Todd D. Carpenter (234464)
CARLSON LYNCH, LLP
1350 Columbia Street, Suite 603
San Diego, CA 92101
Tel: 619-762-1910
Fax: 619-756-6991
tcarpenter@carlsonlynch.com

Karen Hanson Riebel (*pro hac vice* forthcoming)
Kate M. Baxter-Kauf (*pro hac vice* forthcoming)
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Avenue South, Suite 2200
Minneapolis, MN 55401
khriebel@locklaw.com
kmbaxter-kauf@locklaw.com

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

AARON SHARP, on behalf of himself and all others similarly situated,

Plaintiff,

v.

ACCELLION, INC.,

Defendant.

Case No.:

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Aaron Sharp ("Plaintiff") brings this Class Action Complaint on behalf of himself and all others similarly situated, against Defendant**,** Accellion, Inc. ("Accellion" or "Defendant"), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to him, which are based on personal knowledge:

NATURE OF THE CASE

1. Businesses that handle sensitive, personally identifying information ("PII") or personal medical information ("PMI") owe a duty of reasonable care to the individuals to whom that data relates. This duty arises because it is foreseeable that the exposure of PII or PMI to unauthorized persons—and especially hackers with nefarious intentions—will result in harm to the affected individuals.

2. This harm manifests in a number of ways, including identity theft and financial fraud, and the exposure of a person's PII or PMI through a data breach, which ensures that that person will be at a

substantially increased and certainly impending risk of these crimes compared to the rest of the population, potentially for the rest of their lives. Mitigating that risk, to the extent it is even possible to do so, requires individuals to devote significant time and money to closely monitor their credit, financial accounts, health records, and email accounts, and take a number of additional prophylactic measures.

3. Accellion advertises its safety as a major selling point. "When employees click the Accellion button, they know it's the safe, secure way to share sensitive information with the outside world."[1] Accellion provides cloud-based file transferring solutions to a variety of different industries including governmental agencies, healthcare, financial services, legal, and higher education.

4. After choosing Accellion as a cloud solution provider, its clients provide Accellion access to data that includes highly sensitive PII and PMI, which Accellion then transfers and stores on its own systems. Through these connections, Accellion knowingly obtains consumer PII and PMI, and has a resulting duty to securely maintain such information in confidence.

5. Plaintiff brings this class action on behalf of individual consumers whose PII and/or PMI was accessed and exposed to unauthorized third parties during a data breach of Accellion's systems, which occurred in December 2020 and lasted until at least January 2021 (the "Data Breach").

6. Plaintiff, on behalf of himself and the Classes as defined herein, brings claims for actual damages, statutory damages, and punitive damages, with attorneys' fees, costs, and expenses under the California Confidentiality of Medical Information Act ("CMIA"), Cal. Civ. Code § 56, *et seq.*, and further sues Defendant for negligence, negligence *per se*, unjust enrichment, and declaratory judgment.

7. The information accessed and exposed during the Data Breach was derived from hundreds of Accellion's institutional clients, involving the PII and PMI of millions of individual consumers.

8. Based on the public statements of Accellion and certain of its institutional clients to date, a wide variety of PII and PMI was implicated in the breach, including, but not limited to: names, drivers license information, dates of birth, phone numbers, email addressed, bank account information, social security numbers, medical information, and insurance information.

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

9. One of Accellion's customers, The Kroger Company ("Kroger"), recently confirmed that they used Accellion as a third-party vendor, and that some of their clinic and pharmacy customers' information was accessed and exposed during the Data Breach.

10. Since the Data Breach, more Accellion institutional clients have announced—either in public statements, notice letters, or both—that their consumers' PII and PMI was also compromised in the Data Breach.

11. As a direct and proximate result of Accellion's inadequate data security, and its breach of its duty to handle PII and PMI with reasonable care, Plaintiff and Class Members' PII and/or PMI has been accessed by hackers and exposed to an untold number of unauthorized individuals.

12. Plaintiff and Class Members are now at a significantly increased risk of fraud, identity theft, and similar forms of criminal mischief, which risk may last for the rest of their lives. Consequently, Plaintiff and Class Members must devote substantially more time, money, and energy protecting themselves, to the extent possible, from these crimes.

13. To recover from Accellion for these harms, Plaintiff and the Classes seek damages in an amount to be determined at trial, declaratory judgment, and injunctive relief requiring Accellion to: 1) disclose, expeditiously, the full nature of the Data Breach, the institutional clients affected, and the types of PII and PMI accessed, obtained, or exposed by the hackers; 2) implement improved data security practices to reasonably guard against future breaches of PII and PMI possessed by Accellion; and 3) provide, at its own expense, all impacted victims with lifetime identity theft protection services.

PARTIES

14. Plaintiff Aaron Sharp is an adult individual who at all relevant times has been a citizen and resident of the State of Kentucky. Plaintiff has used Kroger's pharmacy on a continuous basis since at least 2000 through the present.

15. In March 2020, Plaintiff learned of the Data Breach, that Kroger used Accellion as a third-party vendor, and that as a result of that relationship, Plaintiff's PII and PMI may have been accessed or exposed to unknown, unauthorized third parties during the Data Breach.

16. Defendant, Accellion, Inc., is a Delaware corporation in the business of cloud-based file transfer solutions with its principal place of business in Palo Alto, California.

JURISDICTION AND VENUE

17. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, because Plaintiff and at least one member of each of the Classes, as defined below, is a citizen of a different state than Defendant, there are more than 100 members of each of the Classes, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interests and costs.

18. This Court has personal jurisdiction over Defendant because it is headquartered in and is a citizen of the State of California.

19. Venue is proper in this District, pursuant to 28 U.S.C. § 1391(b)(1), because a substantial part of the acts, omissions, and events giving rise to Plaintiff's claims occurred in this District. Further, Defendant resides in this District and is a resident of California.

FACTUAL BACKGROUND

A. Background of Accellion's Business Model

20. Accellion advertises itself as a defense to data breaches, stating: "[t]he Accellion enterprise content firewall prevents data breaches and compliance violations from third party cyber risk."[2] "With on-premise, private cloud, hybrid and FedRAMP deployment options, the Accellion content firewall provides the security and governance CISOs need to protect their organizations, mitigate risk, and adhere to rigorous compliance regulations."[3]

21. Accellion claims to have "protected more than 25 million end users at more than 3,000 global corporations and government agencies . . . ."[4]

22. Accellion recognizes that "[q]uality patient care requires accurate diagnosis, effective treatment, and bullet-proof data security."[5] Accellion markets its secure solutions to its healthcare clients, stating "[t]he Accellion enterprise content firewall allows hospitals and clinics, payers, and government

[2] https://www.accellion.com/company/
[3] *Id.*
[4] *Id.*
[5] https://www.accellion.com/solutions/healthcare/

health agencies to share X-rays, diagnoses, insurance information and other PHI securely and in compliance with patient privacy regulations like HIPAA, HITECH and GDPR."[6]

23. Accellion offers many different software solutions to its customers, including secure email, secure file sharing, secure mobile sharing, secure web forms, and secure managed file transfer.[7]

24. These programs perform a variety of functions, the most crucial being to share sensitive content with third parties in an easy and safe manner.

25. In short, the very nature of Accellion's core business involves providing its clients with a way to securely share sensitive and private data, including the PII and PMI of the institutional clients' own clients, patients, and consumers.

26. As a result, Accellion knows that its customers, and the individuals whose PII and PMI is shared with Accellion, must rely on Accellion to safeguard confidential data entrusted to it.

27. Due to the very nature of its business, then, Accellion knew that its data center hosting facilities contained sensitive PII and PMI and as a result, posed an attractive target for cybercriminals.

B. The Data Breach and Public Disclosure

28. On December 16, 2020, Accellion FTA (File Transfer Application), an older product offered by Defendant, triggered a built-in anomaly detector on one of Accellion's client's devices.[8]

29. From December 16th through the 19th, Defendant investigated the anomaly and detected the vulnerabilities affecting Accellion FTA - 9.12.370 – SQL Injection (CVE-2021-27101) and OS Command Execution (CVE-2021-27104).[9]

30. On December 20th and 23rd, Defendant released two patches: FTA 9.12.380 and FTA 9.12.411, respectively, to remedy the vulnerabilities.[10]

31. Despite this timeline, Accellion claims to have "released a fix within 72 hours."[11]

---

[6] *Id.*
[7] https://www.accellion.com/platform/enterprise-content-firewall/
[8] accellion-fta-attack-mandiant-report-full.pdf
[9] *Id.*
[10] *Id.*
[11] https://gizmodo.com/the-accellion-data-breach-seems-to-be-getting-bigger-1846250357

32. Accellion claims that it notified all Accellion FTA customers of the Data Breach on December 23, 2020.[12]

33. In announcing that the fix did not completely contain the Data Breach within that 72 hour period, Accellion stated: "This initial incident was the beginning of a concerted cyberattack on the Accellion FTA product that continued into January 2021. Accellion identified additional exploits in the ensuing weeks and developed and released patches to close each vulnerability."[13]

34. In Accellion's initial statement, it indicated that less than 50 clients were affected.[14]

35. Accellion experienced a second exploit on January 20, 2021, and became aware of it on January 22, 2021, through multiple customer service inquiries.[15] In response, Accellion issued a critical security alert advising its FTA customers to shut down their FTA system immediately.[16]

36. Kroger was notified of the Data Breach on January 23, 2021, at which point Kroger discontinued the use of Accellion's services.[17]

37. From January 22nd to the 25th, Defendant investigated the exploit and identified two more vulnerabilities - Server-Side Request Forgery (CVE-2021-27103) and OS Command Execution (CVE-2021-27102).[18]

38. On January 25th and 28th, Defendant released patches FTA 9.12.416 and FTA_9.12.432, respectively, to remediate the vulnerabilities.[19]

39. The University of Colorado, one of Accellion's higher education clients affected by the Data Breach, puts the number of clients affected by the Data Breach at approximately 300.[20]

---

[12] *Id.*
[13] *Id.*
[14] *Id.*
[15] accellion-fta-attack-mandiant-report-full.pdf
[16] *Id.*
[17] https://www.kroger.com/i/accellion-incident
[18] accellion-fta-attack-mandiant-report-full.pdf
[19] *Id.*
[20] https://gizmodo.com/the-accellion-data-breach-seems-to-be-getting-bigger-1846250357

40. One governmental agency client of Accellion affected by the Data Breach, the Washington State Auditor's Office, has indicated that approximately 1.4 million individuals who filed unemployment insurance claims in 2020 were at risk of having their PII exposed in this Data Breach.[21]

41. News reports indicate that other major Accellion clients have also confirmed that they have been affected by Data Breach. These clients include the law firm Jones Day[22], Singapore telephone company Singtel[23], the Reserve Bank of New Zealand[24], and the Australian Securities and Investments Commission[25].

42. Kroger believes the following information, which includes Plaintiff's information, has been involved in the Data Breach[26]:

> **What information may have been involved?** ^
>
> At this time, based on the information provided by Accellion and our own investigation, Kroger believes the categories of affected data may include certain associates' HR data, certain pharmacy records, and certain money services records. Importantly, there was no impact to grocery store data or systems; credit or debit card information; or customer account passwords.

43. The total number of institutional clients and individual clients affected by the Data Breach is unknown.

C. Accellion Knew the Risks of Storing PII and PMI and the Foreseeable Harm to Victims

44. At all relevant times, Accellion knew it was storing valuable, sensitive PII and PMI and that as a result, Accellion's systems would be attractive targets for cybercriminals.

---

[21] https://www.databreachtoday.com/washington-state-breach-tied-to-accellion-vulnerability-a-15909

[22] https://news.bloomberglaw.com/business-and-practice/jones-day-hit-by-data-breach-as-vendor-accellion-hacks-widen

[23] https://www.singtel.com/personal/support/about-accellion-security-incident

[24] https://www.bankinfosecurity.com/nz-reserve-bank-issues-update-on-accellion-breach-a-16008

[25] https://www.securityweek.com/australian-corporate-regulator-discloses-breach-involving-accellion-software

[26] *Id.*

45. Accellion also knew that any breach of its systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII and PMI was compromised.

46. These risks are not merely theoretical; in recent years, numerous high-profile breaches have occurred at businesses such as Equifax, Yahoo, Marriott, Anthem, and many others.

47. PII has considerable value and constitutes an enticing and well-known target to hackers. Hackers easily can sell stolen data as a result of the "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[27] PMI can be used for medical fraud and to submit false medical claims for reimbursement.

48. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. According to the IRTC, in 2019, there were 1,473 reported data breaches in the United States, exposing 164 million sensitive records and 705 million "non-sensitive" records.[28]

49. In tandem with the increase in data breaches, the rate of identity theft and the resulting losses has also increased over the past few years. For instance, in 2018, 14.4 million people were victims of some form of identity fraud, and 3.3 million people suffered unrecouped losses from identity theft, nearly three times as many as in 2016. And these out-of-pocket losses more than doubled from 2016 to $1.7 billion in 2018.[29]

50. Even if stolen PII or PMI does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and

[27] Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/.

[28] *Data Breach Reports: 2019 End of Year Report*, IDENTITY THEFT RESOURCE CENTER, at 2, *available at* https://notified.idtheftcenter.org/s/resource#annualReportSection.

[29] Insurance Information Institute, *Facts + Statistics: Identity theft and cybercrime*, available at https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20(1) (last accessed March 1, 2021).

affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

51. Stolen names and email addresses can also facilitate attacks known as "credential stuffing," where the attacker, armed with a known valid email address, can attempt to log-in to online accounts using the common formulas for usernames (email address, first initial and last name, or full name) and common passwords, or use software to mount a brute-force attack (guessing many passwords in rapid succession) against weak login portals.

D. Plaintiff and Class Members Suffered Damages

52. For the reasons mentioned above, Accellion's negligence, which allowed the Data Breach to occur, caused Plaintiff and members of the Classes significant injuries and harm in several ways. Plaintiff and members of the Classes must immediately devote time, energy, and money to: 1) closely monitor their credit, financial accounts, email and other accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

53. Once PII or PMI is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff and Class members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of Accellion's negligence.

54. Plaintiff and Class members are also at a continued risk because their information remains in Accellion's systems, which have already been shown to be susceptible to compromise and attack.

CLASS ALLEGATIONS

55. Plaintiff brings this case individually and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the following classes (collectively, the "Classes"):

The FI Class

> All individuals in the United States whose PII was compromised in the Accellion data breach which occurred starting in December 2020 (the "FI Class").

The PMI Class

All individuals in the United States whose PMI, as defined in CMIA, Cal. Civ. Code § 56.05(j), was compromised in the Accellion data breach which occurred starting in December 2020 (the "PMI Class").

56. Excluded from the Classes is Defendant, its subsidiaries and affiliates, its officers, directors and members of their immediate families and any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

57. Plaintiff reserves the right to modify or amend the definition of the proposed Classes prior to moving for class certification.

58. The requirements of Rule 23(a)(1) are satisfied. The classes described above are so numerous that joinder of all individual members in one action would be impracticable. The disposition of the individual claims of the respective class members through this class action will benefit both the parties and this Court. The exact size of the classes and the identities of the individual members thereof are ascertainable through Defendant's records, including but not limited to, the files implicated in the Data Breach, but based on public information, the Classes include millions of individuals.

59. The requirements of Rule 23(a)(2) are satisfied. There is a well-defined community of interest and there are common questions of fact and law affecting members of the Classes. The questions of fact and law common to the Classes predominate over questions which may affect individual members and include the following:

a. Whether Defendant had a duty to protect the PII and PMI of Plaintiff and Class Members;

b. Whether Defendant's computer systems and data security practices used to protect Plaintiff's and the Classes' PII and PMI violated CMIA;

c. Whether Defendant was negligent in collecting and storing Plaintiff's and Class Members' PI and PMI I, and breached it duties thereby;

d. Whether Plaintiff and Class Members are entitled to damages as a result of Defendant's wrongful conduct;

e. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

f. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

60. The requirements of Rule 23(a)(3) are satisfied. Plaintiff's claims are typical of the claims of the members of the Classes. The claims of the Plaintiff and members of the Classes are based on the same legal theories and arise from the same failure by Defendant to safeguard PII and PMI.

61. Plaintiff and members of the Classes were each consumers who had relationships with organizations that were clients of Accellion, each having their PII and PMI obtained by an unauthorized third party.

62. The requirements of Rule 23(a)(4) are satisfied. Plaintiff is an adequate representative of the Classes because his interests do not conflict with the interests of the members of the Classes. Plaintiff will fairly, adequately, and vigorously represent and protect the interests of the members of the Classes and has no interests antagonistic to the members of the Classes. In addition, Plaintiff has retained counsel who are competent and experienced in the prosecution of class action litigation. The claims of Plaintiff and the Class members are substantially identical as explained above.

63. The requirements of Rule 23(b)(3) are satisfied here because a class action is the superior method of litigation these issues, and common issues will predominate. While the aggregate damages that may be awarded to the members of the Classes are likely to be substantial, the damages suffered by the individual members of the Classes are relatively small. As a result, the expense and burden of individual litigation make it economically infeasible and procedurally impracticable for each member of the Classes to individually seek redress for the wrongs done to them. Certifying the case as a Class will centralize these substantially identical claims in a single proceeding, which is the most manageable litigation method available to Plaintiff and the Classes and will conserve the resources of the parties and the court system, while protecting the rights of each member of the Classes. Defendant's uniform conduct is generally applicable to the Classes as a whole, making relief appropriate with respect to each Class member.

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiff and the Classes)

64. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

65. Accellion owed a duty under common law to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting their PII and PMI in its possession from being compromised, lost, stolen, accessed and misused by unauthorized persons.

66. Accellion's duty to use reasonable care arose from several sources, including but not limited to those described below.

67. Accellion had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Defendant. By collecting and storing valuable PII and PMI that is routinely targeted by criminals for unauthorized access, Accellion was obligated to act with reasonable care to protect against these foreseeable threats.

68. Accellion's duty also arose from Accellion's position as a vendor to healthcare, educational, and other organizations. Accellion undertakes its collection of highly sensitive information generally without the knowledge or consent of consumers and consumers cannot "opt out" of Accellion's data collection activities. Accellion holds itself out as a trusted steward of consumer data, and thereby assumes a duty to reasonably protect that data. Because of its role as a cloud computing and file transfer vendor to a large number of organizations, Accellion was in a unique and superior position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

69. Accellion breached the duties owed to Plaintiff and Class Members and thus was negligent. Accellion breached these duties by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII and PMI; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate

and adjust its information security program in light of the circumstances alleged herein; and (f) failing to detect the breach at the time it began or within a reasonable time thereafter.

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

71. As a direct and proximate result of Accellion's negligence, Plaintiff and Class Members have suffered injuries, including:

a. Theft of their PII and/or PMI;

b. Costs associated with requested credit freezes;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

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

e. 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 of their credit;

f. Lowered credit scores resulting from credit inquiries following fraudulent activities;

g. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Accellion Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

h. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PMI being placed in the hands of criminals;

i. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Accellion with the mutual understanding that Accellion would safeguard Plaintiff's and Class Members data against theft and not allow access and misuse of their data by others; and

j. Continued risk of exposure to hackers and thieves of their PII and/or PMI, which remains in Accellion's possession and is subject to further breaches so long as Accellion fails to undertake appropriate and adequate measures to protected Plaintiff.

72. As a direct and proximate result of Accellion's negligence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION
NEGLIGENCE PER SE
(On Behalf of Plaintiff and the Classes)

73. Plaintiff restates and realleges all proceeding factual allegations above as if fully set forth herein.

74. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as Accellion or failing to use reasonable measures to protect PII and PMI. Various FTC publications and orders also form the basis of Accellion's duty.

75. Pursuant to the CMIA, Defendant had a duty to implement safeguards to protect Plaintiff's and the PMI Class members' PII and PMI.

76. Accellion violated Section 5 of the FTC Act (and similar state statutes) and the CMIA by failing to use reasonable measures to protect PII and PMI and not complying with the industry standards. Accellion's conduct was particularly unreasonable given the nature and amount of PII and PMI it obtained and stored and the foreseeable consequences of a data breach involving PII and PMI of organizations' patients, clients, and consumers.

77. Accellion's violation of Section 5 of the FTC Act (and similar state statutes) and the CMIA constitutes negligence *per se*.

78. Plaintiff and members of the Class are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) was intended to protect.

79. Plaintiff and members of the PMI Class are patients within the class of persons CMIA was intended to protect..

80. Moreover, the harm that has occurred is the type of harm that the FTC Act (and similar state statutes) and CMIA was intended to guard against. Indeed, the FTC has brought dozens of enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members.

81. As a direct and proximate result of Accellion's negligence, Plaintiff and Class Members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Classes)

82. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

83. Plaintiff and Class Members have an interest, both equitable and legal, in the PII and PMI about them that was conveyed to, collected by, and maintained by Accellion and that was ultimately accessed or compromised in the Data Breach.

84. Accellion benefitted by the conferral upon it of the PII and PMI pertaining to Plaintiff and Class Members and by its ability to retain and use that information. Accellion understood that it was in fact so benefitted.

85. Accellion also understood and appreciated that the PII and PMI pertaining to Plaintiff and Class Members was private and confidential and its value depended upon Accellion maintaining the privacy and confidentiality of that PII and PMI.

86. Plaintiff and the Class Members' PII and PMI would not have been transferred to and entrusted with Accellion but for its express and implied commitments to its clients that the PII and PMI would be maintained safely and securely.

87. As a result of Accellion's wrongful conduct as alleged in this Complaint (including among other things its utter failure to employ adequate data security measures, its continued maintenance and use of the PII and PMI belonging to Plaintiff and Class Members without having adequate data security

measures, and its other conduct facilitating the theft of that PII and PMI), Accellion has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and Class Members.

88. Accellion's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiff's and Class Members' sensitive PII and PMI, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identify thieves.

89. Under the common law doctrine of unjust enrichment, it is inequitable for Accellion to be permitted to retain the benefits it received, and is still receiving, without justification, from the use of Plaintiff and Class Members' PII and PMI in an unfair and unconscionable manner. Accellion's retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

90. The benefit conferred upon, received, and enjoyed by Accellion was not conferred officiously or gratuitously, and it would be inequitable and unjust for Accellion to retain the benefit.

91. Accellion is therefore liable to Plaintiff and Class Members for restitution in the amount of the benefit conferred on Accellion as a result of its wrongful conduct, including specifically the value to Accellion of the PII and PMI that was stolen in the Data Breach and the profits Accellion received from the use of that information.

FOURTH CAUSE OF ACTION
CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT, Cal. Civ. Code § 6, *et seq.*
(On Behalf of Plaintiff and the PMI Class)

92. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

93. Defendant is a "provider of health care" as defined in Cal. Civ. Code § 56.06, and is therefore subject to the requirements of the CMIA, Cal. Civ. Code §§ 56.10(a) and (d), 56.35, 56.36(b), 56.101(a) and (b).

94. Defendant is organized in part for the purpose of maintaining medical information in order to make that information available to an individual or provider of health care, for purposes of information management, diagnosis, or treatment, and is therefore a "provider of heath care" under the CMIA.

95. Plaintiff and the PMI Class members are "patients," as defined in CMIA, Cal. Civ. Code § 56.06(k), as they are "natural person[s], whether or not still living, who received health care services from a provider of health care and to whom medical information pertains."

96. Defendant disclosed "medical information," as defined in CMIA, Cal. Civ. Code § 56.05(j), to unauthorized persons without first obtaining consent, in violation of Cal. Civ. Code § 56.10(a). References to that "medical information" have been discussed as "PMI" in the instant complaint.

97. Defendant's negligence resulted in the release of individually identifiable medical information, PMI, pertaining to Plaintiff and the PMI Class to unauthorized persons and the breach of the confidentiality of that information. Defendant's negligent failure to maintain, preserve, store, abandon, destroy, and/or dispose of Plaintiff's and PMI Class members' medical information in a manner that preserved the confidentiality of the information contained therein, in violation of the CMIA.

98. Defendant's computer systems did not protect and preserve the integrity of electronic medical information in violation of Cal. Civ. Code § 56.101(b)(1)(A).

99. Plaintiff and the PMI Class were injured and have suffered damages, as described above, from Defendant's illegal disclosure and negligent release of their PMI in violation of Cal. Civ. Code §§ 56.10 and 56.101, and therefore seek relief under Civ. Code §§ 56.35 and 56.36, including actual damages, nominal statutory damages of $1,000, punitive damages of $3,000, injunctive relief, and attorney fees, expenses and costs.

FIFTH CAUSE OF ACTION
DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Classes)

100. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

101. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

102. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' PII and PMI and whether Accellion is currently maintaining data security measures

adequate to protect Plaintiff's and Class Members from further data breaches that compromise their PII and PMI. Plaintiff alleges that Accellion's data security measures remain inadequate. Accellion denies these allegations. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of his PII and PMI and remains at imminent risk that further compromises of his PII and/or PMI will occur in the future.

103. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Accellion owes a legal duty to secure consumers' PII and PMI and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, HIPAA, and various state statutes; and

b. Accellion continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII and PMI.

104. This Court also should issue corresponding prospective injunctive relief requiring Accellion to employ adequate security protocols consistent with law and industry standards to protect consumers' PII and PMI.

105. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Accellion. The risk of another such breach is real, immediate, and substantial. If another breach at Accellion occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

106. The hardship to Plaintiff if an injunction does not issue exceeds the hardship to Accellion if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Accellion of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Accellion has a pre-existing legal obligation to employ such measures.

107. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Accellion, thus

eliminating the additional injuries that would result to Plaintiff and consumers whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE Plaintiff on behalf of herself and all other similarly situated, prays for relief as follows:

a. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Classes and Plaintiff's attorneys as Class Counsel to represent the Classes;

b. For an order finding in favor of Plaintiff and the Classes on all counts asserted herein;

c. For damages in an amount to be determined by the trier of fact;

d. For an order of restitution and all other forms of equitable monetary relief;

e. Declaratory and injunctive relief as described herein;

f. Awarding Plaintiff's reasonable attorneys' fees, costs, and expenses;

g. Awarding pre- and post-judgment interest on any amounts awarded; and,

h. Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMANDED

A jury trial is demanded on all claims so triable.

Dated: April 7, 2021

CARLSON LYNCH LLP

By: */s/Todd D. Carpenter*

Todd D. Carpenter (234464)
1350 Columbia St., Ste. 603
San Diego, CA 92101
Tel.: 619-762-1900
Fax: 619-756-6991
tcarpenter@carlsonlynch.com

Karen Hanson Riebel (*pro hac vice* forthcoming)
Kate M. Baxter-Kauf (*pro hac vice* forthcoming)
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Avenue South, Suite 2200
Minneapolis, MN 55401
khriebel@locklaw.com
kmbaxter-kauf@locklaw.com

Attorneys for Plaintiff

CIVIL COVER SHEET

The JS-CAND 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved in its original form by the Judicial Conference of the United States in September 1974, is required for the Clerk of Court to initiate the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

AARON SHARP, on behalf of himself and all others similarly situated,

(b) County of Residence of First Listed Plaintiff Fayette County, KY
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*

CARLSON LYNCH, LLP, 1350 Columbia St., Ste. 603, San Diego, CA 92101
Telephone: (619) 762-1900

DEFENDANTS

ACCELLION, INC.

County of Residence of First Listed Defendant
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 2 U.S. Government Defendant
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☒ 4
Citizen of Another State	☒ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment Of Veteran's Benefits
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☒ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury -Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury – Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities–Employment
- ☐ 446 Amer. w/Disabilities–Other
- ☐ 448 Education

PRISONER PETITIONS

HABEAS CORPUS
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

OTHER
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee–Conditions of Confinement

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC § 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC § 158
- ☐ 423 Withdrawal 28 USC § 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent–Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS–Third Party 26 USC § 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC § 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced & Corrupt Organizations
- ☐ 480 Consumer Credit
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation–Transfer ☐ 8 Multidistrict Litigation–Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. § 1332(d)(2)(A) and 28 U.S.C. § 1391(b)(1)

Brief description of cause:
Negligence; Negligence Per Se, Unjust Enrichment, Cal. Confidentiality of Medical Information Act, Declaratory Judgment

VII. REQUESTED IN COMPLAINT:

✓ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, Fed. R. Civ. P.

DEMAND $

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S), IF ANY *(See instructions):*

JUDGE Hon. Edward J. Davila DOCKET NUMBER 5:21-cv-01155-EJD

IX. DIVISIONAL ASSIGNMENT (Civil Local Rule 3-2)

(Place an "X" in One Box Only) ☒ **SAN FRANCISCO/OAKLAND** ☐ **SAN JOSE** ☐ **EUREKA-MCKINLEYVILLE**

DATE 04/07/2021 **SIGNATURE OF ATTORNEY OF RECORD** /s/ Todd D. Carpenter

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS-CAND 44

Authority For Civil Cover Sheet. The JS-CAND 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved in its original form by the Judicial Conference of the United States in September 1974, is required for the Clerk of Court to initiate the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I. a) Plaintiffs-Defendants. Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

b) County of Residence. For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

c) Attorneys. Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)."

II. Jurisdiction. The basis of jurisdiction is set forth under Federal Rule of Civil Procedure 8(a), which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.

(1) United States plaintiff. Jurisdiction based on 28 USC §§ 1345 and 1348. Suits by agencies and officers of the United States are included here.

(2) United States defendant. When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.

(3) Federal question. This refers to suits under 28 USC § 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.

(4) Diversity of citizenship. This refers to suits under 28 USC § 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)

III. Residence (citizenship) of Principal Parties. This section of the JS-CAND 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. Nature of Suit. Place an "X" in the appropriate box. If the nature of suit cannot be determined, be sure the cause of action, in Section VI below, is sufficient to enable the deputy clerk or the statistical clerk(s) in the Administrative Office to determine the nature of suit. If the cause fits more than one nature of suit, select the most definitive.

V. Origin. Place an "X" in one of the six boxes.

(1) Original Proceedings. Cases originating in the United States district courts.

(2) Removed from State Court. Proceedings initiated in state courts may be removed to the district courts under Title 28 USC § 1441. When the petition for removal is granted, check this box.

(3) Remanded from Appellate Court. Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.

(4) Reinstated or Reopened. Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.

(5) Transferred from Another District. For cases transferred under Title 28 USC § 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.

(6) Multidistrict Litigation Transfer. Check this box when a multidistrict case is transferred into the district under authority of Title 28 USC § 1407. When this box is checked, do not check (5) above.

(8) Multidistrict Litigation Direct File. Check this box when a multidistrict litigation case is filed in the same district as the Master MDL docket.

Please note that there is no Origin Code 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.

VI. Cause of Action. Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC § 553. Brief Description: Unauthorized reception of cable service.

VII. Requested in Complaint. Class Action. Place an "X" in this box if you are filing a class action under Federal Rule of Civil Procedure 23.

Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.

Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. Related Cases. This section of the JS-CAND 44 is used to identify related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

IX. Divisional Assignment. If the Nature of Suit is under Property Rights or Prisoner Petitions or the matter is a Securities Class Action, leave this section blank. For all other cases, identify the divisional venue according to Civil Local Rule 3-2: "the county in which a substantial part of the events or omissions which give rise to the claim occurred or in which a substantial part of the property that is the subject of the action is situated."

Date and Attorney Signature. Date and sign the civil cover sheet.