TINA WOLFSON (SBN 174806)
*twolfson@ahdootwolfson.com*
ROBERT AHDOOT (SBN 172098)
*rahdoot@ahdootwolfson.com*
**AHDOOT& WOLFSON, PC**
2600 W. Olive Avenue, Suite 500
Burbank, CA 91505-4521
Telephone: 310.474.9111
Facsimile: 310.474.8585

Andrew W. Ferich (*pro hac vice* to be filed)
*aferich@ahdootwolfson.com*
**AHDOOT & WOLFSON, PC**
201 King of Prussia Road, Suite 650
Radnor, PA 19087
Telephone: 310.474.9111
Facsimile: 310.474.8585

Timothy G. Blood (SBN 149343)
*tblood@bholaw.com*
Paula R. Brown (SBN 254142)
*pbrown@bholaw.com*
Jennifer L. MacPherson (SBN 202021)
*jmacpherson@bholaw.com*
**BLOOD HURST & O'REARDON, LLP**
501 West Broadway, Suite 1490
San Diego, CA 92101
Telephone: 619.338.1100
Facsimile: 619.338.1101

Laurence D. King (SBN 206423)
*lking@kaplanfox.com*
Matthew B. George (SBN 239322)
*mgeorge@kaplanfox.com*
**KAPLAN FOX & KILSHEIMER LLP**
1999 Harrison Street, Suite 1560
Oakland, CA 94612
Telephone: 415.772.4700
Facsimile: 415.772.4707

*Attorneys for Plaintiffs and the Proposed Class*

**UNITED STATES DISTRICT COURT**

**NORTHERN DISTRICT OF CALIFORNIA – SAN JOSE DIVISION**

JOHN HARBOUR and TAMI WISNESKY, JOWELI VUNISA, and J. DOE, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

CALIFORNIA HEALTH & WELLNESS PLAN, HEALTH NET OF CALIFORNIA, INC., HEALTH NET LIFE INSURANCE COMPANY, CENTENE CORPORATION, HEALTH NET COMMUNITY SOLUTIONS, INC., HEALTH NET LLC, and ACCELLION, INC.

Defendants.

Case No. 5:21-cv-03322-EJD

Hon. Edward J. Davila

**FIRST AMENDED CLASS ACTION COMPLAINT**

**JURY TRIAL DEMANDED**

Complaint Filed May 4, 2021

Plaintiffs John Harbour, Tami Wisnesky, Joweli Vunisa, and J. Doe ("Plaintiffs"), individually and on behalf of all others similarly situated, upon personal knowledge of facts pertaining to themselves and on information and belief as to all other matters, by and through undersigned counsel, bring this First Amended Class Action Complaint against Defendants California Health and Wellness Plan ("CHW"), Health Net of California, Inc., Health Net Life Insurance Company, Health Net Community Solutions, Inc., Centene Corporation, and Health Net LCC (collectively, "Health Net" or "Health Net Defendants") (together with CHW, "Health Defendants"); and Accellion, Inc. ("Accellion") (altogether, "Defendants").

## NATURE OF THE ACTION

1. Plaintiffs bring this class action on behalf of themselves and all other individuals ("Class Members") who had their sensitive personal information—including but not limited to names, email addresses, phone numbers, home addresses, dates of birth, and for some individuals, Social Security numbers (SSN), bank account and routing information, and other personally identifying information (collectively, "PII"), as well as information used to process health insurance claims, prescription information, medical records and data, and other sensitive personal health information (collectively, "PHI")—disclosed to unauthorized third parties during a massive breach of Accellion's File Transfer Appliance software (the "Data Breach").

2. Accellion made headlines in late 2020/early 2021 (and continues to receive a raft of negative publicity) following its December 23, 2020 disclosure to numerous clients that criminals breached Accellion's client-submitted data via a vulnerability in its represented "secure" file transfer application.[1]

3. Accellion is a software company that provides third-party file transfer services to clients. Accellion makes and sells a file transfer service product called the File Transfer Appliance ("FTA"). Accellion's FTA is a 20-year-old, obsolete, "legacy product" that was "nearing end-of-life"[2] at the time of the Data Breach, thus leaving it vulnerable to compromise and security incidents.

[1] Lucas Ropek, *The Accellion Data Breach Seems to Be Getting Bigger,* GIZMODO (Feb. 11, 2021, 8:47 P.M.), https://gizmodo.com/the-accellion-data-breach-seems-to-be-getting-bigger-1846250357 (last visited Nov. 22, 2021).

[2] ACCELLION, *Accellion Provides Update to Recent FTA Security Incident* (Feb. 1, 2021),

4. During the Data Breach, unauthorized persons gained access to Accellion's clients' files by exploiting a vulnerability in Accellion's FTA platform.

5. Health Net is a nationwide healthcare conglomerate that provides insurance through HMO and PPO plans to patients, including through subsidiaries Health Net of California, Inc., Health Net Life Insurance Company, Health Net Community Solutions, Inc. On January 25, 2021, Health Net was notified by Accellion of the Data Breach and that certain Health Net files were accessed.

6. Health Net only began advising customers of its Data Breach two months after the fact, on or about March 24, 2021. Health Net disclosed the Data Breach on its website,[3] identifying that Accellion informed Health Net of the Data Breach; that the "hacker was able to get access to Accellion's system"; and that "[t]he hacker was able to view or save Health Net's files stored by Accellion." Health Net informed victims that their "personal information was included in the files that were on Accellion's system" which "happened between January 7 and January 25, 2021" and "may have included [victims'] name and one or more of the following: Address; Date of birth; Insurance ID Number; Health information, such as your medical condition(s) and treatment information."

7. CHW is a sister company to Health Net, both of which are owned by Centene Corporation. CHW is a Managed Care Organization that provides coordinated health care, pharmacy, vision and transportation services to members.

8. Similarly, CHW began advising customers of its Data Breach at the same time as Health Net, approximately two months after the Data Breach, on or about March 24, 2021. CHW disclosed the Data Breach on its website,[4] identifying that Accellion informed CHW of the Data Breach; that the "hacker was able to get access to Accellion's system"; and that "[t]he hacker was

---

https://www.accellion.com/company/press-releases/accellion-provides-update-to-recent-fta-security-incident/ (last visited Nov. 22, 2021).

[3] HEALTH NET, *News*, *Health Net received information that one of our business partners was a victim of a cyber-attack* (Mar. 24, 2021), https://www.healthnet.com/content/healthnet/en_us/news-center/news-releases/cyber-accellion.html (last visited Nov. 22, 2021).

[4] CALIFORNIA HEALTH & WELLNESS, *News, California Health & Wellness received information that one of our business partners was a victim of a cyber-attack* (Mar. 24, 2021) https://www.cahealthwellness.com/newsroom/cyber-accellion.html (last visited Nov. 22, 2021).

able to view or save CHW's files stored by Accellion." CHW informed victims that their "personal information was included in the files that were on Accellion's system" which "happened between January 7 and January 25, 2021" and "may have included [victims'] name and one or more of the following: Address; Date of birth; Insurance ID Number; Health information, such as your medical condition(s) and treatment information."

9. According to early reports, 1,236,902 patients and customers of Health Net—686,556 customers of Health Net Community Solutions, 523,709 customers of Health Net of California, and 26,637 customers of Health Net Life Insurance Company—and 80,138 customers of CHW, for a total of approximately 1.3 million people (just with respect to Health Defendants alone), are reported to have had their PII and PHI impacted and exposed during the Data Breach.[5]

10. Since the time of the breach, it has been confirmed that the number of impacted Class members is 1,506,868 individuals.

11. At the time of the Data Breach, Health Defendants, along with reportedly hundreds of others, were clients of Accellion. Accellion's services to Health Defendants, and other customers, included the use of Accellion's outdated and vulnerable FTA platform for large file transfers. The PHI and PII of Defendants, as well as millions of other class members who are clients or affiliated with other Accellion clients impacted by the Data Breach ("Impacted Accellion Clients"), was accessed by and disclosed to criminals without authorization because who were able to exploit vulnerabilities in Accellion's FTA product.

12. Defendants were well aware of the data security shortcomings in Accellion's FTA product. Nevertheless, Defendants continued to use FTA, putting millions at risk of being impacted by a breach.

13. Defendants' failures to ensure that Accellion's file transfer services and products were adequately secure fell far short of their obligations and Plaintiffs' and class members'

[5] Jessica Davis, *Accellion Breach Tally for Centene's Subsidiaries: 1.3M Patients Impacted,* HEALTH IT SECURITY (Apr. 6, 2021), https://healthitsecurity.com/news/accellion-breach-tally-for-centenes-subsidiaries-1.3m-patients-impacted (last visited Nov. 22, 2021).

reasonable expectations for data privacy, jeopardized the security of Plaintiffs' and class members' PHI and PII, and put Plaintiffs and class members at serious risk of fraud and identity theft.

14. As a result of Defendants' conduct and the resulting Data Breach, Plaintiffs' and millions of class members' privacy has been invaded, their PII and PHI is now in the hands of criminals, and they face a substantially increased risk of identity theft and fraud. Accordingly, these individuals now must take immediate and time-consuming action to protect themselves from such identity theft and fraud.

**PARTIES**

15. Plaintiff John Harbour is a citizen of the state of California and resides in Chico, California. Believing CHW would implement and maintain reasonable security and practices to protect his PII and PHI, Mr. Harbour provided this information to CHW. On or about March 24, 2021, CHW sent Plaintiff Harbour, and Plaintiff Harbour received, a letter confirming that his PII and PHI was impacted by the Data Breach. In the letter, CHW identified that the nature of the information involved includes "your name and one or more of the following types of information: Address, Date of birth, Insurance ID Number, [and] Health information, such as your medical condition(s) and treatment information . . . ." Mr. Harbour has spent over eight hours monitoring his accounts and changing passwords to try and protect his accounts.

16. Plaintiff Tami Wisnesky is a citizen of the state of California and resides in Westchester, California. Believing Health Net would implement and maintain reasonable security and practices to protect her PII and PHI, Ms. Wisnesky provided this information to Health Net. On or about March 24, 2021, Health Net sent Plaintiff Wisnesky, and Plaintiff Wisnesky received, a letter confirming that her PII and PHI was impacted by the Data Breach. In the letter, Health Net identified that the nature of the information involved includes "your name and one or more of the following types of information: Address, Date of birth, Insurance ID Number, [and] Health information, such as your medical condition(s) and treatment information . . . ." On or about January 12, 2021, Plaintiff Wisnesky suffered a fraudulent charge of approximately $303 on prepaid card account. On January 13, 2021, she suffered another $303 fraudulent charge. Plaintiff disputed both charges, but the prepaid card company would not refund these charges. As a result of the Data

Breach, Ms. Wisnesky has suffered out of pocket harm, and has also spent many hours across numerous days monitoring her accounts in an attempt to try to protect her accounts and the privacy of her data.

17. Plaintiff Joweli Vunisa, is a citizen of California and resides in Sacramento, California. Believing CHW would implement and maintain reasonable security and practices to protect his PII and PHI, Mr. Vunisa provided this information to CHW. On or about March 24, 2021, CHW sent Plaintiff Vunisa, and Plaintiff Vunisa received, a letter confirming that his PII and PHI was impacted by the Data Breach. In the letter, CHW identified that the nature of the information involved includes "your name and one or more of the following types of information: Address, Date of birth, Insurance ID Number, [and] Health information, such as your medical condition(s) and treatment information . . . ." As a result of the Data Breach, Mr. Vunisa has suffered out of pocket harm, and has also spent time monitoring his accounts in an attempt to try to protect his accounts and the privacy of her data.

18. Plaintiff J. Doe is a citizen of California and resides in San Francisco, California. Believing CHW would implement and maintain reasonable security and practices to protect their PII and PHI, Plaintiff Doe provided this information to CHW. On or about March 24, 2021, CHW sent Plaintiff Doe, and Plaintiff Doe received, a letter confirming that their PII and PHI was impacted by the Data Breach. In the letter, CHW identified that the nature of the information involved includes "your name and one or more of the following types of information: Address, Date of birth, Insurance ID Number, [and] Health information, such as your medical condition(s) and treatment information . . . ." As a result of the Data Breach, Plaintiff Doe has suffered out of pocket harm, and has also spent time monitoring their accounts in an attempt to try to protect their accounts and the privacy of their data.

19. Defendant California Health & Wellness Plan is, on information and belief, a California corporation, with principal places of business located in Sacramento, California and St. Louis, Missouri. CHW is a wholly-owned subsidiary of Centene Corporation. Per its website, it is a Managed Care Organization and sister company to Health Net, LLC. It provides coordinated health care, pharmacy, vision and transportation services to its members.

20. Defendant Health Net, LLC, a sister organization to CHW, is a Delaware corporation, with its headquarters in Woodland Hills, California, and St. Louis, Missouri. Health Net, LLC is the parent corporation of Health Net of California, Inc., Health Net Life Insurance Company, and Health Net Community Solutions, Inc. Health Net LLC is also a subsidiary of Centene Corporation. Per its website, Health Net provides health plans for individuals, families, and businesses. The company offers access to substance abuse programs, behavioral health services, employee assistance programs and managed health care products related to prescription drugs, with many services available through its subsidiaries, including Health Net Community Solutions, Health Net of California, Inc., and Health Net Life Insurance Company. Health Net LLC is a Fortune 50 company with 3,000 employees and 85,000 providers, and it provides health coverage to more than 20 million Americans, including service to 3 million people in California.

21. Defendant Health Net of California, Inc., is a California corporation with its principal place of business in Woodland Hills, California. Health Net of California, Inc. is a subsidiary of Health Net, LLC.

22. Defendant Health Net Life Insurance Company is a California corporation with its principal place of business in St. Louis Missouri. Health Net Life Insurance Company is a subsidiary of Health Net, LLC.

23. Defendant Health Net Community Solutions, Inc. is a California corporation with its principal place of business in Woodland Hills, California. Health Net Community Solutions, Inc. is a subsidiary of Health Net, LLC.

24. Defendant Centene Corporation is a Delaware corporation, with headquarters in St. Louis, Missouri. Centene is a multi-national healthcare enterprise that provides programs and services to government sponsored healthcare programs, focusing on under-insured and uninsured individuals. Centene operates in two segments, namely managed care and specialty services. In March 2016, Centene acquired Health Net.

25. Defendant Accellion Inc. is a Delaware corporation with corporate headquarters located at 1804 Embarcadero Road, Suite 200, Palo Alto, California 94303.

## JURISDICTION AND VENUE

26. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(a) and (d), because the matter in controversy, exclusive of interest and costs, exceeds the sum or value of five million dollars ($5,000,000.00) and is a class action in which one or more Class Members are citizens of states different from Defendants.

27. The Court has personal jurisdiction over Defendants because Defendants have principal offices in California, conduct significant business in California, and/or otherwise have sufficient minimum contacts with and intentionally avail themselves of the markets in California.

28. Venue properly lies in this district because, *inter alia,* Defendants have principal places of business in this district; transact substantial business, have agents, and are otherwise located in this district; and/or a substantial part of the conduct giving rise to Plaintiffs' claims occurred in this judicial district.

## FACTUAL ALLEGATIONS

### A. Accellion and Its Unsecure File Transfer Platform, FTA

29. Accellion is a Palo Alto-based software company that makes, markets, and sells file transfer platforms and services.

30. Accellion touts its products and services as "prevent[ing] data breaches"[6] and as being secure. On its website, Accellion states:

> The Accellion enterprise content firewall *prevents data breaches and compliance violations from third party cyber risk*. CIOs and CISOs *rely on the Accellion platform for complete visibility, security and control* over . . . *sensitive content* across email, file sharing, mobile, enterprise apps, web portals, SFTP, and automated inter-business workflows.[7]

31. Accellion also touts its commitment to data privacy, claiming that "[d]ata privacy is a fundamental aspect of the business of Accellion . . . ."[8]

---

[6] ACCELLION, *About Accellion,* https://www.accellion.com/company/ (last visited Nov. 22 2021).
[7] *Id.* (emphasis added).
[8] ACCELLION, *Accellion Privacy Policy*, https://www.accellion.com/privacy-policy/ (last visited May 3, 2021).

32. Accellion markets its products and services as capable of safely transferring sensitive Personal Information through file sharing, claiming that "[w]hen employees click the Accellion button, they know it's the *safe*, *secure* way to share sensitive information. . . ."[9]

33. Despite these assurances and claims, Accellion failed to offer safe and secure file transfer products and services and failed to adequately protect Plaintiffs' and class members' PHI and PII entrusted to it by Accellion's clients, including CHW and Health Net.

34. Accellion's FTA product, which the Health Defendants and certain of Accellion's other clients used, was not secure and, by Accellion's own acknowledgment, outdated.

35. The FTA is Accellion's twenty-year-old "legacy" file transfer software, which purportedly is designed and sold for large file transfers.[10]

36. Accellion's FTA is an obsolete "legacy product" that was "nearing end-of-life,"[11] thus leaving it vulnerable to compromise and security incidents. Accellion acknowledged that the FTA program is insufficient to keep file transfer processes secure "in today's breach-filled, over-regulated world" where "you need even broad protection and control."[12] On the page dedicated to Accellion FTA, Accellion's website states: "End-of-Life Announced for FTA. No Renewals After April 30, 2021."[13]

37. Key people within Accellion have acknowledged the need to leave the FTA platform behind due to the security concerns raised by it. Accellion's Chief Marketing Officer Joel York confirmed that Accellion is encouraging its clients to discontinue use of FTA because it does not protect against modern data breaches: "It just wasn't designed for these types of threats . . . ."[14]

---

[9] ACCELLION, *About Accellion*, https://www.accellion.com/company/ (last visited Nov. 22, 2021) (emphasis added).

[10] ACCELLION, *Accellion Responds to Recent FTA Security Incident* (Jan. 12, 2021), https://www.accellion.com/company/press-releases/accellion-responds-to-recent-fta-security-incident/ (last visited Nov. 22, 2021).

[11] ACCELLION, *Press Release, Accellion Provides Update to Recent FTA Security Incident* (Feb. 1, 2021), https://www.accellion.com/company/press-releases/accellion-provides-update-to-recent-fta-security-incident/ (last visited Nov. 22, 2021).

[12] ACCELLION, *Accellion FTA*, https://www.accellion.com/products/fta/ (last visited Nov. 22, 2021).

[13] *Id.*

[14] Jim Brunner & Paul Roberts, *Banking, Social Security info of more than 1.4 million people exposed in hack involving Washington State Auditor*, SEATTLE TIMES (Feb. 3, 2021, 4:57 P.M.), https://www.seattletimes.com/seattle-news/politics/personal-data-of-1-6-million-washington-unemployment-claimants-exposed-in-hack-of-state-auditor/ (last visited Nov. 22, 2021).

38. Accellion's Chief Information Security Officer Frank Balonis stated: "Future exploits of [FTA] . . . are a constant threat. We have encouraged all FTA customers to migrate to kiteworks for the last three years and have accelerated our FTA end-of-life plans in light of these attacks. We remain committed to assisting our FTA customers, but strongly urge them to migrate to kiteworks as soon as possible."[15]

39. Despite knowing that FTA left Accellion's customers (like the Health Defendants) and third parties interacting and transacting with its customers (like Plaintiffs and class members) exposed to security threats, Accellion continued to offer, and Health Defendants continued to utilize, the FTA file transfer product at the time of the Data Breach.

**B. The Data Breach**

40. On December 23, 2020, the inevitable happened: Accellion confirmed to numerous clients that it experienced a massive security breach whereby criminals were able to gain access to sensitive client data via a vulnerability in its FTA platform.[16]

41. According to reports, the criminals exploited as many as four vulnerabilities in Accellion's FTA to steal sensitive data files associated with hundreds of Accellion's clients, including corporations, law firms, banks, universities, and other entities.

42. With respect to how Accellion's FTA was compromised, one report indicates:

> The adversary exploited [the FTA's] vulnerabilities to install a hitherto unseen Web shell named DEWMODE on the Accellion FTA app and used it to exfiltrate data from victim networks. Mandiant's telemetry shows that DEWMODE is designed to extract a list of available files and associated metadata from a MySQL database on Accellion's FTA and then download files from that list via the Web shell. Once the downloads complete, the attackers then execute a clean-up routine to erase traces of their activity.[17]

---

[15] ACCELLION, *Press Release, Accellion Provides Update to Recent FTA Security Incident* (Feb. 1, 2021), https://www.accellion.com/company/press-releases/accellion-provides-update-to-recent-fta-security-incident/ (last visited Nov. 22, 2021).

[16] Lucas Ropek, *The Accellion Data Breach Seems to Be Getting Bigger,* GIZMODO (Feb. 11, 2021, 8:47 P.M.), https://gizmodo.com/the-accellion-data-breach-seems-to-be-getting-bigger-1846250357 (last visited Nov. 22, 2021).

[17] Jai Vljayan, *Accellion Data Breach Resulted in Extortion Attempts Against Multiple Victims*, DARKREADING (Feb. 22, 2021, 4:50 P.M.), https://www.darkreading.com/attacks-breaches/accellion-data-breach-resulted-in-extortion-attempts-against-multiple-victims/d/d-id/1340226 (last visited Nov. 22, 2021).

43. The criminals, reportedly associated with the well-known Clop ransomware gang, the FIN11 threat group, and potentially other threat actors, launched the attacks in mid-December 2020. The attacks continued from at least mid-December 2020 and into January 2021, as these actors continued to exploit vulnerabilities in the FTA platform. Following the attacks, the criminals resorted to extortion, threatening Accellion's clients, e.g., by email, with making the stolen information publicly available unless ransoms were paid.[18]

44. An example of a message sent by the criminals to a client of Accellion that was victimized during the breach is below[19]:

> Hello!
>
> Your network has been hacked, a lot of valuable data stolen. <description of stolen data, including the total size of the compressed files> We are the CLOP ransomware team, you can google news and articles about us. We have a website where we publish news and stolen files from companies that have refused to cooperate. Here is his address http://[redacted].onion/ - use TOR browser or http://[redacted].onion.dog/ - mirror. We are visited by 20-30 thousand journalists, IT experts, hackers and competitors every day. We suggest that you contact us via chat within 24 hours to discuss the current situation. <victim-specific negotiation URL> - use TOR browser We don't want to hurt, our goal is money. We are also ready to provide any evidence of the presence of files with us.

45. Accellion has remained in the headlines through the first half of 2021 (and continues to receive a raft of negative publicity) following its mid-December 2020 disclosure of the massive Data Breach. The list of groups and clients who used Accellion's unsecure FTA product and were impacted by the Data Breach continues to increase.

46. The list, to date, reportedly includes, among others:

- Allens
- American Bureau of Shipping ("ABS")
- Arizona Complete Health

[18] Ionut Ilascu, *Global Accellion data breaches linked to Clop ransomware gang,* BLEEPINGCOMPUTER (Feb. 22, 2021, 9:06 A.M.), https://www.bleepingcomputer.com/news/security/global-accellion-data-breaches-linked-to-clop-ransomware-gang/ (last visited Nov. 22, 2021).

[19] *Id.*

- The Australia Securities and Investments Commission
- Bombardier
- CSX
- Danaher
- Flagstar Bank
- Fugro
- Goodwin Proctor
- Harvard Business School
- Jones Day
- The Kroger Co.
- The Office of the Washington State Auditor
- QIMR Berghofer Medical Research Institute
- Qualys
- The Reserve Bank of New Zealand
- Shell
- Singtel
- Southern Illinois University School of Medicine
- Stanford University
- Steris
- Transport for New South Wales
- Trillium Community Health Plan
- University of California system
- University of Colorado
- University of Maryland, Baltimore
- University of Miami (Florida)
- Yeshiva University

### C. Health Net and CHW Announce They Were Impacted by the Data Breach

47. On or about March 24, 2021, Health Net publicly confirmed the following on its website[20]:

> ## Health Net received information that one of our business partners was a victim of a cyber-attack
>
> Date: 03/24/21
>
> Member Notice Letter
>
> Dear Member,
>
> On January 25, 2021, Health Net, LLC (Health Net) received information that one of our business partners was a victim of a cyber-attack. A cyber-attack means a hacker was able to steal data.
>
> Health Net works with Accellion. Health Net uses Accellion's system to exchange files with your health providers and others who help support our operations.
>
> ### What Happened
>
> The hacker was able to get access to Accellion's system. The hacker was able to view or save Health Net's files stored by Accellion. Your personal information was included in the files that were on Accellion's system.
>
> This happened between January 7 and January 25, 2021.
>
> ### What Information Was Involved
>
> Your information may have included your name and one or more of the following:
>
> - Address
> - Date of birth
> - Insurance ID Number
> - Health information, such as your medical condition(s) and treatment information

48. Separately, Health Net's sister company, CHW, provided a nearly identical notice on its website following the Data Breach[21]:

[20] HEALTH NET, *News, Health Net received information that one of our business partners was a victim of a cyber-attack* (Mar. 24, 2021), https://www.healthnet.com/content/healthnet/en_us/news-center/news-releases/cyber-accellion.html (last visited Nov. 22, 2021).

[21] CALIFORNIA HEALTH & WELLNESS, *News, California Health & Wellness received information that one of our business partners was a victim of a cyber-attack* (Mar. 24, 2021), https://www.cahealthwellness.com/newsroom/cyber-accellion.html (last visited Nov. 22, 2021).

## California Health & Wellness received information that one of our business partners was a victim of a cyber-attack

Date: 03/24/21

Member Notice Letter

Dear Member,

On January 25, 2021, California Health & Wellness (CHW) received information that one of our business partners was a victim of a cyber-attack. A cyber-attack means a hacker was able to steal data.

CHW works with Accellion. CHW uses Accellion's system to exchange files with your health providers and others who help support our operations.

### What Happened

The hacker was able to get access to Accellion's system. The hacker was able to view or save CHW's files stored by Accellion. Your personal information was included in the files that were on Accellion's system.

This happened between January 7 and January 25, 2021.

### What Information Was Involved

Your information may have included your name and one or more of the following:

- Address
- Date of birth
- Insurance ID Number
- Health information, such as your medical condition(s) and treatment information

49. Health Net and CHW each confirmed that they are working with the Federal Bureau of Investigations (FBI) regarding the Data Breach.

**D. Impact of the Data Breach**

50. The actual extent and scope of the impact of the Data Breach on sister companies Health Net and CHW remains uncertain.

51. Unfortunately for Plaintiffs and class members, the damage is already done. Criminals now possess their sensitive PII and PHI, and their only purpose is to monetize that data by selling it on the dark web or using it to commit fraud.

52. Health Defendants have known that the FTA software is unsecured and should no longer be used in connection with data transfers. Indeed, "[m]ultiple cybersecurity experts . . . highlight that Accellion FTA is a 20-year-old application designed to allow an enterprise to securely

transfer large files but it is nearing the end of life," and that "Accellion asked its customers late last year to switch over to a new product it offers called kiteworks."[22] On information and belief, Defendants all failed to make the switch to kiteworks and knowingly continued to use FTA, exposing class members' PII and PHI to the risk of theft, identity theft, and fraud.

53. The harm caused to Plaintiffs and class members by the Data Breach is already apparent. As identified herein, criminal hacker groups already are threatening Accellion's clients with demands for ransom payments to prevent sensitive PII and PHI from being disseminated publicly.

54. Even if companies that were impacted by the Accellion Data Breach pay these ransoms, there is no guarantee that the criminals making the ransom demands will suddenly act honorably and destroy the sensitive PHI and PII. In fact, there is no motivation for them to do so, given the burgeoning market for sensitive PII and PHI on the dark web.

55. The Data Breach was particularly damaging given the nature of Accellion's FTA. In the words of one industry expert: "[The] vulnerabilities [in Accellion's FTA] are particularly damaging, because in a normal case an attacker has to hunt to find your sensitive files, and it's a bit of a guessing game, but in this case the work is already done . . . By definition everything sent through Accellion was pre-identified as sensitive by a user."[23]

56. The Data Breach creates a heightened security concern for Plaintiffs and class members because SSNs and sensitive financial and health information were included. Theft of SSNs creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of her SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

---

[22] Jonathan Greig, *Kroger data breach highlights urgent need to replace legacy, end-of-life tools*, TECHREPUBLIC (Feb. 24, 2021, 6:17 A.M.), https://www.techrepublic.com/article/kroger-data-breach-highlights-urgent-need-to-replace-legacy-end-of-life-tools/ (last visited Nov. 22, 2021).

[23] Lily Hay Newman, *The Accellion Breach Keeps Getting Worse—and More Expensive*, WIRED.COM (Mar. 8, 2021, 7:00 A.M.), https://www.wired.com/story/accellion-breach-victims-extortion/ (last visited Nov. 22, 2021) (quoting Jake Williams, founder of the security firm Rendition Infosec).

57. Given the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. Per the United States Attorney General, Social Security numbers "can be an identity thief's most valuable piece of consumer information."[24]

58. Health Defendants had a duty to keep Plaintiffs' and other patients—and Accellion had a duty to keep all class members'— PHI and PII confidential and to protect it from unauthorized disclosures. Plaintiffs and class members provided their PII and PHI to Health Net, CHW, and other Impacted Accellion Clients with the understanding that those entities and any business partners to whom those entities disclosed PHI and PII (i.e., Accellion) would comply with their obligations to keep such information confidential and secure from unauthorized disclosures.

59. Defendants' data security obligations were particularly important given the substantial increase in data breaches—particularly those involving health information—in recent years, which are widely known to the public and to anyone in Accellion's industry of data collection and transfer.

60. Data breaches are by no means new, and they should not be unexpected. These types of attacks should be anticipated by companies that store sensitive and personally identifying information, and these companies must ensure that data privacy and security is adequate to protect against and prevent known attacks.

61. It is well known amongst companies that store sensitive personally identifying information that sensitive information—like the SSNs and medical information stolen in the Data Breach—is valuable and frequently targeted by criminals. In a recent article, *Business Insider* noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers . . . . Many of them were caused by flaws in . . . systems either online or in stores."[25]

---

[24] *Fact Sheet: The Work of the President's Identity Theft Task Force*, DEP'T OF JUSTICE, (Sept. 19, 2006), https://www.justice.gov/archive/opa/pr/2006/September/06_ag_636.html (last visited Nov. 22, 2021).

[25] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUSINESS INSIDER (Nov. 19, 2019, 8:05 A.M.), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1 (last visited Nov. 22, 2021).

62. Identity theft victims are frequently required to spend many hours and large amounts of money repairing the impact to their credit. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, tax fraud, phone or utilities fraud, and bank/finance fraud.

63. There may be a time lag between when sensitive personal information is stolen and when it is used. According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, *stolen data may be held for up to a year or more before being used to commit identity theft*. Further, once stolen data have been sold or posted on the Web, *fraudulent use of that information may continue for years*. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[26]

64. With access to an individual's PII, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and SSN to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[27]

65. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the dark web and the "cyber black-market" for years. As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen SSNs and other PII directly on various illegal websites making the information publicly available, often for a price.

66. A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[28] Indeed,

---

[26] *Id*. at 29 (emphasis added).

[27] *See* FEDERAL TRADE COMMISSION, WARNING SIGNS OF IDENTITY THEFT, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited May 3, 2021).

[28] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010, 5:00 A.M.), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims (last visited

data breaches and identity theft have a crippling effect on individuals and detrimentally impact the entire economy as a whole.

67. Medical information and other PHI is especially valuable to identity thieves. According to a 2012 Nationwide Insurance report, "[a] stolen medical identity has a $50 street value – whereas a stolen social security number, on the other hand, only sells for $1."[29] In fact, the medical industry has experienced disproportionally higher instances of computer theft than any other industry.

68. A recent study also concluded the value of information available on the dark web sufficient to commit identity theft or fraud is about $1,010 per identity. The study identified that "[a] full range of documents and account details allowing identity theft can be obtained for $1,010."[30]

69. Despite the known risk of data breaches and the widespread publicity and industry alerts regarding other notable (similar) data breaches, Defendants failed to take reasonable steps to adequately protect against the Data Breach and exposure of Plaintiffs' and class members' PII and PHI, and to properly phase out the unsecure FTA platform, leaving Accellion's clients and its clients' customers exposed to risk of fraud and identity theft.

70. Accellion is, and at all relevant times has been, aware that the PII and PHI it handles and stores in connection with providing its file transfer services is highly sensitive. As a company that provides file transfer services involving highly sensitive and personally identifying information, Accellion is aware of the importance of safeguarding that information and protecting its systems and products from security vulnerabilities.

71. Defendants were aware, or should have been aware, of regulatory and industry guidance regarding data security, and they were alerted to the risk associated with failing to ensure that Accellion's FTA was adequately secured, or phasing out the platform altogether.

---

Nov. 22, 2021).

[29] CLAIMS JOURNAL, *Study: Few Aware of Medical Identity Theft Risk*, (June 14, 2012), http://www.claimsjournal.com/news/national/2012/06/14/208510.htm (last visited May 3, 2021).

[30] CISON, *You Are Worth $1,010 on the Dark Web, New Study by PrivacyAffairs Finds* (Mar. 8, 2021, 5:15 ET), https://www.prnewswire.com/news-releases/you-are-worth-1-010-on-the-dark-web-new-study-by-privacyaffairs-finds-301241816.html (last visited Nov. 22, 2021).

72. Despite the well-known risks of hackers and cybersecurity intrusions, Defendants failed to employ adequate data security measures in connection with the Health Defendants' use of Accellion's FTA platform in a meaningful way in order to prevent breaches, including the Data Breach.

73. The security flaws inherent to Accellion's FTA file transfer platform—and continuing to market and sell a platform with known, unpatched security issues—run afoul of industry best practices and standards. Had Accellion adequately protected and secured FTA, or stopped supporting the product when it learned years ago about its vulnerabilities, it could have prevented the Data Breach.

74. Despite the fact that Accellion was on notice of the very real possibility of data theft associated with the FTA platform, it still failed to make necessary changes to the product or to stop offering and supporting it, and permitted a massive intrusion to occur that resulted in the FTA platform's disclosure of Plaintiffs' and class members' PII and PHI to criminals.

75. Defendants permitted the PHI and PII of Health Defendants' customers, and other class members, to be compromised and disclosed to criminals by failing to take reasonable steps against an obvious threat.

76. Industry experts are clear that a data breach is indicative of data security failures. Indeed, industry-leading research and advisory firm Aite Group has identified that: "If your data was stolen through a data breach that means you were somewhere out of compliance" with payment industry data security standards.[31]

77. As a result of the events detailed herein, Plaintiffs and class members suffered harm and loss of privacy, and will continue to suffer future harm, resulting from the Data Breach, including but not limited to: invasion of privacy; loss of privacy; loss of control over personal information and identities; fraud and identity theft; unreimbursed losses relating to fraud and identity theft; loss of value and loss of possession and privacy of PII and PHI; harm resulting from damaged

[31] Lisa Baertlein, *Chipotle Says Hackers Hit Most Restaurants in Data Breach*, REUTERS (May 26, 2017), http://www.reuters.com/article/us-chipotle-cyber-idUSKBN18M2BY (last visited Nov. 22, 2021).

credit scores and information; loss of time and money preparing for and resolving fraud and identity theft; loss of time and money obtaining protections against future identity theft; and other harm resulting from the unauthorized use or threat of unauthorized exposure of PII and PHI.

78. Victims of the Data Breach have likely already experienced harms, which is made clear by news of attempts to exploit this information for money by the hackers responsible for the breach.

79. As a result of Accellion's failure to ensure that its FTA product was protected and secured, or to phase out the platform upon learning of FTA's vulnerabilities, the Data Breach occurred. As a result of the Data Breach, and of all Defendants' failure to part ways with the unsecure FTA despite the known risks and vulnerabilities associated therewith, Plaintiffs' and class members' privacy has been invaded, their PII and PHI is now in the hands of criminals, they face a substantially increased risk of identity theft and fraud, and they must take immediate and time-consuming action to protect themselves from such identity theft and fraud.

## CLASS ALLEGATIONS

80. Plaintiffs brings this action on behalf of themselves and the following class:

> All residents of the United States who were notified by the Health Net Defendants that their PHI and PII may have been compromised as a result of the FTA Data Breach.

81. Excluded from the Class are: (1) the Judges presiding over the Action, Class Counsel, and members of their families; (2) the Health Net Defendants and Accellion, their subsidiaries, parent companies, successors, predecessors, and any entity in which the Health Net Defendants or Accellion or their parents, have a controlling interest, and their current or former officers and directors; (3) Persons who properly opt out; and (4) the successors or assigns of any such excluded Persons.

82. **Numerosity**: Members of the class are so numerous that their individual joinder is impracticable, as the proposed class includes 1,506,868 members who are geographically dispersed.

83. **Typicality**: Plaintiffs' claims are typical of class members' claims. Plaintiffs and all class members were injured through Defendants' uniform misconduct, and Plaintiffs' claims are

identical to the claims of the class members they seek to represent. Accordingly, Plaintiffs' claims are typical of class members' claims.

84. **Adequacy**: Plaintiffs' interests are aligned with the class they seek to represent and Plaintiffs have retained counsel with significant experience prosecuting complex class action cases, including cases involving alleged privacy and data security violations. Plaintiffs and their counsel intend to prosecute this action vigorously. The class's interests are well-represented by Plaintiffs and undersigned counsel.

85. **Superiority**: A class action is the superior—and only realistic—mechanism to fairly and efficiently adjudicate Plaintiffs' and other class member's claims. The injury suffered by each individual class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for class members individually to effectively redress Defendants' wrongdoing. Even if class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

86. **Commonality and Predominance:** The following questions common to all class members predominate over any potential questions affecting individual class members:

- whether Defendants engaged in the wrongful conduct alleged herein;
- whether Defendants' data security practices and the vulnerabilities of Accellion's FTA product resulted in the disclosure of Plaintiffs' and other Class members' PII and PHI;
- whether Defendants violated consumer protection and data privacy statutes, as alleged herein;
- whether Defendants violated privacy rights and invaded Plaintiffs' and class members' privacy; and

- whether Plaintiffs and class members are entitled to damages, equitable relief, or other relief and, if so, in what amount.

87. Given that Defendants engaged in a common course of conduct as to Plaintiffs and the class, similar or identical injuries and common law and statutory violations are involved, and common questions outweigh any potential individual questions.

## CAUSES OF ACTION

### COUNT I

### Negligence
### (Against All Defendants)

88. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

89. Accellion negligently sold its FTA product which it has acknowledged is vulnerable to security breaches, despite representing that the product could be used securely for large file transfers.

90. Health Defendants negligently utilized the FTA, which was known to be a vulnerable, legacy or "end-of-life" product that was unsuited for secure file transfers.

91. Defendants were entrusted with, stored, and otherwise had access to the PHI and PII of Plaintiffs and class members.

92. Defendants knew, or should have known, of the risks inherent to storing the PHI and PII of Plaintiffs and class members, and to not ensuring that the FTA product was secure. These risks were reasonably foreseeable to Defendants, because Accellion had previously recognized and acknowledged the data security concerns with its FTA product.

93. Defendants owed duties of care to Plaintiffs and class members whose PHI and PII had been entrusted to Defendants.

94. Defendants breached those duties by failing to provide fair, reasonable, or adequate data security in connection with the use of Accellion's FTA product for file transfers. Defendants had a duty to safeguard Plaintiffs' and class members' PHI and PII and to ensure that its systems and products adequately protected that information. Defendants breached this duty.

95. Health Defendants' duty of care arises from their knowledge that customers entrust them with highly sensitive PII and PHI that they are intended to, and represent that they will, handle securely.

96. Accellion's duty of care arises from its knowledge that its customers, like Health Net, CHW, and others, entrust to it highly sensitive PII and PHI that Accellion is intended to, and represents that it will, handle securely. Only Defendants were in a position to ensure that the systems and products they use for file transfers are sufficient to protect against breaches that exploited the FTA product and the harms that Plaintiffs and class members have now suffered.

97. A "special relationship" exists between Defendants, on the one hand, and Plaintiffs and class members, on the other hand. Defendants entered into a "special relationship" with Plaintiffs and class members by agreeing to accept, store, and have access to sensitive PII and PHI provided by Plaintiffs and class members.

98. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiffs and class members, Plaintiffs and class members would not have been injured.

99. Defendants acted with wanton disregard for the security of Plaintiffs' and class members' PII and PHI, especially in light of the fact that for a long period of time, Accellion warned of, and Health Defendants (and other Accellion customers) know of, the data security concerns relating to the FTA.

100. The injury and harm suffered by Plaintiffs and class members was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known they were failing to meet their duties, and that Defendants' breach would cause Plaintiffs and class members to experience the foreseeable harms associated with the exposure of their PII and PHI.

101. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and class members have suffered actual harm and now face an increased risk of future harm, resulting from fraud or other misuses of their PII and PHI.

102. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and class members have suffered injury, or are reasonably certain to suffer injury, and are entitled to damages in an amount to be proven at trial.

**COUNT II**

**Negligence Per Se**
**(Against All Defendants)**

103. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

104. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), Health Defendants had a duty to provide adequate data security practices in connection with safeguarding Plaintiffs' and class members' PII and PHI.

105. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), Accellion had a duty to provide adequate data security practices, including in connection with its sale of its FTA platform, to safeguard Plaintiffs' and class members' PII and PHI.

106. Pursuant to HIPAA (42 U.S.C. § 1302d *et. seq*.), Defendants each had a duty to implement reasonable safeguards to protect Plaintiffs' and class members' PII and PHI.

107. Defendants breached their duties to Plaintiffs and class members under the Federal Trade Commission Act (15 U.S.C. § 45), HIPAA (42 U.S.C. § 1302d *et. seq*.), Cal. Civ. Code §§ 1798.100, *et seq.*, Cal. Civ. Code §§ 56, *et seq.*, among other statutes, by failing to provide fair, reasonable, or adequate data security in connection with the sale and use of the FTA platform in order to safeguard Plaintiffs' and class members' PII and PHI.

108. Defendants' failure to comply with applicable laws and regulations constitutes negligence per se.

109. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiffs and class members, Plaintiffs and class members would not have been injured.

110. The injury and harm suffered by Plaintiffs and class members was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that they were failing to meet their duties, and that Defendants' breach would cause Plaintiffs and class members to experience the foreseeable harms associated with the exposure of their Personal Information.

111. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and class members now face an increased risk of future harm. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and class members have suffered injury and are entitled to damages in an amount to be proven at trial.

**COUNT III**

**Breach of Implied Contract**
**(Against CHW and all Health Net Defendants)**

112. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

113. CHW and the Health Net Defendants offered to provide healthcare, health insurance, pharmacy, and other health-related and medical services to Plaintiffs and class members in exchange for payment.

114. In connection with receiving these health-related services, Plaintiffs and class members entered into implied contracts with CHW and Health Net.

115. Pursuant to these implied contracts, Plaintiffs and class members paid money to CHW and the Health Net Defendants, whether directly or through their insurers, and provided them with their PII and PHI. In exchange, CHW and Health Net agreed, among other things: (1) to provide health-related services to Plaintiffs and class members; (2) to take reasonable measures to protect the security and confidentiality of Plaintiffs' and class members' PII and PHI; and (3) to protect Plaintiffs and class members' PII and PHI in compliance with federal and state laws and regulations and industry standards.

116. The protection of PII and PHI was a material term of the implied contracts between Plaintiffs and class members, on the one hand, and CHW and, separately, Health Net, on the other hand. Had Plaintiffs and class members known that the Health Defendants would not adequately protect customers' PII and PHI, they would not have paid for health-related services from them.

117. Plaintiffs and class members performed their obligations under the implied contracts when they provided CHW and Health Net with their PII and PHI and paid—directly

or through their insurers—for healthcare or other health-related services from those Defendants.

118. Necessarily implicit in the agreements between Plaintiffs/class members and the Health Defendants was the Health Defendants' obligation to take reasonable steps to secure and safeguard Plaintiffs' and class members' PII and PHI.

119. CHW and the Health Net Defendants breached their obligations under their implied contracts with Plaintiffs and class members by failing to implement and maintain reasonable security measures to protect their PII and PHI.

120. CHW's and the Health Net Defendants' breaches of their obligations under implied contracts with Plaintiffs and class members directly resulted in the Data Breach and/or the exposure of Plaintiffs and class members' PHI and PII to unauthorized persons.

121. The damages sustained by Plaintiffs and class members as described above were the direct and proximate result of CHW's and the Health Net Defendants' material breaches of their agreements.

122. Plaintiffs and other class members were damaged by these breaches of implied contracts because: (i) they paid—directly or through their insurers—for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII and PHI was was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII and PHI has been breached; (v) they were deprived of the value of their PII and PHI, for which there is a well-established national and international market; and/or (vi) they lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face.

**COUNT IV**

**Violations of California's Consumer Privacy Act**
**Cal. Civ. Code § 1798.100, *et seq.* ("CCPA")**
**(Against All Defendants)**

123. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

124. The CCPA was enacted to protect consumers' sensitive information from collection and use by businesses without appropriate notice and consent.

125. Through the conduct complained of herein, Defendants violated the CCPA by subjecting Plaintiffs' and California class members' PII and PHI to unauthorized access and exfiltration, theft, or disclosure as a result of Defendants' violation of their duties to implement and maintain reasonable security procedures and practices appropriate to the nature and protection of that information. Cal. Civ. Code § 1798.150(a).

126. In accordance with Cal. Civ. Code §1798.150(b), on May 3, 2021, prior to the filing of this Complaint, Plaintiffs' counsel served Defendants with notice of these CCPA violations by certified mail, return receipt requested.

127. On behalf of California class members, Plaintiffs seek injunctive relief in the form of an order enjoining Defendants from continuing to violate the CCPA.

128. If Defendants fail to agree to rectify the violations detailed above, individually and on behalf of California class members, Plaintiffs will seek actual, punitive, and statutory damages, restitution, and any other relief the Court deems proper as a result of Defendants' CCPA violations.

**COUNT V**

**Violation of the California Confidentiality of Medical Information Act**
**Cal. Civ. Code §§ 56, *et seq.* ("CMIA")**
**(Against All Defendants)**

129. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

130. Section 56.10(a) of the California Civil Code provides that "[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[.]"

131. CHW and the Health Net Defendants are providers of healthcare within the meaning of Cal. Civ. Code § 56.05(d).

132. Accellion is a "contractor" within the meaning of Cal. Civ. Code § 56.05(d) and/or a "business organized for the purpose of maintaining medical information" and/or a "business that

offers software or hardware to consumers . . . that is designed to maintain medical information" within the meaning of Cal. Civ. Code § 56.06(a) and (b), and maintained and continues to maintain "medical information," within the meaning of Civil Code § 56.05(j), for "patients," within the meaning of Cal. Civ. Code § 56.05(k).

133. Plaintiffs and California Medical Information Class members are "patients" within the meaning of Cal. Civ. Code § 56.05(k) and are "endanger[ed]" within the meaning of Cal. Civ. Code § 56.05(e), because Plaintiffs and California Medical Information Class members fear that disclosure of their PHI and Medical Information could subject them to harassment or abuse.

134. Plaintiffs and California Medical Information Class members, as patients, had their Medical Information created, maintained, preserved, and stored on Defendants' computer networks at the time of the Data Breach.

135. Defendants, through inadequate security, allowed an unauthorized third party to gain access to Plaintiffs and other California Medical Information Class members' Medical Information, PHI, other PII without the prior written authorization required by Cal. Civ. Code § 56.10 of the CMIA.

136. Defendants violated Cal. Civil Code § 56.101 of the CMIA by failing to maintain and preserve the confidentiality of Plaintiffs' and other California Medical Information Class members' Medical Information.

137. As a result of Defendants' above-described conduct, Plaintiffs and California Medical Information Class members have suffered damages from the unauthorized disclosure and release of their Medical Information.

138. As a direct and proximate result of Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, and violation of the CMIA, Plaintiffs and California Medical Information Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent, immediate and the continuing increased risk of identity theft, identity fraud and medical fraud—risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the

confidentiality of their Medical Information, (iv) statutory damages under the CMIA, (v) deprivation of the value of their Medical Information, for which there is a well-established national and international market, and/or (vi) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

139. Plaintiffs, individually and for each member of the California Medical Information Class, seeks nominal damages of one thousand dollars ($1,000) for each violation under Cal. Civ. Code § 56.36(b)(1), and actual damages suffered, if any, pursuant to Cal. Civ. Code § 56.36(b)(2), injunctive relief, as well as punitive damages of up to $3,000 per Plaintiff and California Medical Information Class member, and attorneys' fees, litigation expenses and court costs, pursuant to Civil Code § 56.35.

**COUNT VI**

**Violations of the California Customer Records Act**
**Cal. Civ. Code §§ 1798.80, *et seq.* ("CCRA")**
**(Against All Defendants)**

140. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

141. "[T]o ensure that personal information about California residents is protected," the California legislature enacted Civil Code § 1798.81.5, which requires that any business that "owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

142. By failing to implement reasonable measures to protect the Class's PHI and PII, Defendants violated Civil Code § 1798.81.5.

143. In addition, by failing to promptly notify all affected Class members that their PHI and PII Information had been exposed, Defendants violated Civil Code § 1798.82.

144. As a direct or proximate result of Defendants' violations of Civil Code §§ 1798.81.5 and 1798.82, Plaintiffs and California Class members were (and continue to be) injured and have suffered (and will continue to suffer) the damages and harms described herein.

145. In addition, by violating Civil Code §§ 1798.81.5 and 1798.82, Defendants "may be enjoined" under Civil Code Section 1798.84(e).

146. Defendants' violations of Civil Code §§ 1798.81.5 and 1798.82 also constitute unlawful acts or practices under the UCL, which affords the Court discretion to enter whatever orders may be necessary to prevent future unlawful acts or practices.

147. Plaintiffs accordingly request that the Court enter an injunction requiring Defendants to implement and maintain reasonable security procedures, including, but not limited to: (1) ordering that Accellion cease support of, and that Health Defendants and Accellion end the use of the FTA platform; (2) ordering that Defendants utilize strong industry standard data security measures and file transfer software for the transfer and storage of customer data; (3) ordering that Defendants, consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis; (4) ordering that Defendants engage third party security auditors and internal personnel to run automated security monitoring; (5) ordering that Defendants audit, test and train security personnel regarding any new or modified procedures; (6) ordering that Defendants purge, delete, and destroy in a reasonably secure manner Class member data not necessary for its provisions of services; (7) ordering that Defendants, consistent with industry standard practices, conduct regular database scanning and security checks; (8) ordering that Defendants, consistent with industry standard practices, evaluate all file transfer and other software, systems, or programs utilized for storage and transfer of sensitive PHI and PII for vulnerabilities to prevent threats to customers; (9) ordering that Defendants, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (10) ordering Defendants to meaningfully educate its customers about the threats they face as a result of the loss of their PHI and PII to third parties, as well as the steps Defendants' customers must take to protect themselves.

148. Plaintiffs further request that the Court require Defendant Accellion to identify all of its impacted clients other than the Health Defendants, and to identify and notify all members of the

Class who have not yet been informed of the Data Breach, and to notify affected persons of any future data breaches by email within 24 hours of discovery of a breach or possible breach and by mail within 72 hours.

**COUNT VII**

**Violations of the California Unfair Competition Law**
**Cal. Bus. & Prof. Code §§ 17200, *et seq.* ("UCL")**
**(Against All Defendants)**

149. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

150. Defendants engaged in unfair and unlawful business practices in violation of the UCL.

151. Plaintiffs suffered injury in fact and lost money or property as a result of Defendants' alleged violations of the UCL.

152. The acts, omissions, and conduct of Defendants as alleged constitute a "business practice" within the meaning of the UCL.

**Unlawful Prong**

153. Defendants violated the unlawful prong of the UCL by violating, without limitation, the CCRA, CCPA, and CMIA, as alleged above.

154. Health Defendants further violated the unlawful prong of the UCL by failing to honor the terms of their implied contracts with Plaintiffs, as alleged above.

155. Defendants' conduct also undermines California public policy—as reflected in statutes like the California Information Practices Act, Cal. Civ. Code §§ 1798, *et seq.*, the CCPA concerning consumer privacy, the CMIA concerning medical records and information, and the CCRA concerning customer records—which seek to protect customer and consumer data and ensure that entities who solicit or are entrusted with personal data utilize reasonable security measures.

**Unfair Prong**

156. Defendants' acts, omissions, and conduct also violate the unfair prong of the UCL because Defendants' acts, omissions, and conduct, as alleged herein, offended public policy and constitute immoral, unethical, oppressive, and unscrupulous activities that caused substantial injury,

including to Plaintiffs and other Class members. The gravity of Defendants' conduct outweighs any potential benefits attributable to such conduct and there were reasonably available alternatives to further Defendants' legitimate business interests, other than Defendants' conduct described herein.

157. Defendants' failure to utilize, and to disclose that they do not utilize, industry standard security practices but, instead, utilize the unsecured FTA platform, constitutes an unfair business practice under the UCL. Defendant's conduct is unethical, unscrupulous, and substantially injurious to the Class. While Defendants' competitors have spent the time and money necessary to appropriately safeguard their products, service, and customer information, Defendants have not—to the detriment of its customers and to competition.

**Fraudulent Prong**

158. By failing to disclose that they do not enlist industry standard security practices and utilized the unsecured FTA platform despite it being a legacy product that was known to be vulnerable, all of which rendered Class members particularly vulnerable to data breaches, Health Defendants engaged in UCL-violative practices.

159. A reasonable consumer would not have done business or paid for CHW's or the Health Net Defendants' services if they knew the truth about their security procedures and that they used a third-party vendor, i.e., Accellion, for file transfers that utilize unsecured transfer applications. By withholding material information about their security practices, Health Defendants were able to obtain customers who provided and entrusted their PII and PHI in connection with transacting business with the Health Defendants. Had Plaintiffs known the truth about Health Defendants' security procedures and that they do busines with Accellion using Accellion's unsecured FTA, Plaintiffs would not have done business with the Health Defendants.

160. As a result of Defendants' violations of the UCL, Plaintiffs and Class members are entitled to injunctive relief including, but not limited to: (1) ordering that Accellion cease support of, and that the Health Defendants and Accellion end the use of the FTA platform; (2) ordering that Defendants utilize strong industry standard data security measures and file transfer software for the transfer and storage of customer data; (3) ordering that Defendants, consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security

personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis; (4) ordering that Defendants engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (5) ordering that Defendants audit, test and train its security personnel regarding any new or modified procedures; (6) ordering that Defendants purge, delete, and destroy in a reasonably secure manner Class member data not necessary for its provisions of services; (7) ordering that Defendants, consistent with industry standard practices, conduct regular database scanning and security checks; (8) ordering that Defendants, consistent with industry standard practices, evaluate all file transfer and other software, systems, or programs utilized for storage and transfer of sensitive PII and PHI for vulnerabilities to prevent threats to customers; (9) ordering that Defendants, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (10) ordering Defendants to meaningfully educate its customers about the threats they face as a result of the loss of their PII and PHI to third parties, as well as the steps Defendants' customers must take to protect themselves.

161. As a result of Defendants' violations of the UCL, Plaintiffs and Class members have suffered injury in fact and lost money or property, as detailed herein. They agreed to transact business and purchase services from Health Defendants, or made purchases or spent money that they otherwise would not have made or spent, had they known the truth. Class members lost PHI and PII, which is their property, and privacy in that information. Class members lost money as a result of dealing with the fallout of the Data Breach, including, among other things, negative credit reports, the value of time they expended monitoring their credit and transactions, resolving fraudulent charges, and resolving issues that resulted from the fraudulent charges and replacement of cards. Plaintiffs and Class members are exposed to an ongoing risk of harm because their PHI and PII is not adequately protected by Defendants, and is now in the hands of criminals. Plaintiffs and Class members will continue to spend time, money, and resources in attempting to prevent and rectify fraud resulting from their PII and PHI being exposed by Defendants.

162. Plaintiffs request that the Court issue sufficient equitable relief to restore Class members to the position they would have been in had Defendants not engaged in violations of the UCL, including by ordering restitution of all funds that Defendants may have acquired from Plaintiffs and Class members as a result of those violations.

**COUNT VIII**

**Invasion of Privacy**
**(Intrusion Upon Seclusion)**
**(Against All Defendants)**

163. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

164. Plaintiffs and class members had a reasonable expectation of privacy in the PII and PHI that Defendants disclosed without authorization.

165. By failing to keep Plaintiffs' and class members' PII and PHI safe, knowingly utilizing the unsecure FTA platform, and disclosing PHI and PII to unauthorized parties for unauthorized use, Defendants unlawfully invaded Plaintiffs' and class members' privacy by, *inter alia*:

a. intruding into Plaintiffs' and class members' private affairs in a manner that would be highly offensive to a reasonable person; and

b. invading Plaintiffs' and class members' privacy by improperly using their PHI and PII properly obtained for a specific purpose for another purpose, or disclosing it to some third party;

c. failing to adequately secure their PII and PHI from disclosure to unauthorized persons;

d. enabling the disclosure of Plaintiffs' and class members' PII and PHI without consent.

166. Defendants knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiffs' and class members' position would consider its actions highly offensive.

167. Defendants knew that Accellion's FTA platform was vulnerable to data breaches prior to the Data Breach.

168. Defendants invaded Plaintiffs' and class Members' right to privacy and intruded into Plaintiffs' and class members' private affairs by disclosing their PII and PHI to unauthorized persons without their informed, voluntary, affirmative, and clear consent.

169. As a proximate result of such unauthorized disclosures, Plaintiffs' and class members' reasonable expectations of privacy in their PII and PHI was unduly frustrated and thwarted. Defendants' conduct amounted to a serious invasion of Plaintiffs' and class members' protected privacy interests.

170. In failing to protect Plaintiffs' and class members' PII and PHI, and in disclosing that information, Defendants acted with malice and oppression and in conscious disregard of Plaintiffs' and class members' rights to have such information kept confidential and private.

171. Plaintiffs seek injunctive relief on behalf of the class, restitution, and all other damages available under this Count.

**COUNT IX**

**Violation of the California Constitution, art. 1, § 1**
**(Against All Defendants)**

172. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

173. Plaintiffs and California Class members had a reasonable expectation of privacy in their PHI and PII that Defendants disclosed without authorization.

174. By failing to keep Plaintiffs' and California Class members' PII and PHI safe, and by disclosing said information to unauthorized parties for unauthorized use, Defendants invaded Plaintiffs' and California Class members' privacy by, *inter alia*:

a. intruding into their private affairs in a manner that would be highly offensive to a reasonable person; and

b. violating their right to privacy under California Constitution, Article 1, Section 1, through the improper use of private information properly obtained for a specific purpose for another purpose, or the disclosure of it to some third party.

175. Defendant invaded Plaintiff's and Class Members' right to privacy and intruded into Plaintiff's and Class Members' private affairs by disclosing their Personal Information to unauthorized persons without their informed, voluntary, affirmative, and clear consent.

176. Plaintiffs and California Class members have a reasonable expectation of privacy and a constitutionally protected privacy interest in their confidential PHI and PII.

177. As a proximate result of these unauthorized disclosures, Plaintiffs' and California Class members' reasonable expectations of privacy in their PII and PHI was unduly frustrated and thwarted, and their constitutional right to privacy was violated. Defendants' conduct amounted to a serious invasion of Plaintiff's and Class Members' protected privacy interests.

178. In failing to protect Plaintiffs' and California Class members' PII and PHI, and in disclosing the same, Defendants acted with malice and oppression and in conscious disregard of Plaintiffs' and California Class members' constitutional rights to have such information kept confidential and private.

179. Plaintiffs and California Class members seek compensatory and punitive damages, injunctive relief, restitution, attorneys' fees and costs, and all other damages available under this Count.

**COUNT X**

**Declaratory Relief**
**28 U.S.C. § 2201**
**(Against All Defendants)**

180. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

181. An actual controversy has arisen and exists between Plaintiffs and members of the Class, on the one hand, and Defendants, on the other hand, concerning the Data Breach and Defendants' failure to protect Plaintiffs' and class members' PHI and PII, including with respect to the issue of whether Defendants took adequate measures to protect that information. Plaintiffs and class members are entitled to judicial determination as to whether Defendants have performed and are adhering to all data privacy obligations as required by law or otherwise to protect Plaintiffs' and class members PHI and PII from unauthorized access, disclosure, and use.

182. A judicial determination of the rights and responsibilities of the parties regarding Defendants' privacy policies and whether they failed to adequately protect PHI and PII is necessary and appropriate to determine with certainty the rights of Plaintiffs and the class members, and so that there is clarity between the parties as to Defendants' data security obligations with respect to PHI and PII going forward, in view of the ongoing relationships between the parties.

**COUNT XI**

**Breach of Contract**
**(Against CHW and all Health Net Defendants)**

183. Plaintiffs realleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

184. Health Net's Privacy Policies—the Notice of Privacy Practices (NPP),[32] Web Privacy Policy (WPP),[33] and its Privacy Notice for California Residents (California Privacy Notice)[34]—formed an express contract in which Defendants promised to protect nonpublic personal information given to Defendants or that Defendants gathered on their own, from disclosure.

185. Plaintiffs and Class members performed their obligations under the contracts when they provided their PII/PHI to Defendants in relation to their purchase of Defendants' products and services.

186. Defendants breached their contractual obligation to protect the nonpublic personal information Defendants gathered when the information was exposed as part of the Data Breach.

187. As a direct and proximate result of the Data Breach, Plaintiffs and Class members have been harmed and have suffered, and will continue to suffer, damages and injuries.

---

[32] Health Net, *Privacy Practices, Notice of Privacy Practices*, (effective Aug. 14, 2017), https://www.healthnet.com/content/healthnet/en_us/disclaimers/legal/privacy-practices.html (last visited Nov. 22, 2021).

[33] Health Net, Privacy Policy, Web Privacy Policy, https://www.healthnet.com/content/healthnet/en_us/disclaimers/legal/privacy-policy.html (last visited Nov. 22, 2021).

[34] *Id.*

**COUNT XII**

**Breach of Confidence**
**(Against CHW and all Health Net Defendants)**

188. Plaintiffs realleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

189. At all times during Plaintiff's and Class Members' interactions with Defendants, Defendants were fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' PII that Plaintiffs and Class Members provided to Defendants.

190. Defendants' relationship with Plaintiffs and Class Members was governed by terms and expectations that Plaintiff's and Class Members' PII/PHI would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

191. Plaintiffs and Class Members provided their PII/PHI to Defendants with the explicit and implicit understandings that Defendants would protect and not permit the PII/PHI to be disseminated to any unauthorized third parties.

192. Plaintiffs and Class Members provided their PII/PHI to Defendants with the explicit and implicit understandings that Defendants would take precautions to protect that PII from unauthorized disclosure.

193. Defendants voluntarily received in confidence Plaintiff's and Class Members' PII/PHI with the understanding that PII/PHI would not be disclosed or disseminated to unauthorized third parties or to the public.

194. Due to Defendants' failure to prevent and avoid the Data Breach from occurring, Plaintiff's and Class Members' PII/PHI was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

195. As a proximate result of such unauthorized disclosures, Plaintiffs and Class Members suffered damages.

**COUNT XIII**

**Violation of the California HIV Disclosure Laws, Cal. Health & Safety Code § 120980 (Against All Defendants)**

196. Plaintiffs realleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

197. Among other things, California's Health & Safety Code prohibits the disclosure of HIV related information, including a patient's HIV status and test results. Cal. Health & Safety Code § 120980. Prior to disclosing Plaintiff's and Class Members' HIV-related health information, Defendants did not obtain any express written consent required by the statute. Defendants' disclosure of its patients' HIV status, test results, and treatment along with their personal identifying characteristics, is a negligent, willful, and malicious violation of the Health & Safety Code section 120980.

198. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have had their HIV related medical information, HIV status, and test results disclosed to third-parties without their express written authorization and have suffered damages as described in this Complaint. Accordingly, Health Net is liable for "all actual damages, including damages for economic, bodily, or psychological harm." Cal. Health & Safety Code § 120980(d). Additionally, Defendants are liable for civil penalties, fines, costs and attorneys' fees as permitted under the statute.

**PRAYER FOR RELIEF**

Plaintiffs, individually and on behalf of the class members, by and through undersigned counsel, respectfully request that the Court grant the following relief:

A. Certify this case as a class action pursuant to Fed. R. Civ. P. 23, and appoint Plaintiffs as class representative and undersigned counsel as class counsel;

B. Award Plaintiffs and class members actual and statutory damages, punitive damages, and monetary damages to the maximum extent allowable;

C. Award declaratory and injunctive relief as permitted by law or equity to assure that class members have an effective remedy, including enjoining Defendants from continuing the unlawful practices as set forth above;

D. Award Plaintiffs and class members pre-judgment and post-judgment interest to the maximum extent allowable;

E. Award Plaintiffs and class members reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Award Plaintiffs and Class Members such other favorable relief as allowable under law or at equity.

**JURY TRIAL DEMANDED**

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

Dated: November 23, 2021

Respectfully submitted,

**AHDOOT & WOLFSON, PC**

By: */s/ Tina Wolfson*

Tina Wolfson (SBN 174806)
Robert Ahdoot (SBN 172098)
2600 W. Olive Avenue, Suite 500
Burbank, CA 91505-4521
Telephone: 310.474.9111
Facsimile: 310.474.8585
*twolfson@ahdootwolfson.com*
*rahdoot@ahdootwolfson.com*

and

Andrew W. Ferich (*pro hac vice* to be filed)
**AHDOOT & WOLFSON, PC**
201 King of Prussia Road, Suite 650
Radnor, PA 19087
Telephone: 310.474.9111
Facsimile: 310.474.8585
*aferich@ahdootwolfson.com*

Timothy G. Blood (149343)
Paula R. Brown (254142)
Jennifer L. MacPherson (202021)
**BLOOD HURST & O'REARDON, LLP**
501 West Broadway, Suite 1490
San Diego, CA 92101
Telephone: 619.338.1100
Facsimile: 619.338.1101
*tblood@bholaw.com*
*pbrown@bholaw.com*
*jmacpherson@bholaw.com*

Laurence D. King (SBN 206423)
Matthew B. George (SBN 239322)
**KAPLAN FOX & KILSHEIMER LLP**
1999 Harrison Street, Suite 1560
Oakland, CA 94612
Telephone: 415.772.4700
Facsimile: 415.772.4707
*lking@kaplanfox.com*
*mgeorge@kaplanfox.com*

*Attorneys for Plaintiffs and the Proposed Class*