FILE BY FAX

Simon Grille (State Bar No. 294914)
Jordan Elias (State Bar No. 228731)
Adam E. Polk (State Bar No. 273000)
Trevor T. Tan (State Bar No. 281045)
GIRARD SHARP LLP
601 California Street, Suite 1400
San Francisco, California 94108
Telephone: (415) 981-4800
Facsimile: (415) 981-4846
Email: sgrille@girardsharp.com
Email: jelias@girardsharp.com
Email: apolk@girardsharp.com
Email: ttan@girardsharp.com

Counsel for Plaintiffs

[Additional Counsel Appear on Signature Page]

SUPERIOR COURT FOR THE STATE OF CALIFORNIA
COUNTY OF ALAMEDA

MICHAEL ERAZO, MIGUEL OCHOA, JAMIE MCDOLE, ARIELLE FIELDS, ALVARO GALVIS, ROSE BECKER, STEVE GOLDFIELD, and KARLINA CHAVEZ, on behalf of themselves and all others similarly situated,

Plaintiffs,

vs.

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

Defendants.

Lead Case No. RG21097796
Consolidated and Related to:
Nos. RG21107152, RG21107777

CONSOLIDATED CLASS ACTION COMPLAINT

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 California Consumer Records Act, Civ. Code § 1798.80 *et seq.*;
4. Violation of the Information Practices Act, Civ. Code § 1798.1 *et seq.*;
5. Violation of the Unfair Competition Law, Bus. & Prof. Code § 17200 *et seq.*;
6. Negligence; and
7. Invasion of Privacy

DEMAND FOR JURY TRIAL

Plaintiffs Michael Erazo, Miguel Ochoa, Jamie McDole, Arielle Fields, Alvaro Galvis, Rose Becker, Steve Goldfield, and Karlina Chavez ("Plaintiffs"), individually and on behalf of the proposed class defined below, bring this consolidated action against Defendants The Regents of the University of California ("UC Regents") and Accellion, Inc. ("Accellion"), and allege as follows:

I. SUMMARY OF THE ACTION

1. Defendants neglected to secure highly 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"). For members of the affected UC populations, PII stolen in the Data Breach includes (but is not limited to) full names, addresses, birthdates, Social Security numbers, telephone numbers, driver's license and passport information, financial information including bank routing and account numbers, health and related benefit information, and disability information, as well as other personal information provided to UC.

2. Neither Defendant notified the affected group until March 29, 2021. At that point, university officials acknowledged "this is a real and serious attack on Accellion that has impacted UC." 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 Plaintiffs and the other members of the proposed class who lost control of their sensitive personal facts and must deal with the fallout. PII taken in the UC hack has already been disclosed on the internet. Plaintiffs were alerted by a credit monitoring service that their PII is now on the dark web, 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)."[1]

3. Plaintiffs' information continues to reside on or remain accessible through Defendants' systems, and remains at risk. Plaintiffs by this action seek compensatory and statutory damages, together with injunctive relief to remediate Defendants' deficient cyber security and provide credit monitoring, identity theft insurance, and credit repair services (or the money needed to secure those services) to protect them and the other breach victims from identity theft and fraud.

II. PARTIES

4. Plaintiff Michael Erazo is a citizen and resident of Alameda County, California.

5. Plaintiff Miguel Ochoa is a citizen and resident of Kern County, California.

6. Plaintiff Jamie McDole is a citizen and resident of Sacramento County, California.

7. Plaintiff Arielle Fields is a citizen and resident of Sacramento County, California.

8. Plaintiff Alvaro Galvis is a citizen and resident of Orange County, California.

9. Plaintiff Rose Becker is a citizen and resident of Los Angeles County, California.

10. Plaintiff Steve Goldfield is a citizen and resident of Alameda County, California.

11. Plaintiff Karlina Chavez is a citizen and resident of Los Angeles County, California.

12. 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.

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

[1] https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/ (last visited Oct. 1, 2021).

III. JURISDICTION AND VENUE

14. 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.

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

16. 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

Plaintiffs' PII is Hacked in the Data Breach

Michael Erazo

17. Plaintiff Michael Erazo was employed by UC Berkeley as a student employee, Community Service Officer, and Public Safety Dispatcher from 2002 to 2017.

18. During his time as a student at UC Berkeley, Mr. Erazo received health care services from the student health facilities, including University Health Services and the Tang Center. In order to receive treatment and other health care services, Mr. Erazo provided personally identifying information, including his name, address, e-mail address, and telephone number. He also provided information concerning his medical history, mental or physical condition, and treatment history. For several years, Mr. Erazo was enrolled in a health insurance plan through UC.

19. 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. His personal information was exposed in the Data Breach. Mr. Erazo signed up for the Experian credit monitoring service that UC offered for one year. Experian notified him that it had discovered his PII on the dark web.

20. The exposure of his private and confidential information in the Data Breach has caused Mr. Erazo to suffer stress related to his personal information being compromised and to

devote significantly more time to checking his credit reports and financial accounts for fraudulent activity. Mr. Erazo has anxiety and increased concerns over the loss of his privacy.

Miguel Ochoa

21. Plaintiff Miguel Ochoa was a student at UC Irvine from 2014 to 2019, and a part-time student employee at UC Irvine from 2016 until 2019. In 2019, UC Irvine hired him as a full-time employee, after which Mr. Ochoa left the position on good terms to pursue a graduate degree.

22. During his time as a student at UC Irvine, Mr. Ochoa received health care services from the student health facilities, including the UCI Student Health Center. In order to receive treatment and other health care services, Mr. Ochoa provided personally identifying information, including his name, address, e-mail address, and telephone number. He also provided information concerning his medical history, mental or physical condition, and treatment history. Mr. Ochoa was enrolled in a health plan, as well, through UCI.

23. On April 14, 2021, Mr. Ochoa received an email from UC officials informing him of the Data Breach and advising him to take protective measures. Mr. Ochoa signed up for the Experian credit monitoring service that UC offered for one year. Mr. Ochoa also received a letter from UC, dated June 30, informing him that his date of birth, Social Security number, and health insurance information were exposed in the Data Breach. Experian notified him that it had discovered his email address, phone number, and Social Security number on the dark web.

24. The exposure of his private and confidential information, including health information, in the Data Breach has caused Mr. Ochoa to suffer stress related to his personal information being compromised and to devote significantly more time to checking his credit reports and financial accounts for fraudulent activity. Mr. Ochoa has anxiety and increased concerns over the loss of his privacy.

Jamie McDole

25. Plaintiff Jamie McDole has been employed by UC Davis as a nurse Case Manager since 2008. She also previously attended UC Davis as a student.

26. Ms. McDole has received health care and is enrolled in health insurance through UC Davis. She provided UC Davis with her medical history including her immunization history. She also provided UC Davis with personally identifying information, including her name, address, e-mail address, and telephone number.

27. After learning of the Data Breach, Ms. McDole placed a credit alert for activity associated with her identity and signed up for the Experian credit monitoring service that UC offered for one year. On April 21, 2021, Ms. McDole was notified that her Social Security number had been found on the dark web. The notification specified "universityofcalifornia.edu" as the "potentially breached site" enabling this unauthorized disclosure.

28. Ms. McDole received a letter from UC, dated June 30, informing her that her date of birth, Social Security number, and health insurance information were exposed in the Data Breach.

29. In September 2021, Ms. McDole discovered fraudulent charges on her credit card and had to spend time closing the account. She has also experienced an increase in scam and phishing telephone calls since the Data Breach.

30. The exposure of her private and confidential information, including health information, in the Data Breach has caused Ms. McDole to suffer stress related to her personal information being compromised and to devote significantly more time to checking her credit reports and financial accounts for fraudulent activity. Ms. McDole has anxiety and increased concerns over the loss of her privacy.

Arielle Fields

31. Plaintiff Arielle Fields has been employed by the UC Davis Medical Center as a clinical nurse since approximately March 2020.

32. During her time as a UC Davis employee, Ms. Fields received health care services from UC Davis Medical Center facilities. In order to receive treatment and other health care services, Ms. Fields provided personally identifying information, including her

name, address, e-mail address, and telephone number. She also provided information concerning her medical history, mental or physical condition, and treatment history.

33. Beginning in or about April 2021, Ms. Fields began to receive emails from UC Regents informing her of the Data Breach and advising her to take protective measures. On May 14, 2021, Ms. Fields received an email titled, "Notice of Data Breach," informing her that an unauthorized third party had gained access to files which may contain her data, and that the impacted information "may include" her name, address, telephone number, Social Security number, driver's license information, passport information, financial information including bank routing and account numbers, health and related benefit information, disability information and birthdate, as well as other personal information.

34. After the Data Breach, sometime in June 2021, Ms. Fields learned that an unauthorized third party opened a debit/checking account in her name through Wells Fargo in May 2021.

35. Additionally, after the Data Breach, in or about May 2021, Ms. Fields was locked out of her Wells Fargo mortgage account and was not able to access her mortgage payments and account. She also discovered that her Experian credit monitoring account was hacked; she was locked out of that account as well.

36. Ms. Fields experienced an increase in scam and phishing telephone calls after the Data Breach.

37. When Ms. Fields signed up for Experian's credit monitoring service, Experian reported to Ms. Fields that her Social Security number was on the dark web.

38. As a result of the Data Breach, Ms. Fields spent time dealing with its consequences, including time spent on the telephone and going to Wells Fargo Bank to cancel the fraudulent debit/checking account, calling Wells Fargo to unlock her mortgage, time spent trying to unlock and eventually cancelling her Experian account, and dealing with the unsolicited telephone calls she received. Additionally, she spent time investigating credit monitoring and identity theft insurance options, and self-monitoring her accounts with greater frequency.

39. Ms. Fields suffered annoyance and stress as a result of the Data Breach and experiences anxiety concerning the related loss of her privacy.

Alvaro Galvis

40. Plaintiff Alvaro Galvis has been employed by the University of California, Irvine Medical Center intermittently since July 2019. He currently has a dual appointment with UCI Medical Center and Children's Hospital of Orange County, which is affiliated with UCI Medical Center, working as a sixth-year Pediatric Infectious Disease Fellow.

41. During his time as a UCI employee, Dr. Galvis received health care services from the UCI Medical Center. In order to receive treatment and other health care services, Dr. Galvis provided personally identifying information, including his name, address, e-mail address, and telephone number. He also provided information concerning his medical history, mental or physical condition, and treatment history.

42. On or around June 30, 2021, Dr. Galvis received a letter from UC Regents informing him of the Data Breach and that "the impacted files" contain his date of birth and Social Security number.

43. After the Data Breach, someone from the United Kingdom attempted to place fraudulent charges on his bank account using his debit card account number.

44. Experian Identity Works notified Dr. Galvis that it discovered his PII on the dark web. The notification specified "universityofcalifornia.edu" as the "potentially breached site" enabling this unauthorized disclosure.

45. Since the Data Breach, Dr. Galvis has experienced an increase in scam and phishing telephone calls.

46. As a result of the Data Breach, Dr. Galvis has spent time and money in an attempt to protect against identity and to stop the spam calls to his cell phone, including by purchasing subscriptions to Geico Identity Theft Insurance and Robokiller. Dr. Galvis also placed a fraud alert on his credit report, and purchased a subscription for delete.me in an attempt to remove his PII from the dark web.

47. Dr. Galvis has also spent time dealing with the Data Breach by investigating credit monitoring and identity theft insurance options, taking action in response to the attempted fraudulent charges to his bank account, and self-monitoring his accounts with greater frequency.

48. Dr. Galvis suffered annoyance and stress as a result of the Data Breach and experiences anxiety concerning the related loss of his privacy.

Rose Becker

49. From 2019 to the present, Plaintiff Rose Becker has been a student at the University of California, Los Angeles.

50. During her time as a student at UCLA, Ms. Becker received health care services from the student health facilities, including the UCLA Arthur Ashe Student Health & Wellness Center. In order to receive treatment and other health care services, Ms. Becker provided personally identifying information, including her name, address, e-mail address, and telephone number. She also provided information concerning her medical history, mental or physical condition, and treatment history.

51. On or around March 31, 2021, Ms. Becker received an email from UC Regents informing her of the Data Breach. She received additional emails regarding the Data Breach from the "UC Office of the President," on April 2, 2021, and from the "Office of the Administrative Vice Chancellor," on April 8, 2021.

52. In April 2021, Ms. Becker was notified by Experian that her Social Security number had been found on the dark web. The notification identified the "potential site" of the exposed PII as universityofcalifornia.edu.

53. In July 2021, Ms. Becker received a letter from UC Regents dated June 30, 2021, informing her of the Data Breach and that "[t]he impacted files contain your Social Security number."

54. After the Data Breach, Ms. Becker spent time dealing with its consequences, including time spent on the telephone, sorting through her unsolicited emails, investigating

credit monitoring and identity theft insurance options, and self-monitoring her accounts with greater frequency.

55. Ms. Becker suffered annoyance and stress as a result of the Data Breach and experiences anxiety concerning the related loss of her privacy.

Steve Goldfield

56. From approximately 1985 to 1996, Plaintiff Steve Goldfield was an employee of UC Berkeley, College of Engineering.

57. During his time as a UC Berkeley employee, Mr. Goldfield received health care treatment from campus medical facilities. In order to receive treatment, Mr. Goldfield provided personally identifying information, including his name, address, e-mail address, and telephone number.

58. On or around April 2 and 4, 2021, Mr. Goldfield received emails from UC Regents notifying him of the Data Breach.

59. On or around May 3, 2021, Mr. Goldfield was notified by UC Regents as follows: "you may have recently been notified by Experian that your Social Security number or other personal information has been found on the 'dark web,' or areas of the Internet commonly used for illegal activity."

60. As a result of the Data Breach, Mr. Goldfield spent several hours closing his bank account, opening and configuring a new bank account, and notifying his pension holders of the new account.

61. Also as a result of the Data Breach, Mr. Goldfield spent other time dealing with its consequences, including time spent on the telephone, sorting through his unsolicited emails, investigating credit monitoring and identity theft insurance options, and self-monitoring his accounts with greater frequency.

62. Mr. Goldfield suffered annoyance and stress as a result of the Data Breach and experiences anxiety concerning the related loss of his privacy.

Karlina Chavez

63. Plaintiff Karlina Chavez has been employed by UC Irvine as an administrative assistant since approximately July 2016.

64. In connection with her employment, Ms. Chavez provided UC Regents personally identifying information such as her name, address, e-mail address, Social Security number, telephone number and other sensitive personal and financial information.

65. On April 1, 2021, Ms. Chavez received an email from UC Regents informing her of the Data Breach and advising her to take protective measures. Ms. Chavez signed up for the Experian credit monitoring service that UC offered for one year.

66. On April 7, 2021 and again on April 17, Ms. Chavez was notified by Experian that her email address had been found on the dark web. On April 20, and again on August 2, Experian notified her that Social Security number also had been found on the dark web. The Experian notices dated April 20 and August 2 stated that the potential site of the exposed PII was "universityofcalifornia.edu."

67. On May 12 and 14, 2021, Ms. Chavez received a set of emails from UC Regents, one addressed to her and the other to her husband Andres Chavez (who is a beneficiary to her UC benefits), each email providing an updated "NOTICE OF DATA BREACH." The notices state that "an unauthorized party gained access to files that contain personal information relating to members of the UC community, including employees (current and former) and their dependents. . . [and] [t]he impacted information may include full names, addresses, telephone numbers, Social Security numbers, driver's license information, passport information, financial information including bank routing and account numbers, health and related benefit information, disability information and birthdates, as well as other personal information."

68. Ms. Chavez was the victim of identity theft after the Data Breach, both before and after she received UCI's notifications. Ms. Chavez had money fraudulently taken from her bank account.

69. Ms. Chavez has had to spend significant time and personal effort dealing with the consequences of the Data Breach, for example in contacting UCI, banks and other

companies, investigating credit monitoring options, closing her accounts that experienced fraudulent activity, remediating the consequences of identity theft and self-monitoring her accounts with greater frequency.

70. Ms. Chavez, as a result of the Data Breach, has experienced increased concerns about the loss of her privacy and the increased threat of personal and financial harm.

* * *

71. Each Plaintiff suffered injury in the form of damage to and diminution in the value of their personal information—a form of property that Plaintiffs entrusted to Defendants and which was compromised as a result of the Data Breach.

72. Plaintiffs' PII, including Social Security numbers, is now on the dark web and accessible to identity thieves and cyber criminals.

73. Each Plaintiff suffered and continues to experience stress, annoyance, and anxiety as a result of the Data Breach and the loss of privacy from their sensitive personal information being compromised.

74. Each Plaintiff suffered a present injury arising from the present and continuing risk of fraud, identity theft, and misuse resulting from their PII—especially their Social Security numbers and personal health information—being placed in the hands of unauthorized third parties.

75. Plaintiffs have a continuing interest in ensuring that their PII is protected and safeguarded from future breaches.

The Accellion Data Breach

76. 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."[2] Accellion holds itself out as providing a platform that ensures that PII can be securely transmitted between and among individuals and entities.

77. Accellion has represented that its content firewall:

[2] https://www.accellion.com/company/ (last visited June 30, 2021).

> 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).[3]

78. Accellion states 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."[4]

79. 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."[5]

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

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

82. 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).

83. 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.

---

[3] *Id.*

[4] https://www.accellion.com/platform/simple/secure-third-party-communication/ (last visited June 30, 2021).

[5] https://www.accellion.com/privacy-policy/ (last visited June 30, 2021).

84. 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.

85. As a result of these vulnerabilities, Accellion FTA was targeted by 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.

86. The cybersecurity firm Mandiant described the Accellion vulnerabilities as being "of critical severity because they were subject to exploitation via unauthenticated remote code execution."[6] 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 extortionary activity using some of the compromised information.

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

88. Four of Accellion's servers were compromised in the breach.

89. Accellion possesses logs of files that were downloaded from its FTA during the breach.

90. In the wake of the Data Breach, Accellion disclosed that the intrusion occurred on Accellion FTA. Accellion described that platform as a "20 year old product nearing end-of 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."[7]

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

92. UC, however, ignored these warnings and failed to transition from the outdated FTA system to kiteworks (or another secure file-sharing platform) prior to the Data Breach.

---

[6] https://www.accellion.com/sites/default/files/trust-center/accellion-fta-attack-mandiant-report-full.pdf (last visited June 30, 2021).

[7] https://www.accellion.com/company/press-releases/accellion-provides-update-to-recent-fta-security-incident/ (last visited June 30, 2021).

93. Accellion further stated that its "customers were promptly notified of the attack on December 23, 2020."[8] 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

94. On March 29, 2021, 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[9] Blue Shield health savings plan enrollment requests.

95. 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.

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!!!!

[8] *Id.*

[9] 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 the UC Office of the President (UCOP). https://ucpath.berkeley.edu/about-ucpath (last visited June 30, 2021).

96. 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.

97. The UC system first announced the Data Breach on March 31, 2021, 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.

98. On April 2, the UC system issued a more detailed announcement, acknowledging that "Accellion was the target of an international cyber attack where the perpetrators exploited a vulnerability in Accellion's program and attacked roughly 100 organizations. The attackers have published stolen information on the Internet in an attempt to get money from organizations and individuals."[10] The UC system further announced that it would be offering the UC community one year of credit monitoring and identity theft protection through Experian.

99. 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 beneficiaries, retirees and their beneficiaries, students and their families, and potentially other individuals with connections to UC."[11]

100. UC then issued a "Substitute Notice of Breach" on May 10, 2021 and updated it on May 21. In that Notice, UC added to the list of information compromised in the breach. UC announced that "impacted information may include full names, addresses, telephone numbers, Social Security numbers, driver's license information, passport information, financial information including bank routing and account numbers, health and related benefit information, disability information and birthdates, as well as other personal information

[10] https://ucnet.universityofcalifornia.edu/news/2021/04/update-on-accellion-breach-and-what-you-should-do.html (last visited Oct. 1, 2021).

[11] https://ucnet.universityofcalifornia.edu/news/2021/04/frequently-asked-questions-about-the-accellion-data-breach.html (last visited June 30, 2021).

provided to UC. Information provided by students who participated in the 2020 University of California Undergraduate Experience Survey (UCUES) was also impacted and posted to the internet by the threat actor." In addition, "[f]or individuals that submitted applications for admission to the 2020-21 school year, their responses to questions in their application were impacted, [and f]or individuals that started or submitted applications for the 2021-22 school year, their name, email address and phone number were impacted." [12]

101. On June 30 and July 1, UC sent another round of notices to individuals whose personal information was exposed in the Data Breach. The notice to each recipient specifies the category or categories of their personal information that was compromised.[13]

102. UC's announcement describes the Data Breach as "a real and serious attack on Accellion that has impacted UC," and emphasizes "this event is very serious."[14]

103. Each Plaintiff has received alerts that their confidential personal information is now on the dark web.

104. UC is a provider of health care through, among other things, its campus health system and university hospitals. UC, for example, operates five medical centers at UC Davis, UC Irvine, UCLA, UC San Diego, and UC San Francisco. UC also offers on-campus medical services to its students and employees. UC collects a wide array of personal information from students and employees. UCLA, for example, maintains an "Electronic Health Records" (EHR) system.

V. THE GOVERNMENT TORT CLAIMS ACT DOES NOT SHIELD UC REGENTS FROM LIABILITY IN THIS CASE

105. UC Regents is not immune under the Government Tort Claims Act. First, as set forth in more detail in the third and fourth causes of action below, UC breached mandatory duties imposed by the Information Practices Act and the Customer Records Act.

---

[12] https://ucnet.universityofcalifornia.edu/data-security/accellion-notice.html (last visited June 30, 2021).

[13] https://ucnet.universityofcalifornia.edu/data-security/updates-faq/index.html#ind-notice (last visited Sept. 18, 2021).

[14] https://ucnet.universityofcalifornia.edu/data-security/updates-faq/accellion-faq.html (last visited June 30, 2021)

106. Second, UC Regents may be held vicariously liable for negligent acts committed by its employees within the scope of their employment. UC employees were negligent in carrying out the day-to-day operations required to adequately secure Plaintiffs' and Class members' personal information from disclosure to unauthorized third parties or for improper purposes. The UC system recognizes that safeguarding personal information is critically important, as evident from its past commitments to enhance cyber security. *See*, *e.g.*, Plaintiffs' Supplemental Memorandum in Support of Unopposed Motion for Preliminary Approval of Class Settlement at 23, *Adlouni v. UCLA Health Systems Auxiliary, et al.*, No. BC589243 (Cal. Super. Ct. Los Angeles Cty.) (describing prior data breach settlement where UCLA Health agreed to "data security enhancements" and noting that UCLA Health already had "existing data security plans"). UC employees did not adequately implement UC's data security protocols and did not ensure UC's data security standards were followed, including by failing to migrate the outmoded Accellion FTA to kiteworks or another secure platform.

VI. CLASS ACTION ALLEGATIONS

107. Under Code of Civil Procedure section 382, Plaintiffs seek 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 and their officers, directors, and managerial employees. Also excluded 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.

108. Plaintiffs reserve the right to modify, change, or expand the Class definition, including by proposing subclasses, based on discovery and further investigation.

109. 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 exposed the private and confidential information of 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.

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

111. Adequacy of Representation. Plaintiffs are members of the proposed Class and will fairly and adequately represent and protect the other members' interests. Plaintiffs' counsel are competent and experienced in class action and privacy litigation and will pursue this action vigorously. Plaintiffs have no interests adverse to the interests of other Class members.

112. Predominant Common Issues of Law and Fact. There is a well-defined community of interest in the common questions of law and fact that underlie Class members' claims for relief. The questions of law and fact in this case that are common to Class members predominate over questions affecting only individual Class members. Among the questions of law and fact common to the Class are:

a. Whether Defendants had a duty to implement reasonable cybersecurity measures to protect Plaintiffs' 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 Plaintiffs' and Class members' sensitive personal information;

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

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

e. Whether Defendants violated the California Confidentiality of Medical Information Act, Civ. Code § 56 *et seq*. and/or the California Consumer Records Act, Civ. Code § 1798.80, *et seq*.

f. Whether UC Regents violated the Information Practices Act, Civ. Code § 1798.1, *et seq*.;

g. Whether UC Regents are immune from liability given the conduct and breaches in question;

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

i. Whether Plaintiffs and Class members are entitled to statutory damages, actual damages, injunctive and other relief in equity.

113. 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 waste and the risk of inconsistent rulings, and promote efficient adjudication before a single Judge.

114. 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)

115. Plaintiffs incorporate and reallege the foregoing allegations of fact.

116. 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.

117. Plaintiffs are consumers and California residents as defined by Civil Code section 1798.140(g).

118. 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."

119. Accellion collects personal information from, among other sources, consumers who request information from it, consumers who use its services, including users of its mobile applications, and consumers who submit customer support requests.

120. Mandiant found that the hackers who perpetrated the Data Breach used "tooling designed to facilitate exfiltration of data from the FTA system."[15] Accellion's servers were compromised in the breach, and Accellion possesses logs of files that were downloaded from its FTA during the breach.

121. Accellion has annual gross revenues in excess of $25 million. Accellion 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.

122. Plaintiffs' 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, full names,

[15] https://www.accellion.com/sites/default/files/trust-center/accellion-fta-attack-mandiant-report-full.pdf (last visited June 30, 2021).

addresses, telephone numbers, birthdates, Social Security numbers, driver's license information, passport information, financial information including bank routing and account numbers, health and related benefit information, and disability information, as well as other personal information provided to UC.

123. Accellion maintained Plaintiffs' and Class members' PII in a form that allowed criminals to access it.

124. 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 Plaintiffs' and Class members' PII.

125. Consistent with Civil Code section 1798.150, Plaintiffs provided written notice to Accellion identifying the CCPA provisions that Accellion violated. But Accellion failed to cure its violations within 30 days of Plaintiff's notification.

126. CCPA actions for statutory damages "may be brought by a consumer if, prior to initiating any action against a business for statutory damages on an individual or class-wide basis, a consumer provides a business 30 days' written notice identifying the specific provisions of this title the consumer alleges have been or are being violated." Civ. Code § 1798.150(b). In response to the notification, Accellion denied that it violated the CPA and therefore did not provide the required "express written statement that the violations have been cured and that no further violations shall occur[.]"

127. Accordingly, on behalf of the Class, Plaintiffs seek actual and statutory damages under Civil Code section 1798.150(a)(1)(A), injunctive and declaratory relief, and any other relief 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)

128. Plaintiffs incorporate and reallege the foregoing allegations of fact.

129. 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[.]"

130. Each Defendant is a "provider of health care" as defined in Civil Code sections 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. UC Regents operates medical centers, maintains electronic health care records, and provides health care services and plans to Plaintiffs, students, employees, and their dependents. In addition, under subdivision (b) of section 56.06, Accellion provides software that is designed to maintain medical information in order to make such information available to individuals or a provider of health care at the request of the individual or a provider of health care, for the purpose of diagnosis, treatment, or management of a medical condition of the individual. Accellion specifically notes on its website that it provides secure file-sharing services for hospitals and other medical professionals to facilitate "patient care" through the sharing of patient's medical records such as EKG results, x-rays, ultrasounds, MRIs and other "protected health information."[16]

131. Plaintiffs 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 Plaintiffs and Class members reasonably fear that disclosure of their medical information could subject them to abuse, extortion, or other harassment or harm.

132. Plaintiffs 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.

[16] https://www.accellion.com/hipaa-compliance/secure-medical-records-access-how-secure-file-sharing-helps-hospitals-adopting-emrs/ (last visited June 28, 2021).

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

134. In violation of Civil Code section 56.10(e), Defendants disclosed Plaintiffs' and Class members' medical information to persons or entities not engaged in providing direct health care services to Plaintiffs or Class members, their providers of health care, their health care service plans, or their insurers or self-insured employers.

135. 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 Plaintiffs' and Class members' medical information under its care.

136. 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 such information.

137. Defendants also violated Civil Code section 56.101 by failing to maintain and preserve the confidentiality of Plaintiffs' and Class members' medical information.

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

139. 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).

140. That the information taken in the breach was viewed by unauthorized individuals is evidenced by the fact that the personal information was posted on the dark web, the subject of ransom emails, and was used for identity theft and financial account misconduct. The information was necessarily viewed to be used in this manner.

141. 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.

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

143. Defendants' wrongful conduct, actions, inaction, omissions, and want of ordinary care violate the CMIA and directly and proximately caused the Data Breach. Plaintiffs and Class members consequently have suffered (and will continue to suffer) economic damages and other injuries and actual harm including, without limitation: (1) the compromise and theft of their medical information; (2) loss of the opportunity to control how their medical information is used; (3) 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; (4) out-of-pocket costs associated with the prevention and detection of, and recovery from, identity theft and misuse of their medical information; (5) continued undue 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.

144. Plaintiffs 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 per violation, injunctive relief, and attorney fees, expenses and costs.

THIRD CAUSE OF ACTION
Violation of the California Consumer Records Act, Civ. Code § 1798.80, *et seq.* (CCRA)
(Against All Defendants)

145. Plaintiffs incorporate and reallege the foregoing allegations of fact.

146. Plaintiffs and Class members are "customers" within the meaning of Civil Code section 1798.80(c), as they provided personal information to Defendants for the purpose of obtaining services from Defendants.

147. Defendants are "businesses" within the meaning of Civil Code section 1798.80(a). UC Regents is a corporation under Article IX, section 9 of the California Constitution and hence a "business" under the CCRA.

148. The CCRA provides that "[a] person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California . . . whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person . . . in the most expedient time possible and without unreasonable delay[.]" Civ. Code § 1798.82.

149. The Data Breach was a breach of security within the meaning of section 1798.82. PII stolen in the Data Breach, such as full names, addresses, telephone numbers, birthdates, Social Security numbers, driver's license information, financial information, and medical information, as well as other information, constitutes "personal information" within the meaning of section 1798.80(e).

150. In violation of the CCRA, Defendants unreasonably delayed in notifying Plaintiffs and Class members of the Data Breach. Defendants were aware of Data Breach by no later than December 2020, but the Data Breach was not announced until March 31, 2021—after some UC community members began receiving messages threatening to release their personal data. There were no legitimate law enforcement needs justifying the delay. Nor was the delay necessary to determine the scope of the breach and restore the reasonable integrity of Accellion or the UC's electronic data systems.

151. Timely disclosure was necessary so that Plaintiffs 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.

152. As a result of Defendants' unreasonable delay of at least three months in notifying Plaintiffs and Class members of the Data Breach, they were deprived of an opportunity to take timely and appropriate self-protective measures, such as requesting a credit freeze. In addition, as a result of the delay, Plaintiffs and Class members have suffered (and will continue to suffer) economic damages and other injuries and actual harm including, without limitation: (1) the compromise and theft of their personal information; (2) loss of the opportunity to control how their personal information is used; (3) diminution in the value and use of their personal 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; (4) out-of-pocket costs associated with the prevention and detection of, and recovery from, identity theft and misuse of their personal information; (5) continued undue risk to their personal 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 personal information being stolen in the Data Breach.

153. Therefore, on behalf of the Class, Plaintiffs seek actual damages under Civil Code section 1798.84(b), injunctive and declaratory relief, and any other relief deemed appropriate by the Court.

FOURTH CAUSE OF ACTION
Violation of the Information Practices Act,
Civ. Code § 1798.1, *et seq.* (IPA)
(Against UC Regents)

154. Plaintiffs incorporate and reallege the foregoing allegations of fact.

155. Plaintiffs and Class members are "individuals" under Civil Code section 1798.3(d).

156. UC Regents is an "agency" as defined under Civil Code section 1798.3(b).

157. PII stolen in the Data Breach such as full names, addresses, telephone numbers, Social Security numbers, birthdates, driver's license information, financial information, and medical information, as well as other information, constitutes "personal information" under section 1798.3(a) of the Civil Code. UC Regents disclosed this personal information in violation of Civil Code section 1798.24 by failing to adequately secure and maintain it, thereby allowing unauthorized third parties to access and obtain it.

158. In violation of Civil Code section 1798.21, UC Regents failed to establish appropriate and reasonable safeguards to ensure the security and confidentiality of Plaintiffs' and Class members' personal information, and to protect against anticipated threats or hazards to such information.

159. In violation of Civil Code section 1798.29, UC Regents unreasonably delayed in disclosing the Data Breach to Plaintiffs and Class members. The UC system was aware of the Data Breach by no later than December 2020, but did not announce it until March 31, 2021—after some UC community members began receiving messages threatening to release their personal data. There were no legitimate law enforcement needs justifying the delay. Nor was the delay necessary to determine the scope of the breach and restore the reasonable integrity of Accellion or the UC's data system.

160. Civil Code section 1798.45 permits Plaintiffs to bring a civil action against UC Regents for violating the IPA. The UC system's failure to adhere to the requirements of the IPA has adversely affected Plaintiffs' and Class members' interests, including by denying them an opportunity to take timely and appropriate protective measures in response to the Data Breach, such as requesting a credit freeze. In addition, as a result of the delay, Plaintiffs and Class members have suffered (and will continue to suffer) economic damages and other injuries and actual harm including, without limitation: (1) the compromise and theft of their personal information; (2) loss of the opportunity to control how their personal information is used; (3) diminution in the value and use of their personal 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; (4) out-of-pocket costs associated with the prevention

and detection of, and recovery from, identity theft and misuse of their personal information; (5) continued undue risk to their personal 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 personal information being stolen in the Data Breach.

161. Accordingly, Plaintiffs and Class members are entitled to actual damages from UC Regents under Civil Code sections 1795 and 1798.48 in an amount to be determined at trial, as well as injunctive and declaratory relief, reasonable attorneys' fees and costs, and any other relief deemed appropriate by the Court.

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

162. Plaintiffs incorporate and reallege the foregoing allegations of fact.

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

164. Accellion's conduct is unlawful, in violation of the UCL, because it violates the CMIA.

165. Accellion's conduct is fraudulent because it omitted, suppressed, and concealed material facts regarding its failure to take reasonable or adequate precautions to secure Plaintiffs' and Class members' personal information. Despite being aware of vulnerabilities in the FTA system and that its systems had suffered a massive cyberattack—which Plaintiffs and Class members had no reasonable means of knowing—Accellion did not disclose this information to Plaintiffs or Class members.

166. Accellion's conduct also is unfair and deceptive in violation of the UCL. Accellion's unfair and fraudulent business acts and practices include:

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

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

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

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

167. The gravity of harm resulting from Accellion's 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.

168. The harm from Accellion's conduct was not reasonably avoidable by consumers. The individuals 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. Plaintiffs 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.

169. There were reasonably available alternatives that would have furthered Accellion's 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.

170. Accellion's 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 Plaintiffs' and Class members' personal information. A reasonable person would regard Accellion's derelict data security and the Data Breach as important, material facts. Accellion could and should have timely disclosed these facts.

171. As a direct and proximate result of Accellion's unfair methods of competition and unfair or deceptive acts or practices, Plaintiffs lost money or property because their sensitive personal information experienced a diminution of value and because they devoted additional time—which they otherwise would or could have devoted to pecuniary gain—to monitoring their credit reports and financial accounts for fraudulent activity.

172. Plaintiffs 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.

SIXTH CAUSE OF ACTION
Negligence
(Against All Defendants)

173. Plaintiffs incorporate and reallege the foregoing allegations of fact.

174. Defendants collected and stored Plaintiffs' and Class members' personal information, including their names, addresses, telephone numbers, birthdates, Social Security numbers and bank account information.

175. Defendants owed Plaintiffs 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 Plaintiffs and the Class from unauthorized access and use.

176. Defendants' duties also arise by operation of statute. The Customer Records Act, Cal. Civ. Code § 1798.80 *et seq*., imposes a mandatory duty on UC Regents and Accellion to implement and maintain reasonable security procedures and practices to safeguard and protect against the unauthorized disclosure of personal information. The Information Practices Act, Civ. Code § 1798.1 *et seq.*, imposes a mandatory duty on UC Regents "to ensure the security and confidentiality of records, and to protect against anticipated threats or hazards to their security or integrity which could result in any injury."

177. Plaintiffs and Class members were the foreseeable victims of Defendants' inadequate and ineffectual cybersecurity. The natural and probable consequence of Defendants' failing to adequately secure their information networks was Plaintiffs' and Class members' personal information being hacked.

178. Defendants knew or should have known that Plaintiffs' 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, and even within the University of California system. Moreover, the harm to Plaintiffs and Class members from exposure of their highly confidential personal facts was reasonably foreseeable to Defendants.

179. 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.

180. Defendants breached their duty to exercise reasonable care in protecting Plaintiffs' and Class members' personal information by failing to implement and maintain adequate security measures to safeguard Plaintiffs' and Class members' personal information, failing to monitor their systems to identify suspicious activity, and allowing unauthorized access to, and exfiltration of, Plaintiffs' and Class members' confidential personal information. Accellion knew that its FTA system was outdated but took no action to ensure that its customers stopped using it to transfer highly sensitive personal information. UC Regents disregarded warnings concerning Accellion's FTA system.

181. Defendants also owed a duty to timely disclose to Plaintiffs and Class members that their personal information had been or was reasonably believed to have been compromised. Timely disclosure was necessary so that Plaintiffs 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.

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

183. There is a close connection between Defendants' failure to employ reasonable security protections for its employees' personal information and the injuries suffered by Plaintiffs and Class members. When individuals' sensitive personal information is stolen, they face a heightened risk of identity theft and may 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.

184. Defendants were in a special relationship with Plaintiffs and Class members with respect to the hacked information because the end and aim of Defendants' data security measures was to benefit Plaintiffs and Class members by ensuring that their personal information would remain protected and secure. Only Defendants were in a position to ensure that their systems were sufficiently secure to protect Plaintiffs' and Class members' personal and medical information. The harm to Plaintiffs and Class members from its exposure was highly foreseeable to Defendants.

185. The policy of preventing future harm disfavors application of the economic loss rule, particularly given the sensitivity of the private information entrusted to Defendants. A high degree of opprobrium attaches to Defendants' failure to secure Plaintiffs' and class members' personal and extremely confidential facts. Defendants had an independent duty in tort to protect this information and thereby avoid reasonably foreseeable harm to Plaintiffs and class members.

186. UC employees are liable for their acts and omissions "to the same extent as a private person." Gov. Code § 820(a). UC Regents, as a public entity, is vicariously liable for the negligence of its employees occurring within the scope of their employment. Gov. Code §

815.2(a). UC employees, including information technology executives and specialists, were negligent in carrying out the day-to-day operations required to adequately secure Plaintiffs' and Class members' personal information from disclosure to unauthorized third parties or for improper purposes. Although the UC system recognized the importance of safeguarding personal information, UC employees, including information technology executives and specialists, failed to adequately carry out and implement its data security programs and failed to migrate the outdated Accellion FTA to kiteworks or another more secure platform, among other injurious acts and omissions.

187. As a result of Defendants' negligence, Plaintiffs 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.

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

188. Plaintiffs incorporate and reallege the foregoing allegations of fact.

189. Defendants wrongfully intruded upon Plaintiffs' and Class members' seclusion in violation of California law. Plaintiffs 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.

190. Defendants unlawfully invaded Plaintiffs' 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.

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

192. In failing to adequately protect Plaintiffs' 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 these 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 Plaintiffs' position.

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for an order:

A. Certifying this case as a class action, appointing Plaintiffs as Class representatives, and appointing Plaintiffs' counsel to represent the Class;

B. Entering judgment for Plaintiffs and the Class;

C. Awarding Plaintiffs and Class members monetary relief, including nominal damages;

D. Ordering appropriate injunctive or other equitable relief;

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

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

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

JURY TRIAL DEMANDED

Plaintiffs hereby demand a trial by jury on all issues so triable.

Dated: October 7, 2021

Respectfully submitted,

By: /s/ *Simon Grille*

Simon Grille (State Bar No. 294914)
Jordan Elias (State Bar No. 228731)
Adam E. Polk (State Bar No. 273000)
Trevor T. Tan (State Bar No. 281045)
GIRARD SHARP LLP
601 California Street, Suite 1400
San Francisco, CA 94108
Telephone: (415) 981-4800
Facsimile: (415) 981-4846
sgrille@girardsharp.com
jelias@girardsharp.com
apolk@girardsharp.com
ttan@girardsharp.com

WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP
BETSY C. MANIFOLD (182450)
manifold@whafh.com
RACHELE R. BYRD (190634)
byrd@whafh.com

MARISA C. LIVESAY (223247)
livesay@whafh.com
750 B Street, Suite 1820
San Diego, CA 92101
Telephone: 619/239-4599
Facsimile: 619/234-4599
Attorneys for Plaintiffs

MORGAN & MORGAN
John A. Yanchunis (*pro hac* motion pending)
Ryan Maxey (*pro hac* motion pending)
201 North Franklin Street, 7th Floor
Tampa, FL 33602
813-275-5272
jyanchunis@forthepeople.com
rmaxey@forthepeople.com

CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
M. ANDERSON BERRY (SBN 262879)
aberry@justice4you.com
GREGORY HAROUTUNIAN (SBN 330263)
gharoutunian@justice4you.com
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829

Jeff Westerman (SBN 94559)
WESTERMAN LAW CORP.
16133 Ventura Boulevard #685
Encino, CA 91436
310-698-7450
jwesterman@jswlegal.com

Attorneys for Plaintiffs and the Proposed Class

PROOF OF SERVICE

I, Anne von Goetz, hereby declare as follows:

On October 7, 2021, I caused the following to be filed served *via electronic mail*:

- **CONSOLIDATED CLASS ACTION COMPLAINT**

On:

Jacob M. Heath
ORRICK, HERRINGTON & SUTCLIFFE LLP
1000 Marsh Road
Menlo Park, CA 94025-1015
Telephone: (650) 614-7400
Facsimile: (650) 614-7401
Email: jheath@orrick.com

Thomas Fu
ORRICK, HERRINGTON & SUTCLIFFE LLP
777 South Figueroa Street
Suite 3200
Los Angeles, CA 90017-5855
Telephone: (213) 629-2020
Facsimile: (213) 612 2499
Email: tfu@orrick.com

Attorneys for Defendant The Regents of the University of California

Michael H. Rubin
Melanie M. Blunschi
LATHAM & WATKINS LLP
505 Montgomery Street, Suite 2000
San Francisco, California 94111-6538
Telephone: (415) 391-0600
Facsimile: (415) 395-8095
michael.rubin@lw.com
melanie.blunschi@lw.com

Attorneys for Defendant Accellion, Inc.

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct. Executed on October 7, 2021, at San Ramon, California.