documents by email, the intended recipient would receive a link to files hosted on Accellion's FTA, which could then be viewed or downloaded. *Id.*

5. At the time of the Data Breach, the SAO was using Accellion's FTA product to transfer and/or receive files and Accellion knew that SAO was using the FTA product to transfer and/or receive files containing PII.

[1] https://en.wikipedia.org/wiki/Accellion

[2] https://www.bankinfosecurity.com/blogs/accellion-mess-what-went-wrong-p-2989

6. As of 2020, however, FTA was an outdated product "nearing end-of-life."[3] Nevertheless, Accellion continued to market and sell the FTA product to SAO and other entities for use in transferring files containing PII.

7. In December 2020 and continuing into January 2021, unknown threat actors exploited vulnerabilities in the FTA software and gained access to SAO files. The SAO files contained the records of approximately 1.6 million Washington residents who filed claims for unemployment insurance in 2020.

8. Accellion's failure to ensure that the FTA product provided adequate security protocols exposed the PII of more than one million Washington residents, including Plaintiff and the Class Members. As a result of Defendant's conduct, the PII of Plaintiff and the Class was compromised and their PII was disclosed to unknown and unauthorized third parties without their consent.

9. Armed with the PII acquired in this type of cyberattack, threat actors can commit a variety of crimes including, e.g., opening new financial accounts in class members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, and obtaining driver's licenses in Class Members' names but with another person's photograph.

10. As a result of the Data Breach, Plaintiff and the Class Members have and will continue to incur out of pocket costs and expenses for, among other things, purchasing credit monitoring services, credit freezes, credit reports, and/or other protective measures to deter and detect identity theft. Plaintiff and the Class Members have and will continue to spend time, resources, and money in order to mitigate their damages from the Data Breach.

11. As a result of the Data Breach, Plaintiff and the Class Members are at a heightened and imminent risk of fraud and identity theft. Plaintiff and the Class Members must now and in the future closely monitor their bank accounts and credit card accounts to guard against the risk of identity theft.

12. Plaintiff brings this class action lawsuit on behalf of herself and all those similarly situated to address Accellion's inadequate safeguarding of Class Members' PII.

JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million exclusive of interest and

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

costs. At least one Plaintiff and one Defendant are citizens of different states. There are more than 100 putative Class Members.

14. This Court has personal jurisdiction over Defendant because its principal place of business is in California and has sufficient contacts in this District.

15. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because Defendant conducts substantial business in this District and California is the principal place of business for Defendant.

PARTIES

16. Plaintiff Madalyn Brown is an adult individual who resides, and at all relevant times, has resided in Eatonville Washington. Plaintiff Madalyn Brown filed an unemployment claim with the State of Washington in 2020 and her PII was exposed in the Data Breach. She is referred to in this Complaint as "Plaintiff."

17. Accellion, Inc. is a Delaware Corporation with headquarters in Palo Alto, California.

FACTUAL ALLEGATIONS

18. Accellion is a Palo Alto, California-based private cloud solutions company focused on secure file sharing and collaboration.[4] Users of Accellion's file transfer products can access, edit, and share enterprise content from any device while maintaining compliance and security. *Id.*

19. Accellion markets its products as way to safely transfer sensitive information via file sharing. With regard to file sharing, Accellion's website states in relevant part:

Shared Files and Folders | Secure File Sharing

- Give users a simple, secure, private way to share confidential information
- Provide the same ease of use found in consumer cloud file sharing apps
- Designated business users give external parties access privileges to folders and individual files, such as watermarked view-only, download, and upload/edit
- Designated business users request files from external partners so they can upload sensitive content in compliance
- Ensure productivity with tight integration to email, mobile, office and enterprise apps[5]

20. According to its website, 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

[4] https://en.wikipedia.org/wiki/Accellion

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

sensitive content across email, file sharing, mobile, enterprise apps, web portals, SFTP, and automated inter-business workflow…When employees click the Accellion button, they know it's the safe, secure way to share sensitive information with the outside world." [6]

21. Accellion developed, marketed, and sold a file transfer product called Accellion FTA. According to its website, "Accellion FTA helps worldwide enterprises… transfer large and sensitive files securely using a 100% private cloud, on-premises or hosted."[7]

22. Accellion was aware that its FTA program was inadequate to keep file transfer secure. With regard to the FTA product, Acccellion's website states that "in today's breach-filled, over-regulated world, you need even broader protection and control. Protect all your external file sharing – no matter what the source, device or location – with the industry-leading governance and security of Accellion's new platform." *Id*.

23. By the end of 2020, Accellion's product was nearing "end of life."[8] In fact, in a recent interview, Joel York, Accellion's chief marketing officer, said the data breach involved the company's 20-year-old "legacy product," known as FTA, which the company has been encouraging customers to stop using. With regard to the FTA product, Mr. York stated, "It just wasn't designed for these types of threats."[9]

24. In mid-December 2020, Accellion was made aware of a "zero-day vulnerability" in its legacy FTA software.[10] A zero-day vulnerability is a software security flaw that is known to the software vendor but does not have a patch in place to fix the flaw. It has the potential to be exploited by cybercriminals.

25. Accellion attempted to patch the vulnerability, however, the company identified additional exploits in the ensuing weeks and attempted to release patches to close each vulnerability. *Id*. The Data Breach began in December 2020 and continued into January 2021, as cyber attackers repeatedly exploited vulnerabilities in the FTA product.

---

[6] https://www.accellion.com/company/

[7] https://www.accellion.com/products/fta/

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

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

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

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.