Hassan A. Zavareei (SBN 181547)
Tycko &Zavareei LLP
1828 L Street NW, Suite 1000
Washington, D.C. 20036
Telephone: 202-973-0900
Facsimile: 202-973-0950
hzavareei@tzlegal.com
kaizpuru@tzlegal.com

Attorneys for Plaintiffs and the Proposed Class
(Additional Counsel on Signature Page)

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

AMIRESSE DESJARDINS, *individually and on behalf of all others similarly situated*, **Plaintiffs,** **v.** **ACCELLION, INC.,** **Defendant.**	**CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL** Case No. 5:21-cv-4743

Plaintiff Amiresse DesJardins ("Plaintiff"), individually and on behalf of all other persons similarly situated, and through her attorneys of record, alleges the following against Defendant Accellion, Inc. ("Accellion" or "Defendant") based upon personal knowledge with respect to herself, on information and belief derived from investigation of counsel, and review of public documents as to all other matters.

INTRODUCTION

1. Plaintiff brings this action against Defendant for its failure to properly secure and safeguard personally identifiable information ("PII") that was stored on and/or shared with Defendant's File Transfer Appliance ("FTA") software. Although representing its product as

"help[ing] worldwide enterprises . . . transfer large and sensitive files,"[1] Accellion failed to safeguard sensitive PII of Plaintiff and Class Members, including, without limitation, names, email addresses and other contact information, dates of birth, Social Security numbers and/or driver's license or state identification numbers, bank account numbers and bank routing numbers, medical records, academic records, places of employment and/or salary information.

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

3. In December 2020, an unauthorized person exploited two vulnerabilities in Accellion's FTA software to access the files and data that numerous customers of Defendant, including Kroger, had stored on or shared with Accellion FTA ("December Exploit"). On December 20, 2020, Accellion released software patches to address the vulnerabilities targeted in the December Exploit and to increase the frequency of Accellion's checks for anomalous activity. However, Accellion failed to detect any additional vulnerabilities. In January 2021, an unauthorized person exploited two separate vulnerabilities in Accellion's software to once again access files and data stored on or shared by numerous consumers with Accellion FTA ("January Exploit").[2]

4. As a result of the December and January Exploits (collectively, the "Data Breach"), an unauthorized person or persons accessed files and data shared through or stored on Accellion's FTA software.

5. Institutions impacted include government entities, universities, law firms, and medical providers.

---

[1] *See Accellion FTA*, ACCELLION, https://www.accellion.com/products/fta/.

[2] *See* Mandiant (FireEye), *Accellion, Inc.: File Transfer Appliance (FTA) Security Assessment* (Mar. 1, 2021) (hereinafter, "Mandiant Report"), https://www.accellion.com/sites/default/files/trust-center/accellion-fta-attack-mandiant-report-full.pdf.

6. Because these organizations had used Accellion FTA to transfer and store the sensitive information and PII of their customers, clients, patients, and employees, as a result of the Data Breach, unauthorized persons accessed information and data containing the PII of Plaintiff and Class Members, including, without limitation, names, email addresses and other contact information, dates of birth, Social Security numbers and/or driver's license or state identification numbers, bank account numbers and bank routing numbers, medical records, academic records, places of employment and/or salary information.

7. Already, information obtained as a result of the Data Breach, including Social Security numbers, tax information, academic records, and medical records, have been posted on a website called Clop that is run by cybercriminals and that is known to publish samples of stolen data and then demand a ransom not to publish the rest of the information.[3]

8. As a result of Accellion's failure to protect the information it was entrusted with, Plaintiff and Class Members have been exposed to and/or are at a significant risk of identity theft, financial fraud, and other identity-related fraud into the indefinite future. Plaintiff and Class Members have also lost the inherent value of their PII.

PARTIES

9. Plaintiff Amiresse DesJardins is a citizen of Tennessee, residing in Davidson County. Ms. DesJardins is a former employee of Kroger, having worked there as an Overnight Cashier from April 2017 to February 2018. Ms. DesJardins received notice of the Data Breach from Kroger on or about February 19, 2021. Plaintiff's PII was exposed in the Data Breach because the Kroger Family of Companies used Accellion FTA to store and/or share Plaintiff's PII.

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

[3] Lindsay McKenzie, *Secure File Sharing Compromises University Security*, INSIDE HIGHER ED (Apr. 7, 2020), https://www.insidehighered.com/news/2021/04/07/accellion-data-security-breach-latest-hit-universities.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of $5,000,000 exclusive of interest and costs, there are more than 100 putative class members, and minimal diversity exists because putative class members (including named Plaintiff Amiresse DesJardins) are citizens of a different state from Accellion.

12. This Court has personal jurisdiction over Accellion because Accellion is authorized to and regularly conducts business in California and is headquartered in Palo Alto, California.

13. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claim occurred in this District. Accellion is headquartered in this District, implemented and managed Accellion FTA from its headquarters in this district, and the Data Breach occurred at its headquarters in this District.

FACTUAL ALLEGATIONS

Background

14. Accellion is a Palo Alto–based software company that makes, markets, and sells file transfer platforms and services. At the core of its business is providing institutional customers with a way to securely share sensitive and private data, including the PII of its customers' own clients.

15. Accellion touts its commitment to data privacy and security, claiming that "[d]ata privacy is a fundamental aspect of the business of Accellion."[4]

16. Not only is Accellion aware that its customers use its services to transfer the sensitive information and PII of third parties, it actively markets its products for such use: "Organizations in highly regulated industries like healthcare, government, law, and financial services began to view Accellion as critical to ensuring files are shared securely and in compliance with rigorous data privacy standards regulations."[5]

[4] *Privacy Policy*, ACCELLION, https://www.accellion.com/privacy-policy/.
[5] *Accellion Company Overview*, ACCELLION, https://www.accellion.com/sites/default/files/resources/accellion-company-overview.pdf

17. Accordingly, Accellion had a duty to adopt reasonable measures to protect the sensitive data and PII stored on or shared through its system.

18. Among Accellion's many different software solutions for securely transferring sensitive information is Accellion's File Transfer Appliance ("FTA") software, a "20 year old legacy product," with an "end of life" scheduled for April 30, 2021.[6]

19. Accellion FTA's operating system, CENTOS 6, had announced an end of life date of November 30, 2020, which Accellion knew limited its "ability to support the FTA software" after that date.[7]

20. Accellion FTA is regularly used by "worldwide enterprises," to "transfer large and sensitive files securely."[8]

21. Accellion was aware that its customers continued to use FTA in December 2020 and January 2021 and continued to offer FTA services to its customers during that time period.

22. Accellion FTA was used to transfer some of Plaintiff's and Class Members most sensitive and confidential information, including names, email addresses and other contact information, dates of birth, Social Security numbers and/or driver's license or state identification numbers, bank account numbers and bank routing numbers, medical records, academic records, places of employment and/or salary information. In the wrong hands, this sensitive and static information can be used to create myriad financial crimes and can put Plaintiff and Class Members at significant risk of identity theft, financial fraud, and other identity-related fraud into the indefinite future.

The Data Breach

23. On December 16, 2020, an exploit of Accellion FTA triggered FTA's anomaly detector on a customer's device ("December Exploit").[9]

---

[6] *Security Update, Accellion Announces End of Life (EOL) for Its Legacy FTA Product*, ACCELLION (Feb. 25, 2020), https://www.accellion.com/sites/default/files/resources/fta-eol.pdf.

[7] *Id.*

[8] *See Accellion FTA*, ACCELLION, https://www.accellion.com/products/fta/.

[9] Mandiant Report at 5–6.

24. From December 16-19 2020, Accellion investigated the exploit and identified two vulnerabilities affecting Accellion FTA: SQL Injection (CVE-2021-27101) and OS Command Execution (CVE-2021-27104).[10]

25. On December 20, 2020, Accellion released a patch to remediate these vulnerabilities, and on December 23, 2020 Accellion released a patch to increase the frequency of anomaly detector checks.[11]

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

27. Accellion failed to discover any additional vulnerabilities, and attacks on the FTA software continued into January 2021.

28. Accellion experienced a second exploit on January 20, 2021 ("January Exploit"). It became aware of this exploit on January 22, 2021 when multiple customers submitted service inquiries. That same day, Accellion issued a critical security alert advising FTA customers to shut down their FTA systems immediately.[13]

29. From January 22-25, 2021, Accellion investigated the January Exploit, and identified two additional vulnerabilities affecting Accellion FTA: Server-Side Request Forgery (CVE-2021-27103) and OS Command Execution (CVE-2021-27102).[14]

30. Accellion released patches to these address these additional vulnerabilities on January 25th and 28th.[15]

31. According to the Cybersecurity & Infrastructure Security Agency, "Worldwide, actors have exploited the vulnerabilities to attack multiple federal and state, local, tribal, and territorial

[10] *Id.*
[11] *Id.*
[12] Press Release, *Accellion Responds to Recent FTA Security Incident*, ACCELLION (Jan. 12, 2021), https://www.accellion.com/company/press-releases/accellion-responds-to-recent-fta-security-incident/.
[13] Mandiant Report at 4, 7.
[14] *Id.*
[15] *Id.*

(SLTT) government organizations as well as private industry organizations including those in the medical, legal, telecommunications, finance, and energy sectors. . . . In one incident, an attack on an [state, local, tribal, and territorial government] organization potentially included the breach of confidential organizational data. In some instances observed, the attacker has subsequently extorted money from victim organizations to prevent public release of information exfiltrated from the Accellion appliance."[16]

32. To date, the companies affected reportedly include:[17]

- The Reserve Bank of New Zealand
- Australian Securities and Investments Commission
- Bombardier
- Australia's Transport for New South Wales
- Jones Day
- Goodwin Proctor LLP
- Allens
- Washington State Auditor's Office
- Flagstar Bank
- Qualys
- Royal Dutch Shell

[16] Alert (AA21-055A), *Exploitation of Accellion File Transfer Appliance*, CISA (Feb. 25, 2021), https://us-cert.cisa.gov/ncas/alerts/aa21-055a.

[17] *See, e.g.*, Joe Panettieri, *Accellion Vulnerabilities, Cyberattacks and Victims: Customer List and Status Updates*, MSSP ALERT (Apr. 7, 2021), https://www.msspalert.com/cybersecurity-breaches-and-attacks/accellion-vulnerabilities-victim-list/; Ara Aslanian, *4 Areas Of Cyberattack Vulnerability For Law Firms*, LAW360 (Mar. 26, 2021), https://www.law360.com/articles/1368765/4-areas-of-cyberattack-vulnerability-for-law-firms; Arielle Waldman, *Accellion FTA attacks claim more victims*, SEARCHSECURITY (Mar. 3, 2021), https://searchsecurity.techtarget.com/news/252497232/Accellion-FTA-attacks-claim-more-victims; *Lower-profile Accellion hack hit dozens of high-profile targets, including Kroger, CSX, Harvard*, MARKETWATCH (Mar. 7, 2021), https://www.marketwatch.com/story/lower-profile-accellion-hack-hit-dozens-of-high-profile-targets-including-kroger-csx-harvard-01615154005; Lindsay McKenzie, *Secure File Sharing Compromises University Security*, INSIDE HIGHER ED (Apr. 7, 2020), https://www.insidehighered.com/news/2021/04/07/accellion-data-security-breach-latest-hit-universities.

- Singtel
- CSX
- Stanford University
- Trinity Health
- University of California
- University of Colorado
- University of Maryland, Baltimore
- Yeshiva University
- University of Miami
- Harvard Business School
- Kroger Family of Companies
- Kroger Pharmacy
- Health Net
- Trillium Health Plan
- Arizona Complete Health
- Stanford Medicine
- University of Miami Health
- Centene Corp

33. Sensitive information stolen through this Data Breach, including Social Security numbers, academic transcripts, medical records, passports, and federal tax documents have reportedly been made available to download via a website called Clop that is run by cybercriminals.[18] "The Clop website is known to publish samples of stolen data and then demand a ransom not to publish the rest of the information."[19]

[18] Lillian Reed, *University of Maryland, Baltimore says private data was published online following hack*, BALTIMORE SUN (Apr. 1, 2021), https://www.baltimoresun.com/education/bs-md-umb-data-breach-20210401-20210401-o6q24j3inzh7xioii7j7kn72em-story.html.

[19] Lindsay McKenzie, *Secure File Sharing Compromises University Security*, INSIDE HIGHER ED (Apr. 7, 2020), https://www.insidehighered.com/news/2021/04/07/accellion-data-security-breach-latest-hit-universities; Lillian Reed, *University of Maryland, Baltimore says private data was published online*

Effect of the Data Breach

34. Accellion's failure to keep Plaintiff's and Class Members' PII secure has severe ramifications. Given the sensitive nature of the PII stolen in the Data Breach, cyber criminals have the ability to commit identity theft and other identity-related fraud against Plaintiff and class members now and into the indefinite future.

35. The information stolen from Accellion included social security numbers, bank account numbers, and medical records—PII that is highly valued among cyber thieves and criminals on the Dark Web. For example, detailed student health records were stored on the compromised databases. Stolen medical records "can fetch up to $350 on the dark web."[20]

36. PII also has significant monetary value in part because criminals continue their efforts to obtain this data.[21] In other words, if any additional breach of sensitive data did not have incremental value to criminals, one would expect to see a reduction in criminal efforts to obtain such additional data over time. Instead, just the opposite has occurred. For example, the Identity Theft Resource Center reported 1,473 data breaches in 2019, which represents a 17 percent increase from the total number of breaches reported in 2018.[22]

37. The value of PII is key to unlocking many parts of the financial sector for consumers. Whether someone can obtain a mortgage, credit card, business loan, tax return, or even apply for a job depends on the integrity of their PII. Similarly, the businesses that request (or require) consumers to share their PII as part of a commercial transaction do so with the expectation that its integrity has not been compromised.

---

following hack, BALTIMORE SUN (Apr. 1, 2021), https://www.baltimoresun.com/education/bs-md-umb-data-breach-20210401-20210401-o6q24j3inzh7xioii7j7kn72em-story.html.

[20] *How Cybercriminals Make Money: How much is your information worth to a cybercriminal via the Dark Web?*, Keeper Security, https://www.keepersecurity.com/how-much-is-my-information-worth-to-hacker-dark-web.html (last visited May 26, 2020).

[21] *Data Breaches Rise as Cybercriminals Continue to Outwit IT*, CIO Magazine (Sept. 28, 2014), available at http://www.cio.com/article/2686167/data-breach/data-breaches-rise-as-cybercriminals-continue-to-outwit-it.html.

[22] *2019 End-of-Year Data Breach Report* (2019), Identity Theft Resource Center, *available at* https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf.

38. Annual monetary losses for victims of identity theft are in the billions of dollars. In 2017, fraudsters stole $16.8 billion from consumers in the United States, which includes $5.1 billion stolen through bank account take-overs.[23]

39. The annual cost of identity theft is even higher. McAfee and the Center for Strategic and International Studies estimates that the likely annual cost to the global economy from cybercrime is $445 billion a year.[24]

40. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, in addition to the irreparable damage that may result from the theft of PII, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, 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" and resolving the consequences of fraud in 2014.[25]

41. The impact of 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.[26] 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.

---

[23] Javelin, *2018 Identity fraud: Fraud Enters A New Era of Complexity*, available at https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity (last visited May 26, 2020).

[24] Insurance Information Institute, *Facts + Statistics: Identity theft and cybercrime*, available at https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (last visited May 26, 2020).

[25] U.S. Department of Justice, *Victims of Identity Theft, 2014* (Revised November 13, 2017), available at http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited May 26, 2020).

[26] Identity Theft Resource Center, *Identity Theft: The Aftermath 2017*, available at https://www.idtheftcenter.org/images/page-docs/Aftermath_2017.pdf (last visited May 26, 2020).

42. It is no wonder, then, that identity theft exacts a severe emotional toll on its victims. The 2017 Identity Theft Resource Center survey[27] evidences the emotional suffering experienced by victims of identity theft:

- 75% of respondents reported feeling severely distressed;
- 67% reported anxiety;
- 66% reported feelings of fear related to personal financial safety;
- 37% reported fearing for the financial safety of family members;
- 24% reported fear for their physical safety;
- 15.2% reported a relationship ended or was severely and negatively impacted by the identity theft; and
- 7% reported feeling suicidal.

43. Identity theft can also exact a physical toll on its victims. The same survey reported that respondents experienced physical symptoms stemming from their experience with identity theft:

- 48.3% of respondents reported sleep disturbances;
- 37.1% reported an inability to concentrate / lack of focus;
- 28.7% reported they were unable to go to work because of physical symptoms;
- 23.1% reported new physical illnesses (aches and pains, heart palpitations, sweating, stomach issues); and
- 12.6% reported a start or relapse into unhealthy or addictive behaviors.[28]

44. There may also be a significant time lag between when PII is stolen and when it is actually misused. According to the U.S. Government Accountability Office, 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

[27] *Id.*
[28] *Id.*

for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[29]

45. The risk of identity theft is particularly acute where detailed personal information is stolen, such as the PII that was compromised in the Data Breach.

46. As the result of the Data Breach, Plaintiff and Class Members have suffered or will suffer economic loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

a. identity theft and fraud resulting from theft of their PII;

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

c. losing the inherent value of their PII;

d. costs associated with purchasing credit monitoring and identity theft protection services;

e. unauthorized access to and misuse of their online accounts;

f. unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

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

h. costs associated with time spent and the loss of productivity or 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, addressing other varied instances of identity theft – such as credit cards, bank accounts, loans, government benefits, and other services procured using the stolen PII, purchasing credit monitoring and identity theft protection services, imposing

[29] U.S. Government Accountability Office, *Report to Congressional Requesters* (June 2007), http://www.gao.gov/new.items/d07737.pdf.

withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance of dealing with the repercussions of the Data Breach;

i. the continued imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being in the possession of one or more unauthorized third parties; and

47. Additionally, Plaintiffs and class members place significant value in data security. According to a recent survey conducted by cyber-security company FireEye, approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more in order to work with a provider that has better data security. Likewise, 70% of consumers would provide less personal information to organizations that suffered a data breach.[30]

48. The Data Breach occurred as a result of Accellion's failure to ensure that its FTA product was protected and secured, despite knowing that Accellion FTA was used by many organizations to transfer and store the PII of third parties. As a result of the Data Breach, Plaintiff's and Class members' privacy has been invaded, their personal information is now in the hands of criminals, and they face a substantially increased risk of fraud, criminal misuse of their PII, and identity theft for years to come.

Plaintiff Amiresse DesJardins's Experience

49. Ms. DesJardins is a former employee of Kroger, having worked there as an Overnight Cashier from April 2017 to February 2018.

50. Prior to the Data Breach, Ms. DesJardins took steps to protect her personal information. She always kept her Social Security card and birth certificate in a secure location in her home, refrained from sending sensitive information over email, and shredded mailings containing sensitive personal information.

[30] FireEye, *Beyond the Bottom Line: The Real Cost of Data Breaches* (May 11, 2016), https://www.fireeye.com/blog/executive-perspective/2016/05/beyond_the_bottomli.html.

51. Upon information and belief, Kroger used Accellion's FTA software to transfer the PII of its current and former employees, including Plaintiff.

52. Kroger Family of Companies was notified of the Data Breach on January 23, 2021, and subsequently discontinued the use of Accellion's services.[31]

53. On or around February 19, 2021, Ms. DesJardins received notice of the Data Breach from Kroger.

54. The notice provided:

> I am writing to let you know about a data security incident affecting Accellion, which was used by the Kroger Family of Companies and many other companies for secure file transfers. This incident involved your personal information. . . .
>
> **What Happened?**
>
> We were recently made aware of a data security incident affecting Accellion, which was used by the Kroger Family of Companies, as well as many other companies, for secure file transfers. Accellion has confirmed that an unauthorized person gained access to certain Kroger Family of Companies files by exploiting a vulnerability in Accellion's file transfer service. We learned that the Accellion incident impacted Kroger's files on January 23, 2021, took immediate action, and we discontinued use of Accellion's services and investigated the scope and impact of the incident The incident was isolated to Accellion's services, and our own IT systems have not been affected by this incident. No grocery store data was impacted. However, the Accellion software was used for secure file transfers of certain Human Resources information of some associates and former associates.
>
> **What Information Was Involved?**
>
> Our investigation into the scope of the incident is ongoing. However, we believe impacted information may include names, email address and other contact information, date of birth, Social Security number, and for some associates or former associates, may have also included certain salary information such as net and gross pay and withholdings. While grocery store systems or data were not impacted, customers of the Pharmacy or Little Clinic may receive a separate notice related to this incident if your pharmacy or clinic information was impacted. . . .

55. In response to Kroger's notice, Plaintiff has already spent over an hour investigating the Data Breach, including conducting independent online research regarding the scope of the breach

[31] *Accelion Incident*, KROGER, https://www.kroger.com/i/accellion-incident.

and communicating with Kroger regarding the breach. She will continue to expend time monitoring her credit and other identity-related information and is exploring options for identity theft protection services.

56. As a result of the Data Breach, Plaintiff has also experienced anxiety, emotional distress, and loss of privacy, and is at an increased risk of future harm.

CLASS ACTION ALLEGATIONS

57. Pursuant to Federal Rule of Civil Procedure 23(b)(1), (b)(2) and (b)(3), Plaintiff seeks certification of the following Nationwide Class:

58. **Nationwide Class:** All residents of the United States whose PII was exposed to unauthorized third parties as a result of the Accellion Data Breach in December 2020 and January 2021.

59. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their judicial staff and immediate family members.

60. **Numerosity. Fed. R. Civ. P. 23(a)(1).** While the exact number of class members is unknown to Plaintiffs at this time, given the number of organizations affected by the Data Breaches, Plaintiff anticipates that the total number of victims is in the hundreds of thousands, if not millions, meaning the members of the Class are so numerous and geographically dispersed that the joinder of all members is impractical.

61. **Commonality and Predominance. Fed. R. Civ. P. 23(a)(2) and (b)(3).** This action involves common questions of law and fact that predominate over any questions affecting individual class members. The common questions include, but are not limited to:

a. Whether Accellion knew or should have known that its FTA service was vulnerable to attack;

b. Whether Accellion failed to take adequate and reasonable measures to ensure such computer and data systems were protected;

c. Whether Accellion failed to take available steps to prevent and stop the Data Breach from happening;

d. Whether Accellion owed duties to Plaintiff and Class Members to protect their PII;

e. Whether Accellion breached its duties to protect the PII of Plaintiff and Class Members by failing to provide adequate data security;

f. Whether Accellion's failure to secure Plaintiff's and class members' PII in the manner alleged violated federal, state and local laws, or industry standards;

g. Whether the Plaintiff's and Class Members' PII was compromised and exposed as a result of the Data Breach and the extent of that compromise and exposure;

h. Whether Plaintiff and Class Members were the intended third-party beneficiaries of any contractual obligations owed by Accellion;

i. Whether, as a result of Accellion's conduct, Plaintiff and Class Members face a significant threat of harm and/or have already suffered harm, and, if so, the appropriate measure of damages to which they are entitled;

j. Whether Plaintiff and Class Members are entitled to compensatory damages;

62. **Typicality. Fed. R. Civ. P. 23(a)(3).** Plaintiffs' claims are typical of other class members' claims because Plaintiffs and class members were subjected to the same allegedly unlawful conduct and damaged in the same way.

63. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiff is an adequate representative of the Class. Plaintiff is a member of the Nationwide Class. Plaintiff has no conflicts of interest with the Class. Plaintiff's counsel is competent and experienced in litigating class actions, including extensive experience in data breach and privacy litigation and consumer protection

claims. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the interests of the Class.

64. **Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs and class members may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiff and the Class Members are relatively small compared to the burden and expense required to individually litigate their claims against Accellion, and thus, individual litigation to redress Accellion's wrongful conduct would be impracticable. Individual litigation by each class member would also strain the court system. Moreover, individual litigation creates the potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

* * *

CLAIMS

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

65. Plaintiff re-alleges and incorporates by reference the allegations in paragraphs 1–64 in this Complaint, as if fully alleged herein.

66. Accellion knew, or should have known, that its customers used Accellion FTA to share certain PII of their own clients, customers, patients, and employees, including names, email addresses and other contact information, dates of birth, Social Security numbers and/or driver's license or state identification numbers, bank account numbers and bank routing numbers, medical records, academic records, places of employment and/or salary information.

67. Accellion knew the importance of securing the data its customers shared through Accellion FTA. In fact, providing a secure method of transferring and sharing sensitive information is the central selling point of Accellion's services.

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

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

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

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

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

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

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

75. Accellion had common law duties to prevent foreseeable harm to Plaintiff and Class Members. These duties existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices. Accellion's duty also arose because it engaged in affirmative conduct—the design, development, and maintenance of the FTA system—and Plaintiff and Class Members were the foreseeable victims of any harm that might arise from Accellion's negligence in engaging in such affirmative conduct.

76. In fact, not only was it foreseeable that Plaintiff and Class Members would be harmed by the failure to protect their PII (including through the failure to adequately design, develop, and maintain the systems on which their PII was stored or processed) because hackers routinely attempt to steal such information and use it for nefarious purposes, Accellion knew that it was more likely than not Plaintiffs and other class members would be harmed by such theft.

77. Accellion knew or should have known that its computer systems and data storage architecture were vulnerable to unauthorized access and targeting by hackers for the purpose of stealing and misusing confidential PII.

78. Accellion knew or should have known that a breach of its systems and data storage architecture would inflict millions of dollars of damages upon Plaintiffs and the Class, and Accellion was therefore charged with a duty to adequately protect this critically sensitive information.

79. Accellion breached the duties it owed to Plaintiff and Class Members described above, and thus was negligent. Accellion breached these duties by, among other things, failing to exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the PII of Plaintiff and Class Members, and failing to adequately design, develop, and maintain security systems consistent with industry standards.

80. But for Accellion's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their PII would not have been compromised.

81. As a direct and proximate result of Accellion's negligence, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following economic and non-economic injuries: ongoing,

imminent, certainly impending threat of identity theft crimes, fraud, and other misuse; actual identity theft crimes, fraud, and other misuse; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes, reviewing bank statements, payment card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

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

82. Plaintiff re-alleges and incorporates by reference the allegations in paragraphs 1–81 in this Complaint, as if fully alleged herein.

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

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

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

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

87. Accellion knew or should have known that its Accellion FTA customers could and would use Accellion FTA to transfer PII of their clients, customers, patients, and employees, such as Plaintiff.

88. Accellion breached the contracts with its Accellion FTA customers by failing to keep secure and confidential the PII of Plaintiff and Class Members.

89. As a direct and proximate result of Accellion's above-described breach of contract, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes, reviewing bank statements, payment card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

COUNT IV
Invasion of Privacy (Intrusion Upon Seclusion)
(On Behalf of Plaintiff and the Nationwide Class)

90. Plaintiff re-alleges and incorporates by reference the allegations in paragraphs 1–89 in this Complaint, as if fully alleged herein.

91. Plaintiff and Class Members had a reasonable expectation of privacy in the PII that Accellion mishandled.

92. Accellion owed a duty to Plaintiff and Class Members to keep their PII contained as a part thereof, confidential.

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

94. By failing to keep Plaintiff's and Class Members' private information safe, and by misusing and/or disclosing said private information to unauthorized parties for unauthorized use, Accellion invaded Plaintiff's and Class Members' privacy by:

a. Intruding into Plaintiff's and Class Members' private affairs in a manner that would be highly offensive to a reasonable person; and

b. Publicizing private facts about Plaintiff and Class Members, which is highly offensive to a reasonable person.

95. Accellion knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiff's position would consider Accellion's actions highly offensive.

96. Accellion invaded Plaintiff's and Class Members' right to privacy and intruded into Plaintiff's and Class Member's private affairs by misusing and/or disclosing their private information without their informed, voluntary, affirmative, and clear consent.

97. As a proximate result of such misuse and disclosures, Plaintiff's and Class Members' reasonable expectation of privacy in their private information was unduly frustrated and thwarted. Accellion's conduct amounted to a serious invasion of Plaintiff's and Class Members' protected privacy interests.

98. In failing to protect Plaintiffs' private information, and in misusing and/or disclosing their private information, Accellion has acted with malice and oppression and in conscious disregard of Plaintiff's and Class Members' rights to have such information kept confidential and private.

99. Plaintiff seeks injunctive relief on behalf of the Class, restitution, and all other damages available under this Count.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all class members proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against Accellion as follows:

1) For an Order certifying the Nationwide Class, the Nationwide Minor Subclass, the California Subclass, and the California Minor Subclass, as defined herein, and appointing Plaintiffs and Plaintiffs' counsel to represent the Class as alleged herein;

2) For an award of compensatory, consequential, and general damages, including nominal damages, as allowed by law in an amount to be determined;

3) For an award of statutory damages and punitive damages, as allowed by law in an amount to be determined;

4) For an award of restitution or disgorgement, in an amount to be determined;

5) Declaratory and injunctive relief as described herein;

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

7) For prejudgment interest on all amounts awarded; and

8) Such other and further relief as the Court may deem just and proper.

JURY DEMAND

Plaintiffs, on behalf of themselves and the Class of all others similarly situated, hereby demand a trial by jury on all issues so triable pursuant to Rule 38 of the Federal Rules of Civil Procedure.

Dated: June 22, 2021

Respectfully submitted,

/s/ Hassan A. Zavareei

Hassan A. Zavareei (CA Bar No. 181547)
Mark A. Clifford*
TYCKO & ZAVAREEI LLP
1828 L Street NW, Suite 1000
Washington, D.C. 20036
Telephone: (202) 973-0900
Facsimile: (202) 973-0950
Email: hzavareei@tzlegal.com
mclifford@tzlegal.com

Sabita Soneji (CA Bar No. 224262)
TYCKO & ZAVAREEI LLP
1970 Broadway Suite 1070
Oakland, CA 94612
Telephone: (510) 254-6808
Facsimile: (202) 973-0950
Email: ssoneji@tzlegal.com

Counsel for Plaintiffs and the Proposed Class

**pro hac vice application forthcoming*