FILE BY FAX

Daniel C. Girard (State Bar No. 114826)
Jordan Elias (State Bar No. 228731)
Adam E. Polk (State Bar No. 273000)
Simon Grille (State Bar No. 294914)
GIRARD SHARP LLP
601 California Street, Suite 1400
San Francisco, California 94108
Telephone: (415) 981-4800
Facsimile: (415) 981-4846
Email: dgirard@girardsharp.com
Email: jelias@girardsharp.com
Email: apolk@girardsharp.com
Email: sgrille@girardsharp.com

Counsel for Plaintiff

SUPERIOR COURT FOR THE STATE OF CALIFORNIA

COUNTY OF ALAMEDA

MICHAEL ERAZO, on behalf of himself and all others similarly situated,

Plaintiff,

vs.

THE REGENTS OF THE UNIVERSITY OF CALIFORNIA and ACCELLION, INC.,

Defendants.

Case No. RG21097796

CLASS ACTION

CLASS ACTION COMPLAINT FOR:

1. Violation of the California Consumer Privacy Act of 2018, Civ. Code § 1798.100 *et seq.*;
2. Violation of the California Confidentiality of Medical Information Act, Civ. Code § 56 *et seq.*;
3. Violation of the Unfair Competition Law, Bus. & Prof. Code § 17200 *et seq.*;
4. Negligence; and
5. Invasion of Privacy

DEMAND FOR JURY TRIAL

Plaintiff Michael Erazo ("Plaintiff"), individually and on behalf of the proposed class defined below, brings this action against Defendants The Regents of the University of California ("UC Regents") and Accellion, Inc. ("Accellion"), and alleges as follows:

I. SUMMARY OF THE ACTION

1. Defendants neglected to secure the sensitive personal information of individuals affiliated with the University of California ("UC"), including employees and their dependents and beneficiaries, retirees and their beneficiaries, and students and their families. The UC system uses Accellion—a cloud solutions company—to collect and transfer personally identifiable information ("PII"). In December 2020 and January 2021, Accellion detected breaches of its electronic information systems that compromised millions of people's most sensitive information (the "Data Breach").

2. For members of the affected UC populations, PII stolen in the Data Breach includes (but is not limited to) names, addresses, telephone numbers, birthdates, Social Security numbers, and bank account information. Also compromised were personal health information related to medical benefits and personal information associated with employee pension plans. UC officials acknowledged "this is a real and serious attack on Accellion that has impacted UC."[1]

3. Accellion has blamed its own customers like UC for the breach, claiming they should have upgraded to one of Accellion's newer products. But it is Plaintiff and the members of the proposed class who lost control of their sensitive information and now must deal with the fallout from the hack. PII taken in the UC hack has been disclosed on the internet, and Plaintiff Erazo recently received an alert from his credit monitoring service informing him that his PII was discovered on the dark web. (The dark web is a hidden network of black-market websites that serves as a "haven for all kinds of illicit activity (including the trafficking of stolen personal information captured through means such as data breaches or hacks)."[2])

[1] https://ucnet.universityofcalifornia.edu/data-security/updates-faq/accellion-faq.html (last visited Apr. 25, 2021).

[2] https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/ (last visited Apr. 26, 2021).

4. Plaintiff by this action seeks compensatory damages together with injunctive relief to remediate Defendants' deficient cybersecurity protocols, and to provide credit monitoring, identity theft insurance, and credit repair services to protect him and the other breach victims from identity theft and fraud.

II. PARTIES

5. Plaintiff Michael Erazo is a citizen and resident of Albany, California. He was employed by UC Berkeley as a student employee, Community Service Officer, and Public Safety Dispatcher from 2002 to 2017. For several years, Mr. Erazo and his wife were enrolled in a health insurance plan through UC. On April 3, 2021, Mr. Erazo received an email from UC officials informing him of the Data Breach and advising him to take protective measures. Mr. Erazo signed up for the Experian credit monitoring service offered by UC for one year. His medical and other personal information was exposed in the Data Breach; Experian notified him that it had discovered his PII on the dark web.

6. Defendant The Regents of the University of California is a government corporation headquartered in Alameda County, California. The Regents serve as the governing body of the University of California.

7. Defendant Accellion, Inc. is a Delaware corporation with its principal place of business in Palo Alto, California.

III. JURISDICTION AND VENUE

8. This Court has jurisdiction over this action under section 410.10 of the California Code of Civil Procedure and Article VI, section 10 of the California Constitution.

9. This Court has personal jurisdiction over Defendants because they are headquartered in and have their principal places of business in California.

10. Venue is proper in this Court under Code of Civil Procedure sections 395 and 395.5 because Defendant UC Regents is headquartered in this county and a substantial part of the acts or omissions giving rise to this action occurred in this county.

IV. FACTUAL ALLEGATIONS

The Accellion Data Breach

11. Accellion is a cloud solutions company that provides an enterprise content firewall that it represents "prevents data breaches and compliance violations from third party cyber risk."[3] Accellion holds itself out as providing a platform that ensures that PII can be securely transmitted between people and entities.

12. Accellion has represented that its content firewall:

> provides the security and governance [information security officers] need to protect their organizations, mitigate risk, and adhere to rigorous compliance regulations . . . . Accellion solutions have protected more than 25 million end users at more than 3,000 global corporations and government agencies, including NYC Health + Hospitals; KPMG; Kaiser Permanente; National Park Service; Tyler Technologies; and the National Institute for Standards and Technology (NIST).[4]

13. Accellion boasts on its website that it "enables millions of executives, employees, customers, vendors, partners, investors, attorneys, doctors, patients, and professionals from every walk of life to do their jobs without putting their organization at risk. When they click the Accellion button, they know it's the safe and secure way to share information with the outside world."[5]

14. Accellion's privacy policy further states that it "control[s] information that is provided directly to [it]," and "takes appropriate steps to ensure data privacy and security including through various hardware and software methodologies."[6] But those steps did not stop hackers from breaching its servers and taking Plaintiff's and class members' highly sensitive personal information.

15. In mid-December 2020, Accellion learned of two security vulnerabilities in its Accellion FTA software, a product that specializes in large file transfers. In technical terms, the

---

[3] https://www.accellion.com/company/ (last visited Apr. 27, 2021).

[4] *Id.*

[5] https://www.accellion.com/platform/simple/secure-third-party-communication/ (last visited Apr. 27, 2021).

[6] https://www.accellion.com/privacy-policy/ (last visited Apr. 27, 2021).

vulnerabilities were described as SQL Injection (CVE-2021-27101) and OS Command Execution (CVE-2021-27104).

16. Approximately four days after learning of these vulnerabilities, Accellion released a software patch to remediate the problem, followed by another patch three days later.

17. In mid-January 2021, Accellion learned of two more security vulnerabilities in its Accellion FTA software. These vulnerabilities were described as Server-Side Request Forgery (CVE-2021-27103) and OS Command Execution (CVE-2021-27102).

18. After learning of these additional vulnerabilities, Accellion issued a critical security alert on January 22 advising FTA customers—including UC—to shut down their FTA systems immediately.

19. Approximately three days after learning of the January vulnerabilities, Accellion released a patch to remediate the problem. Three days later, Accellion released another patch to increase the frequency of security anomaly detection.

20. As a result of these vulnerabilities, Accellion FTA was the subject of a cyberattack that continued into January 2021. Unauthorized third parties gained access to large amounts of PII and other data stored on or being transferred through Accellion FTA.

21. The cybersecurity firm Mandiant described the Accellion vulnerabilities as being "of critical severity because they were subject to exploitation via unauthenticated remote code execution."[7] Mandiant attributed the attack to two separate threat groups—one (UNC2546) responsible for compromising the system, and the other (UNC2582) believed to be responsible for engaging in extortion activity using some of the compromised information.

22. On February 28, Mandiant's review also identified two further vulnerabilities, of "medium" to "high severity."

23. In the wake of the Data Breach, Accellion stated that the intrusion occurred on Accellion FTA. Accellion described that platform as a "20 year old product nearing end-of

[7] https://www.accellion.com/sites/default/files/trust-center/accellion-fta-attack-mandiant-report-full.pdf (last visited Apr. 26, 2021).

life" and maintained it had "encouraged all FTA customers to migrate to kiteworks." Accellion also stated its intent to "accelerate[] our FTA end-of-life plans in light of these attacks."[8]

24. Accellion has attempted to deflect responsibility for the incident. It stated that it has encouraged its customers to upgrade their platform for three years.

25. Accellion has also represented that its "customers were promptly notified of the attack on December 23, 2020."[9] But the UC system did not announce the breach until March 31, 2021—after some UC community members began receiving messages threatening to release their personal data.

The UC Data Breach

26. On March 29, hackers began publishing screenshots of personal data they obtained from the Data Breach. The screenshots showed PII like home addresses, Social Security numbers, immigration status, dates of birth, and passport numbers. Some of the screenshots displayed lists of individuals along with their Social Security numbers, retirement documentation, and benefit adjustment requests. Hackers also posted UC employee benefit application forms and UCPath[10] Blue Shield health savings plan enrollment requests.

27. Also beginning on March 29, holders of UC email accounts began receiving emails that threatened to publish the recipient's personal information. The emails linked to a website that contained a sample of UC employees' personal information. The subject of the emails states, "Your personal data has been stolen and will be published." Email accounts at multiple campuses throughout the UC system received similar messages. The emails, one of which is reproduced below, threaten to publish the stolen information on the dark web and appear to seek a ransom.

---

[8] https://www.accellion.com/company/press-releases/accellion-provides-update-to-recent-fta-security-incident/ (last visited Apr. 27, 2021).

[9] *Id.*

[10] UCPath is the University of California's payroll, benefits, human resources and academic personnel system for all UC employees. The UCPath system is used at every UC location, including campuses, medical centers, research centers, and UC Office of the President (UCOP). https://ucpath.berkeley.edu/about-ucpath (last visited Apr. 26, 2021)

From: [redacted]
Date: Tue, Mar 30, 2021 at 8:55 AM
Subject: Your personal data has been stolen and will be published
To: [redacted]

Good day!
If you received this letter, you are a customer, student, partner or employee of University of California.
The company has been hacked, data has been stolen and will soon be released as the company refuses to protect its peoples' data.

We inform you that information about you will be published on the darknet ([redacted]
dog/universityofcalifornia-edu) if the university does not contact us.
Call or write to this store and ask to protect your privacy!!!!

28. The Data Breach and alarming messages affected UC entities and communities all over the state, including at UC Berkeley, UCLA, UC Davis, UC San Diego, UC Irvine, and UC Merced.

29. The UC system first announced the Data Breach on March 31, providing limited information about the breach and encouraging members of the UC community to take steps to protect their personal information, such as placing a fraud alert or a security freeze.

30. On April 2, the UC system issued a more detailed announcement, acknowledging that "Accellion was the target of international cyber attack where the perpetrators exploited a vulnerability in Accellion's programs and attacked roughly 100 organizations. The attackers have published stolen information on the Internet in an attempt to get money from organizations and individuals."[11] The UC system further announced that it would be offering the UC community one year of credit monitoring and identity theft protection through Experian.

31. On April 5 and April 8, UC disclosed more information about the breach. UC announced: "At this time, we believe the stolen information includes but is not limited to names, addresses, telephone numbers, birth dates, Social Security numbers and bank account information for a range of UC populations, including employees and their dependents and

[11] https://ucnet.universityofcalifornia.edu/news/2021/04/update-on-accellion-breach-and-what-you-should-do.html (last visited Apr. 27, 2021).

beneficiaries, retirees and their beneficiaries, students and their families, and potentially other individuals with connections to UC."[12]

32. UC also confirmed that personal information relating to medical and pension benefits was exposed in the Data Breach.

33. UC's announcement described the Data Breach as "a real and serious attack on Accellion that has impacted UC" and emphasized "that this event is very serious."[13]

34. Plaintiff received alerts that his confidential personal information is now on the dark web.

V. CLASS ACTION ALLEGATIONS

35. Under Code of Civil Procedure section 382, Plaintiff seeks certification of a Class of California citizens whose personally identifiable information was in UC's electronic information systems and was compromised as a result of the 2020-21 breach of Accellion's electronic information systems. Excluded from the Class are Defendants, as well as their officers, directors, and managerial employees. Also excluded from the Class is anyone employed by counsel for the parties in this action and any Judge to whom this case is assigned, as well as his or her staff and immediate family.

36. Plaintiff reserves the right to modify, change, or expand the Class definition, including by proposing subclasses, based on discovery and further investigation.

37. Numerosity. While the exact number of Class members is not known at this time, the Class is so numerous that joinder of all members is impractical. The UC system publicly conceded that the Data Breach impacted a host of UC populations, including employees and their dependents and beneficiaries, retirees and their beneficiaries, students and their families, and potentially other individuals with connections to UC. The identities of Class members are readily ascertainable from information and records in the possession, custody, or control of Defendants, and notice of this action can be readily provided to the Class.

---

[12] https://ucnet.universityofcalifornia.edu/news/2021/04/frequently-asked-questions-about-the-accellion-data-breach.html (last visited Apr. 27, 2021).

[13] https://ucnet.universityofcalifornia.edu/data-security/updates-faq/accellion-faq.html (last visited Apr. 26, 2021)

38. Typicality. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had his PII compromised in the Data Breach. Plaintiff and Class members were injured by the same wrongful acts, practices, and omissions of Defendants, as described herein. Plaintiff's claims thus arise from the same course of conduct that gives rise to the claims of all Class members.

39. Adequacy of Representation. Plaintiff is a member of the proposed Class and will fairly and adequately represent and protect its members' interests. Plaintiff's counsel are competent and experienced in class action and privacy litigation and will pursue this action vigorously. Plaintiff has no interests adverse to the interests of other Class members.

40. Predominant Common Issues of Law and Fact. There is a well-defined community of interest in the common questions of law and fact affecting Class members. The questions of law and fact common to Class members predominate over questions affecting only individual Class members. Among the questions of law and fact common the class are:

a. Whether Defendants had a duty to implement reasonable cybersecurity measures to protect Plaintiff's and Class members' sensitive personal information and to promptly alert them if such information was compromised;

b. Whether Defendants breached their duties by failing to take reasonable precautions to protect Plaintiff's and Class members' sensitive personal information;

c. Whether Defendants acted negligently by failing to implement reasonable data security practices and procedures;

d. Whether Defendants violated the California Confidentiality of Medical Information Act, Civ. Code § 56 *et seq.*;

e. Whether Accellion violated the California Consumer Privacy Act of 2018, Civ. Code § 1798.100 *et seq.*;

f. Whether Defendants' failures to implement reasonable data security protocols and to timely notify Plaintiff and Class members of the Data Breach violate the Unfair Competition Law, Bus. & Prof. Code § 17200 *et seq.*; and

g. Whether Plaintiff and Class members are entitled to statutory damages, actual damages, and other equitable relief.

41. Superiority. This class action is superior to other alternatives for the fair and efficient adjudication of this controversy. Absent a class action, most members of the Class would find the cost of litigating their claims individually to be prohibitively high and would have no effective remedy. Class treatment will conserve judicial resources, avoid the risk of inconsistent rulings, and promote efficiency of adjudication.

42. Defendants have acted or refused to act on grounds generally applicable to the entire Class, thereby making it appropriate for this Court to grant injunctive and declaratory relief with respect to the Class as a whole.

FIRST CAUSE OF ACTION
Violation of the California Consumer Privacy Act of 2018
Civ. Code § 1798.100 *et seq.* (CCPA)
(Against Accellion)

43. Plaintiff incorporates the above allegations as if fully set forth herein.

44. Section 1798.150(a)(1) of the CCP provides, "[a]ny consumer whose nonencrypted or nonredacted personal information, as defined by [Civil Code section 1798.81.5(d)(1)(A)] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for" statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

45. Plaintiff is a consumer and California resident as defined by Civil Code section 1798.140(g).

46. Defendant Accellion is a "business" as defined by Civil Code section 1798.140(c) because it is a "sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners that collects consumers' personal information or on the behalf of which that information is collected and that alone, or jointly

with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California." Defendant has annual gross revenues in excess of $25 million. Defendant annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, householders, or devices.

47. Plaintiff's and Class members' personal information, as defined by Civil Code section 1798.81.5(d)(1)(A), was subject to unauthorized access and exfiltration, theft or disclosure. The Data Breach described herein exposed, without limitation, names, addresses, telephone numbers, birthdates, Social Security numbers, and bank account information.

48. Plaintiff's and Class members' PII was in nonencrypted and nonredacted form, allowing criminals to access it.

49. The Data Breach occurred as a result of Accellion's failure to implement and maintain reasonable security procedures and practices for protecting the exposed information given its nature. Accellion failed to monitor its systems to identify suspicious activity and allowed unauthorized access to Plaintiff's and Class members' PII.

50. Consistent with Civil Code section 1798.150(b)(1), Plaintiff provided written notice to Accellion identifying the CCPA provisions Accellion violated. If Accellion is unable to cure or does not cure the violation within 30 days, Plaintiff will amend this complaint to pursue actual or statutory damages as permitted by Civil Code section 1798.150(a)(1)(A).

51. Plaintiff presently seeks injunctive and declaratory relief, and any other relief as deemed appropriate by the Court, for Accellion's CCPA violations.

SECOND CAUSE OF ACTION
Violation of the California Confidentiality of Medical Information Act
Civ. Code § 56 *et seq.* (CMIA)
(Against All Defendants)

52. Plaintiff incorporates the above allegations as if fully set forth herein.

53. Under section 56.10(a) of the Civil Code, "[a] provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of the

provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization[.]"

54. Each Defendant is a "provider of health care" as defined in Civil Code section 56.06. Each Defendant is organized in part for the purpose of maintaining medical information to make it available to an individual or provider of health care for purposes of information management, diagnosis, or treatment.

55. Plaintiff and Class members are "patients" within the meaning of Civil Code section 50.05(k) and are "endanger[ed]" within the meaning of Civil Code section 56.05(e) because Plaintiff and Class members reasonably fear that disclosure of their medical information could subject them to harassment or abuse.

56. Plaintiff and Class members, as patients, had their individually identifiable "medical information," within the meaning of Civil Code section 56.05(j), created, maintained, preserved, stored, abandoned, destroyed or disposed of on or through Defendants' computer networks at the time of the Data Breach.

57. Defendants, through their failure to implement and maintain reasonable security procedures and practices, allowed unauthorized persons to gain access to, view, and/or download Plaintiff's and Class members' medical information without their consent in violation of Civil Code section 56.10(a).

58. UC Regents continued to use and uploaded sensitive medical information to Accellion FTA despite knowing that the software lacked adequate security to protect it from being hacked. By uploading and transferring files using the outmoded Accellion FTA software, UC Regents took affirmative actions that resulted in the disclosure of medical information.

59. In violation of Civil Code section 56.10(e), Defendant Accellion disclosed Plaintiff's and Class members' medical information to persons or entities not engaged in providing direct health care services to Plaintiff or Class members, their providers of health care, their health care service plans, or their insurers or self-insured employers. Accellion's affirmative actions that resulted in the disclosure of medical information include, among other

things, failing to transition its clients from the legacy FTA software, which lacked adequate security to protect medical information.

60. Defendants violated Civil Code section 56.101 by failing to maintain and preserve the confidentiality of the medical information of Plaintiff and Class members.

61. In violation of Civil Code section 56.101(a), Defendants negligently created, maintained, preserved, stored, abandoned, destroyed, or disposed of Plaintiff's and Class members' medical information in a manner that failed to preserve the security of that information and breached its confidentiality .

62. Medical information that was the subject of the Data Breach included "electronic medical records" or "electronic health records" as defined by Civil Code section 56.101(c).

63. In violation of Civil Code section 56.101(b)(1)(A), Defendants' electronic health record system or electronic medical record system failed to protect and preserve the integrity of electronic medical information.

64. Defendants also violated Civil Code section 56.36(b) by negligently releasing Plaintiff's and Class members' confidential information.

65. Defendants' wrongful conduct, actions, inaction, omissions, and want of ordinary care violate the CMIA and directly and proximately caused the Data Breach. As a result, Plaintiff and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm including, without limitation: (1) loss of the opportunity to control how their medical information is used; (2) diminution in the value and use of their medical information entrusted to Defendants with the understanding that Defendants would safeguard it against theft and not allow it to be accessed and misused by third parties; (3) the compromise and theft of their medical information; (4) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and misuse of their medical information; (5) continued risk to their medical information; and (6) future costs in the form of time, effort, and money they will expend to prevent, detect, contest, and repair the adverse effects of their medical information being stolen in the Data Breach.

66. Plaintiff and Class members were injured and have suffered damages, as described above, from Defendants' illegal disclosure and negligent release of their medical information in violation of Civil Code sections 56.10, 56.36, and 56.101, and accordingly are entitled to relief under Civil Code sections 56.35 and 56.36, including actual damages, nominal statutory damages of $1,000, punitive damages (from Accellion only) of $3,000, injunctive relief, and attorney fees, expenses and costs.

THIRD CAUSE OF ACTION
Violation of the Unfair Competition Law,
Bus. & Prof. Code § 17200 *et seq.* (UCL)
(Against All Defendants)

67. Plaintiff incorporates the above allegations as if fully set forth herein.

68. The UCL proscribes "any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." Cal. Bus. & Prof. Code § 17200.

69. Defendants' conduct is unlawful, in violation of the UCL, because it violates the CCPA and CMIA.

70. Defendants' conduct also is unfair and deceptive in violation of the UCL. Defendants' unfair and fraudulent business acts and practices include:

a. failing to adequately secure the personal information of Plaintiff and Class members from disclosure to unauthorized third parties or for improper purposes;

b. enabling the disclosure of personal and sensitive facts about Plaintiff and Class members in a manner highly offensive to a reasonable person;

c. enabling the disclosure of personal and sensitive facts about Plaintiff and Class members without their informed, voluntary, affirmative, and clear consent;

d. unreasonably delaying in providing notice of the Data Breach and thereby preventing Plaintiff and Class members from taking timely self-protection measures; and

e. omitting, suppressing, and concealing the material fact that Defendants did not reasonably or adequately secure Plaintiff's and Class members' personal information.

71. Defendants' omissions were material because they were likely to deceive reasonable consumers about the adequacy of its data security and ability to protect the confidentiality of Plaintiff's and Class members' personal information.

72. The gravity of harm resulting from Defendants' unfair conduct outweighs any potential utility. The failure to adequately safeguard personal, sensitive information harms the public at large and is part of a common and uniform course of wrongful conduct.

73. The harm from Defendants' conduct was not reasonably avoidable by consumers. The persons affected by the Data Breach—UC employees and their dependents and beneficiaries, retirees and their beneficiaries, students and their families—were required to provide their PII as part of their relationship with the relevant UC institution. Plaintiff and Class members did not know of, and had no reasonable means of discovering, that their information would be exposed to hackers through inadequate data security measures.

74. There were reasonably available alternatives that would have furthered Defendants' business interests of electronically transferring their customers' information while protecting PII, such as discontinuing use of the legacy FTA product and ensuring best practices in cybersecurity defense.

75. A reasonable person would regard Defendants' derelict data security and the Data Breach as important, material facts that could and should have been disclosed.

76. As a direct and proximate result of Defendants' unfair methods of competition and unfair or deceptive acts or practices, Plaintiff lost money or property because his sensitive personal information experienced a diminution of value and because he devoted additional time to monitoring his financial accounts for fraudulent activity.

77. Plaintiff and Class members therefore seek all monetary and non-monetary relief permitted by law, including actual damages, treble damages, injunctive relief, civil penalties, and attorneys' fees and costs under Code of Civil Procedure section 1021.5.

FOURTH CAUSE OF ACTION

Negligence
(Against All Defendants)

78. Plaintiff incorporates the above allegations as if fully set forth herein.

79. Defendants collected and stored the personal information of Plaintiff and Class members, including their names, addresses, telephone numbers, birthdates, Social Security numbers and bank account information.

80. Defendants owed Plaintiff and Class members a duty of reasonable care to preserve and protect the confidentiality of their personal information that they collected. This duty included, among other obligations, maintaining and testing their security systems and computer networks, and taking other reasonable security measures to safeguard and adequately secure the personal information of Plaintiff and the Class from unauthorized access and use.

81. Plaintiff and Class members were the foreseeable victims of Defendants' inadequate cybersecurity. The natural and probable consequence of Defendants' failing to adequately secure their information networks was the hacking of Plaintiff's and Class members' personal information.

82. Defendants knew or should have known that Plaintiff's and Class members' personal information was an attractive target for cyber thieves, particularly in light of data breaches experienced by other entities around the United States. Moreover, the harm to Plaintiff and Class members from exposure of their highly confidential personal facts was reasonably foreseeable to Defendants.

83. Defendants had the ability to sufficiently guard against data breaches by implementing adequate measures to protect their systems, such as by removing the legacy Accellion FTA software and updating to a state of the art and current file transfer software.

84. Defendants breached their duty to exercise reasonable care in protecting Plaintiff's and Class members' personal information by failing to implement and maintain adequate security measures to safeguard Plaintiff's and Class members' personal information,

failing to monitor their systems to identify suspicious activity, and allowing unauthorized access to and exfiltration of Plaintiff's and Class members' confidential personal information.

85. Defendants also owed a duty to timely disclose to Plaintiff and Class members that their personal information had been or was reasonably believed to have been compromised. Timely disclosure was necessary so that Plaintiff and Class members could, among other things: (1) purchase identity protection, monitoring, and recovery services; (2) flag asset, credit, and tax accounts for fraud, including by reporting the theft of their Social Security numbers to financial institutions, credit agencies, and the IRS; (3) purchase or otherwise obtain credit reports; (4) place or renew fraud alerts on a quarterly basis; (5) intensively monitor loan data and public records; and (6) take other steps to protect themselves and attempt to avoid or recover from identity theft.

86. Defendants breached their duty to timely disclose the Data Breach to Plaintiff and Class members. After learning of the Data Breach, Defendants unreasonably delayed in notifying Plaintiff and Class members of the Data Breach. And that unreasonable delay caused foreseeable harm to Plaintiff and Class members by preventing them from taking timely self-protection measures in response to the Data Breach.

87. There is a close connection between Defendants' failure to employ reasonable security protections for its employees' personal information and the injuries suffered by Plaintiff and Class members. When individuals' sensitive personal information is stolen, they face a heightened risk of identity theft and need to: (1) purchase identity protection, monitoring, and recovery services; (2) flag asset, credit, and tax accounts for fraud, including by reporting the theft of their social security numbers to financial institutions, credit agencies, and the IRS; (3) purchase or otherwise obtain credit reports; (4) monitor credit, financial, utility, explanation of benefits, and other account statements on a monthly basis for unrecognized credit inquiries and charges; (5) place and renew credit fraud alerts on a quarterly basis; (6) contest fraudulent charges and other forms of identity theft; (7) repair damage to credit and financial accounts; and (8) take other steps to protect themselves and attempt to avoid or recover from identity theft and fraud.

88. The policy of preventing future harm strongly disfavors application of the economic loss rule, particularly given the extremely sensitive data entrusted to Defendants. Defendants had an independent duty in tort to protect this data and thereby avoid reasonably foreseeable harm to Plaintiff and class members.

89. As a result of Defendants' negligence, Plaintiff and Class members have suffered damages that have included or may, in the future, include, without limitation: (1) loss of the opportunity to control how their personal information is used; (2) diminution in the value and use of their personal information entrusted to Defendant with the understanding that Defendant would safeguard it against theft and not allow it to be accessed and misused by third parties; (3) the compromise and theft of their personal information; (4) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and unauthorized use of financial accounts; (5) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including increased costs to use credit, credit scores, credit reports, and assets; (6) unauthorized use of compromised personal information to open new financial and other accounts; (7) continued risk to their personal information, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect the personal information in its possession; and (8) future costs in the form of time, effort, and money they will expend to prevent, detect, contest, and repair the adverse effects of their personal information being stolen in the Data Breach.

FIFTH CAUSE OF ACTION
Invasion of Privacy
(Against All Defendants)

90. Plaintiff incorporates the above allegations as if fully set forth herein.

91. Defendants wrongfully intruded upon Plaintiff's and Class members' seclusion in violation of California law. Plaintiff and Class members reasonably expected that the personal information they entrusted to Defendants, such as their names, addresses, telephone numbers, birthdates, Social Security numbers and bank account information would be kept

private and secure, and would not be disclosed to any unauthorized third party or for any improper purpose.

92. Defendants unlawfully invaded Plaintiff's and Class members' privacy rights by:

a. failing to adequately secure their personal information from disclosure to unauthorized third parties or for improper purposes;

b. enabling the disclosure of personal and sensitive facts about them in a manner highly offensive to a reasonable person; and

c. enabling the disclosure of personal and sensitive facts about them without their informed, voluntary, affirmative, and clear consent.

93. A reasonable person would find it highly offensive that Defendants, having received, collected, and stored Plaintiff's and Class members' birthdates, Social Security numbers, and other personal details, failed to protect that information from unauthorized disclosure to third parties.

94. In failing to adequately protect Plaintiff's and Class members' personal information, Defendants acted knowingly and in reckless disregard of their privacy rights. Accellion was aware of the security vulnerabilities from its legacy system but failed to ensure that UC patched them, and UC knew of the need to patch those vulnerabilities but failed to do so. Defendants also knew or should have known that their ineffective security measures, and their foreseeable consequences, are highly offensive to a reasonable person in Plaintiff's position.

95. Defendants violated Plaintiff's and Class members' right to privacy under the common law as well as under the California Constitution, Art. I, § 1.

96. Defendants' unlawful invasions of privacy damaged Plaintiff and Class members. As a direct and proximate result of Defendants' unlawful invasions of privacy, Plaintiff and Class members suffered mental distress, and their reasonable expectations of privacy were frustrated and defeated.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for an order:

A. certifying this case as a class action, appointing Plaintiff as a Class representative, and appointing Plaintiff's counsel to represent the Class;

B. entering judgment for Plaintiff and the Class;

C. awarding Plaintiff and Class members monetary relief;

D. ordering appropriate injunctive relief;

E. awarding pre- and post-judgment interest as prescribed by law;

F. awarding reasonable attorneys' fees and costs as permitted by law;

G. granting such further and other relief as may be just and proper.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: April 27, 2021

Respectfully submitted,

By: _____

Daniel C. Girard (State Bar No. 114826)
Jordan Elias (State Bar No. 228731)
Adam E. Polk (State Bar No. 273000)
Simon Grille (State Bar No. 294914)
GIRARD SHARP LLP
601 California Street, Suite 1400
San Francisco, California 94108
Telephone: (415) 981-4800
Facsimile: (415) 981-4846
Email: dgirard@girardsharp.com
Email: jelias@girardsharp.com
Email: apolk@girardsharp.com
Email: sgrille@girardsharp.com

Attorneys for Plaintiff and the Proposed Class